

Konfigurieren des SD-WAN-cEdge-Routers zur Beschränkung des SSH-Zugriffs

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Topologie](#)

[Einschränken des SSH-Zugriffs](#)

[Verbindungsüberprüfung](#)

[Validierung der Zugriffskontrollliste](#)

[Konfiguration der Zugriffskontrollliste](#)

[Konfiguration auf der vManage-GUI](#)

[Verifizierung](#)

[Zugehörige Informationen](#)

[Konfigurationsleitfaden für Cisco SD-WAN-Richtlinien, Cisco IOS XE Version 17.x](#)

Einleitung

In diesem Dokument wird der Prozess zum Beschränken der Secure Shell (SSH)-Verbindung auf den Cisco IOS-XE® SD-WAN-Router beschrieben.

Voraussetzungen

Anforderungen

Die Kontrollverbindung zwischen vManage und cEdge ist erforderlich, um die richtigen Tests durchzuführen.

Verwendete Komponenten

Dieses Verfahren ist nicht auf Softwareversionen in Cisco Edge- oder vManage-Geräten beschränkt. Daher können für diese Schritte alle Versionen verwendet werden. Dieses Dokument gilt jedoch nur für cEdge-Router. Dies ist für die Konfiguration erforderlich:

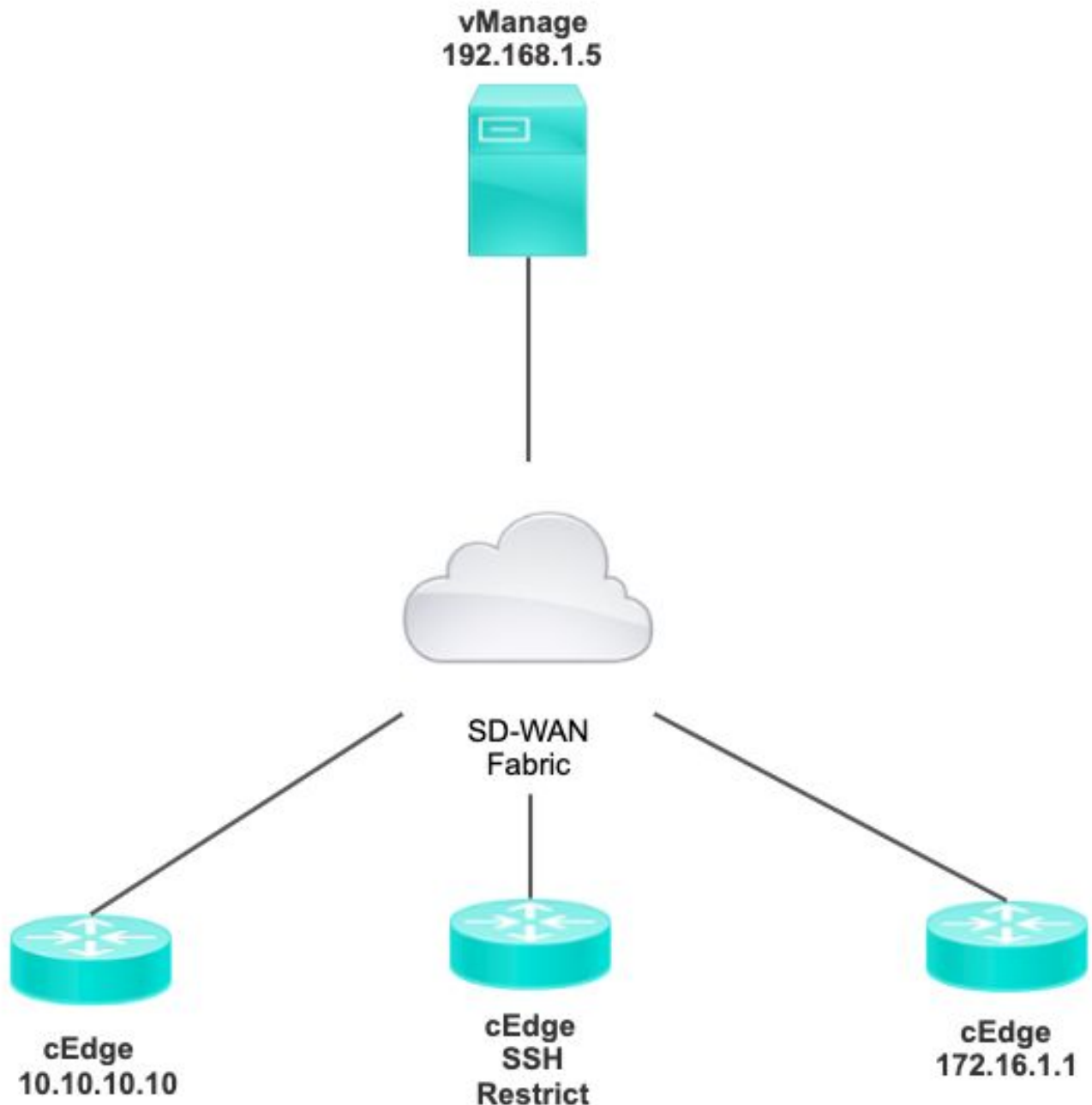
- Cisco cEdge-Router (virtuell oder physisch)
- Cisco vManager

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.

