

Configuration du routeur cEdge SD-WAN pour limiter l'accès SSH

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Topologie](#)

[Procédure de restriction d'accès SSH](#)

[Vérification de connectivité](#)

[Validation de liste de contrôle d'accès](#)

[Configuration de la liste de contrôle d'accès](#)

[Configuration sur l'interface graphique vManage](#)

[Vérification](#)

[Informations connexes](#)

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

Introduction

Ce document décrit le processus de restriction de la connexion Secure Shell (SSH) au routeur Cisco IOS-XE® SD-WAN.

Conditions préalables

Exigences

Les connexions de contrôle entre vManage et cEdge sont nécessaires pour effectuer les tests appropriés.

Composants utilisés

Cette procédure n'est pas limitée aux versions logicielles des périphériques Cisco Edge ou vManage. Par conséquent, toutes les versions peuvent être utilisées avec ces étapes. Cependant, ce document est exclusif pour les routeurs cEdge. Pour configurer, ceci est nécessaire :

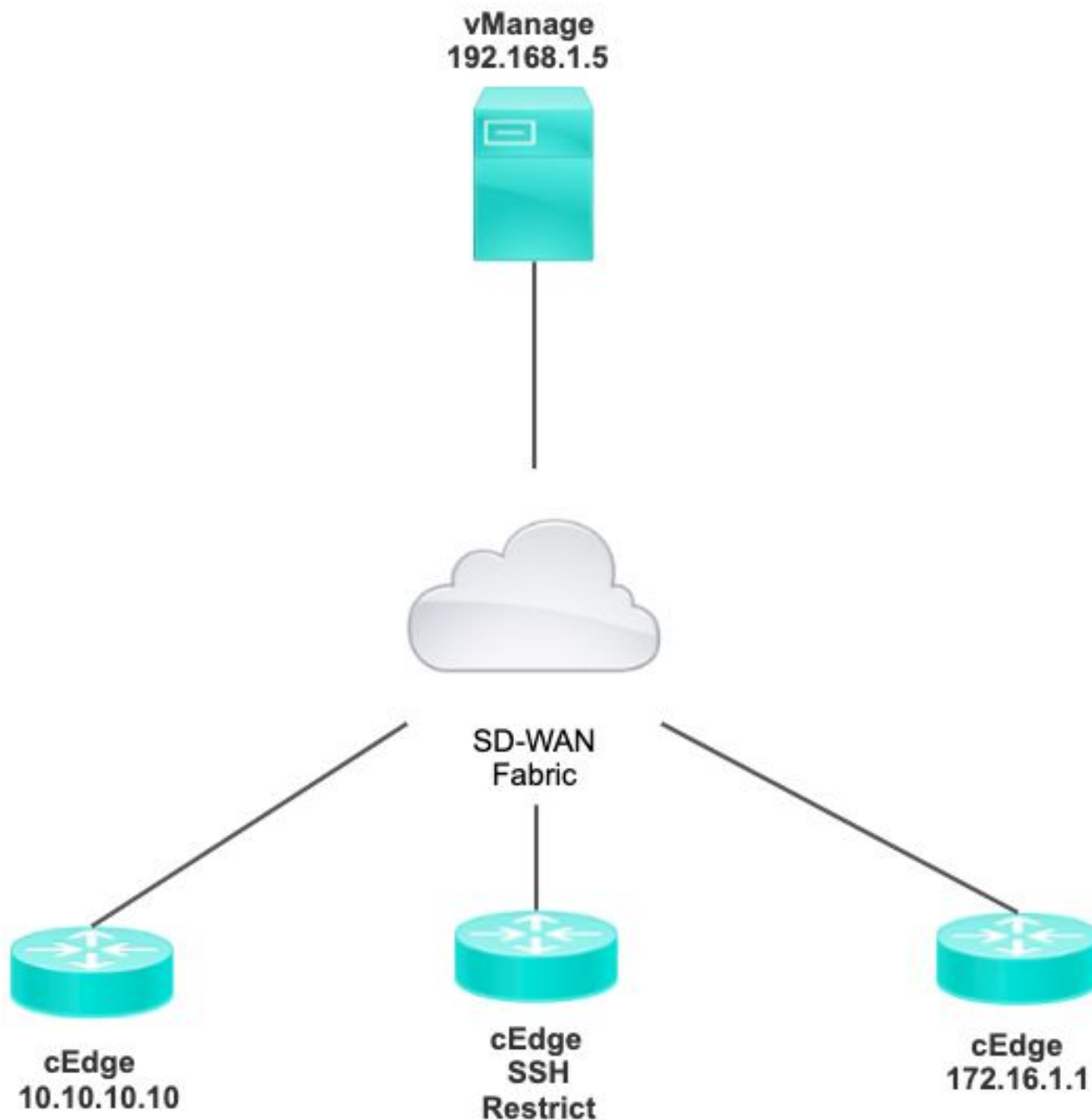
- Routeur Cisco Edge (virtuel ou physique)
- Cisco vManage

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.