Hintergrundinformationen

Zweck dieser Demonstration ist es, die Konfiguration auf cEdge zu zeigen, um den SSH-Zugriff von cEdge 172.16.1.1 einzuschränken, jedoch cEdge 10.10.10.10 und vManage zuzulassen.

Topologie



Einschränken des SSH-Zugriffs

Verbindungsüberprüfung

Es muss überprüft werden, ob der cEdge-Router den vManager erreichen kann. vManage

verwendet standardmäßig IP 192.168.1.5, um sich bei cEdge-Geräten anzumelden.

Öffnen Sie in der vManage-GUI SSH zu cEdge, und stellen Sie sicher, dass die verbundene IP den nächsten Ausgang hat:

```
cEdge#show
users
```

Line	User	Host(s)	Idle	
Location				
*866 vty 0	admin	idle	00:00:00	
192.168.1.5				
Interface	User	Mode	Idle	Peer Address

Stellen Sie sicher, dass vManage für die Anmeldung bei cEdge nicht die Tunnel-, System- oder öffentliche IP-Adresse verwendet.

Um die IP zu bestätigen, die für die Anmeldung bei cEdge verwendet wird, können Sie die nächste Zugriffsliste verwenden.

```
cEdge#show run | section access
ip access-list extended VTY_FILTER_SSH
5 permit ip any any log <<<< with this sequence you can verify the IP of the
device that tried to access.
```

Validierung der Zugriffskontrollliste

Zugriffsliste auf VTY-Leitung angewendet

```
cEdge#show sdwan running-config | section vty
line vty 0 4
access-class VTY_FILTER_SSH in vrf-also
transport input ssh
```

Nachdem die ACL angewendet wurde, können Sie SSH von vManage auf cEdge erneut öffnen und die nächste in den Protokollen generierte Meldung sehen.

Diese Meldung wird durch den Befehl **show logging** angezeigt.

```
*Jul 13 15:05:47.781: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Tadmin] [Source:
192.168.1.5] [localport: 22] at 15:05:47 UTC Tue Jul 13 2022
```

Im vorherigen Protokoll sehen Sie Lokaler Port 22. Das bedeutet, dass 192.168.1.5 versucht hat, SSH in cEdge zu öffnen.

Nachdem Sie nun bestätigt haben, dass die Quell-IP 192.168.1.5 lautet, können Sie die ACL mit der richtigen IP konfigurieren, damit vManage eine SSH-Sitzung öffnen kann.

Konfiguration der Zugriffskontrollliste

Wenn cEdge über mehrere Sequenzen verfügt, stellen Sie sicher, dass die neue Sequenz oben in der ACL hinzugefügt wird.

Vorher:

```
cEdge#show access-list VTY_FILTER_SSH
Extended IP access list VTY_FILTER_SSH
10 permit tcp 10.10.10.10 0.0.0.15 any eq 22 100 deny ip any any log
```

Konfigurationsbeispiel:

```
cEdge#config-transaction
cEdge(config)# ip access-list
cEdge(config)# ip access-list extended VTY_FILTER_SSH
cEdge(config-ext-nacl)# 5 permit ip host 192.168.1.5 any log
cEdge(config-ext-nacl)# commit
Commit complete.
```

Neue Sequenz:

```
cEdge#show access-list VTY_FILTER_SSH
Extended IP access list VTY_FILTER_SSH
5 permit ip host 192.168.1.5 any log <<<< New sequence to allow vManage to SSH
10 permit tcp 10.10.10.10 0.0.0.15 any eq 22 100 deny ip any any log <<<< This sequence deny all
other SSH connections
```

Wenden Sie ACL auf VTY-Leitung an.

```
cEdge#show sdwan running-config | section vty
line vty 0 4      access-class VTY_FILTER_SSH in vrf-also transport input ssh
!
                                     line vty 5 80
                                     access-class VTY_FILTER_SSH in vrf-also transport
input ssh
```

Konfiguration auf der vManage-GUI

Wenn an das cEdge-Gerät eine Vorlage angehängt ist, können Sie das nächste Verfahren verwenden.

Schritt 1: Erstellen Sie eine ACL

Navigieren Sie zu **Konfiguration > Benutzerdefinierte Optionen > Zugriffskontrollliste > Gerätezugriffsrichtlinie hinzufügen > IPv4-Gerätezugriffsrichtlinie hinzufügen**.