Informations générales

L'objectif de cette démonstration est de montrer la configuration sur cEdge pour restreindre l'accès SSH à partir de cEdge 172.16.1.1 mais autoriser cEdge 10.10.10.10 et vManage.

Topologie



Procédure de restriction d'accès SSH

Vérification de connectivité

La vérification de la connectivité est nécessaire pour valider que le routeur cEdge peut atteindre le

vManage. Par défaut, vManage utilise IP 192.168.1.5 pour se connecter aux périphériques cEdge.

À partir de l'interface utilisateur graphique de vManage, ouvrez SSH vers cEdge et assurez-vous que l'adresse IP qui a été connectée présente le résultat suivant :

```
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
```

Vérifiez que vManage n'utilise pas le tunnel, le système ou l'adresse IP publique pour se connecter à cEdge.

Pour confirmer l'adresse IP utilisée pour se connecter à cEdge, vous pouvez utiliser la liste de contrôle d'accès suivante.

```
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.
```

Validation de liste de contrôle d'accès

Liste d'accès appliquée sur la ligne VTY

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

Une fois la liste de contrôle d'accès appliquée, vous pouvez rouvrir SSH de vManage à cEdge et afficher le message suivant généré dans les journaux.

Ce message peut être vu avec la commande : **show logging**.

```
*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
```

Dans le journal précédent, vous pouvez voir le port local 22. Cela signifie que 192.168.1.5 a essayé d'ouvrir SSH vers cEdge.

Maintenant que vous avez confirmé que l'adresse IP source est 192.168.1.5, vous pouvez configurer la liste de contrôle d'accès avec l'adresse IP correcte pour permettre à vManage d'ouvrir une session SSH.

Configuration de la liste de contrôle d'accès

Si cEdge a plusieurs séquences, assurez-vous d'ajouter la nouvelle séquence en haut de la liste de contrôle d'accès.

Avant :

```
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
```

Exemple de configuration :

```
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.
```

Nouvelle séquence :

```
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
```

Appliquez la liste de contrôle d'accès sur la ligne VTY.

```
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
```

Configuration sur l'interface graphique vManage

Si un modèle est attaché au périphérique cEdge, vous pouvez suivre la procédure ci-dessous.

Étape 1. Créez une liste ACL

Accédez à **Configuration > Custom Options > Access Control List > Add Device Access Policy > Add ipv4 Device Access Policy**

Ajoutez le nom et la description de la liste de contrôle d'accès, cliquez sur **Add ACL Sequence**, puis sélectionnez **Sequence Rule**

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

Sélectionnez **Device Access Protocol > SSH**

Sélectionnez ensuite la liste de **préfixes de données source**.

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	

Cliquez sur **Actions**, sélectionnez **Accepter**, puis cliquez sur Save Match And Actions.

Enfin, vous pouvez sélectionner 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) SSH

Source Data Prefix List ×

ALLOWED ×

Source: IP Prefix Example: 10.0.0.0/12

Variables: Disabled

Actions

Accept Enabled

Cancel Save Match And Actions

Save Device Access Control List Policy Cancel

Étape 2. Créer une stratégie localisée

Accédez à **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				

Sélectionnez la liste précédente et cliquez sur **Importer**.

Import Existing Device Access Control List Policy

Policy

SDWAN_CEDGE_ACCESS

Ajoutez le nom et la description de la stratégie, puis cliquez sur **Save Policy Changes**.

Enter name and description for your localized master policy

Policy Name SDWAN_CEDGE

Policy Description SDWAN_CEDGE

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 ⓘ

Preview

Save Policy Changes

Cancel

Étape 3. Joindre la stratégie localisée au modèle de périphérique

Accédez à **Configuration > Template > Device > Sélectionnez le Device et cliquez sur > ... > Edit > Additional Templates > Policy > SDWAN_CEDGE > Update.**

Device

Feature

Basic Information

Transport & Management VPN

Service VPN

Cellular

Additional Templates

TrustSec

Choose...

CLI Add-On Template

Choose...

Policy

SDWAN_CEDGE

Avant d'envoyer le modèle, vous pouvez vérifier la différence de configuration.

Nouvelle configuration ACL

```
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 appliquée à la ligne vty

236	!	217	!
237	line vty 0 4	218	line vty 0 4
238	transport input ssh	219	access-class SDWAN_CEDGE_ACCESS-acl-22 in vrf-also
239	!	220	transport input ssh
240	line vty 5 80	221	!
241	transport input ssh	222	line vty 5 80
242	!	223	access-class SDWAN_CEDGE_ACCESS-acl-22 in vrf-also
243	.	224	transport input ssh
		225	.

Vérification

Vous pouvez maintenant tester à nouveau l'accès SSH à cEdge avec les filtres précédents de vManage avec ce chemin : **Menu > Tools > SSH Terminal**.

Le routeur a tenté d'établir une connexion SSH vers 192.168.10.114m

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

Router#
```

Si vous vérifiez les compteurs ACL, vous pouvez confirmer que Seq 30 a 1 correspondance et que la connexion SSH a été refusée.

```
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)
```

Informations connexes

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

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.