Fügen Sie den Namen und die Beschreibung der ACL hinzu, klicken Sie auf **Add ACL Sequence (ACL-Sequenz hinzufügen)**, und wählen Sie dann **Sequence Rule (Sequenzregel)** aus.

Name	SDWAN_CEDGE_ACCESS
Description	SDWAN_CEDGE_ACCESS

+ Add ACL Sequence

↑↓ Drag & drop to reorder

⋮ Device Access Control List ⋮



Device Access Control List



+ Sequence Rule

Drag and drop to re-arrange rules

Wählen Sie **Device Access Protocol > SSH** aus.

Wählen Sie dann die **Präfixliste für Quelldaten** aus.

Device Access Control List

+ Sequence Rule Drag and drop to re-arrange rules

Match Actions

Source Data Prefix Source Port Destination Data Prefix Device Access Protocol VPN

Match Conditions	Actions
Device Access Protocol (required) SSH	Accept Enabled
Source Data Prefix List ALLOWED x	

Klicken Sie auf **Aktionen**, wählen Sie **Akzeptieren** aus, und klicken Sie dann auf **Save Match And Actions**.

Schließlich können Sie auswählen, **Save Device Access Control List Policy**.

Device Access Control List Device Access Control Lis

Sequence Rule Drag and drop to re-arrange rules

Match **Actions**

Accept Drop **Counter**

Match Conditions

Device Access Protocol (required)

Source Data Prefix List

Source: IP Prefix

Variables: Disabled

Actions

Accept

Cancel **Save Match And Actions**

Save Device Access Control List Policy Cancel

Schritt 2: Lokalisierte Richtlinie erstellen

Navigieren Sie zu **Configuration > Localized Policy > Add Policy > Configure Access Control List > Add Device Access Policy > Import Existing**.

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 Device Access Policy
- Add IPv6 Device Access Policy
- Import Existing**

Name	Type	Description	Mode	Reference Count
No data available				

Wählen Sie die vorherige **ACL aus**, und klicken Sie auf **Importieren**.

Import Existing Device Access Control List Policy

Policy

SDWAN_CEDGE_ACCESS

Fügen Sie den Richtliniennamen und die Richtlinienbeschreibung hinzu, und klicken Sie dann

auf Save Policy Changes.

Policy Overview Forwarding Class/QoS Access Control Lists 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 ⓘ

Schritt 3: Lokalisierte Richtlinie an Gerätevorlage anhängen

Navigieren Sie zu **Configuration > Template > Device > Select the Device**, und klicken Sie auf **> ... > Edit > Additional Templates > Policy > SDWAN_CEDGE > Update**.

Cisco vManage Select Resource Group Configuration · Temp

Device Feature

Basic Information Transport & Management VPN Service VPN Cellular Additional Templates

TrustSec

CLI Add-On Template

Policy

Bevor Sie die Vorlage übertragen, können Sie die Konfigurationsdifferenz überprüfen.

Neue ACL-Konfiguration

```
3 no ip source-route
151 no ip source-route
152 ip access-list extended SDWAN_CEDGE_ACCESS-acl-22
153 10 permit tcp 192.168.1.5 0.0.0.0 any eq 22
154 20 permit tcp 192.169.20.0 0.0.0.15 any eq 22
155 30 deny tcp any any eq 22
156 !
```

ACL auf Posten-VTY angewendet

```
236 !
237 line vty 0 4
238 transport input ssh
239 !
240 line vty 5 80
241 transport input ssh
242 .

217 !
218 line vty 0 4
219 access-class SDWAN_CEDGE_ACCESS-acl-22 in vrf-also
220 transport input ssh
221 !
222 line vty 5 80
223 access-class SDWAN_CEDGE_ACCESS-acl-22 in vrf-also
224 transport input ssh
225 .
```

Verifizierung

Jetzt können Sie den SSH-Zugriff auf cEdge erneut mit früheren Filtern von vManage über den folgenden Pfad testen: **Menü > Tools > SSH Terminal**.

Router versucht, SSH auf 192.168.10.114m zu übertragen

```
Router#ssh 192.168.10.114
% Connection refused by remote host

Router#
```

Wenn Sie die ACL-Zähler überprüfen, können Sie bestätigen, dass für SEQ 30 eine Übereinstimmung gefunden wurde und die SSH-Verbindung abgelehnt wurde.

```
c8000v-1# sh access-lists
Extended IP access list SDWAN_CEDGE_ACCESS-acl-22
 10 permit tcp host 192.168.1.5 any eq 22
 20 permit tcp 192.169.20.0 0.0.0.15 any eq 22
 30 deny tcp any any eq 22 (1 match)
```

Zugehörige Informationen

[Konfigurationsleitfaden für Cisco SD-WAN-Richtlinien, Cisco IOS XE Version 17.x](#)

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.