

# Configurar o roteador SD-WAN cEdge para restringir o acesso SSH

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Topologia](#)

[Restringir o procedimento de acesso SSH](#)

[Verificação de conectividade](#)

[Validação da Lista de Controle de Acesso](#)

[Configuração da Lista de Controle de Acesso](#)

[Configuração na GUI do vManage](#)

[Verificação](#)

[Informações Relacionadas](#)

[Guia de configuração de políticas de SD-WAN da Cisco, Cisco IOS XE versão 17.x](#)

## Introduction

Este documento descreve o processo para restringir a conexão Secure Shell (SSH) ao roteador SD-WAN Cisco IOS-XE®.

## Prerequisites

### Requirements

A conexão de controle entre o vManage e o cEdge é necessária para fazer os testes apropriados.

### Componentes Utilizados

Esse procedimento não está restrito a nenhuma versão de software nos dispositivos Cisco Edge ou vManage, portanto, todas as versões podem ser usadas para executar essas etapas. No entanto, este documento é exclusivo para roteadores cEdge. Para configurar, é necessário:

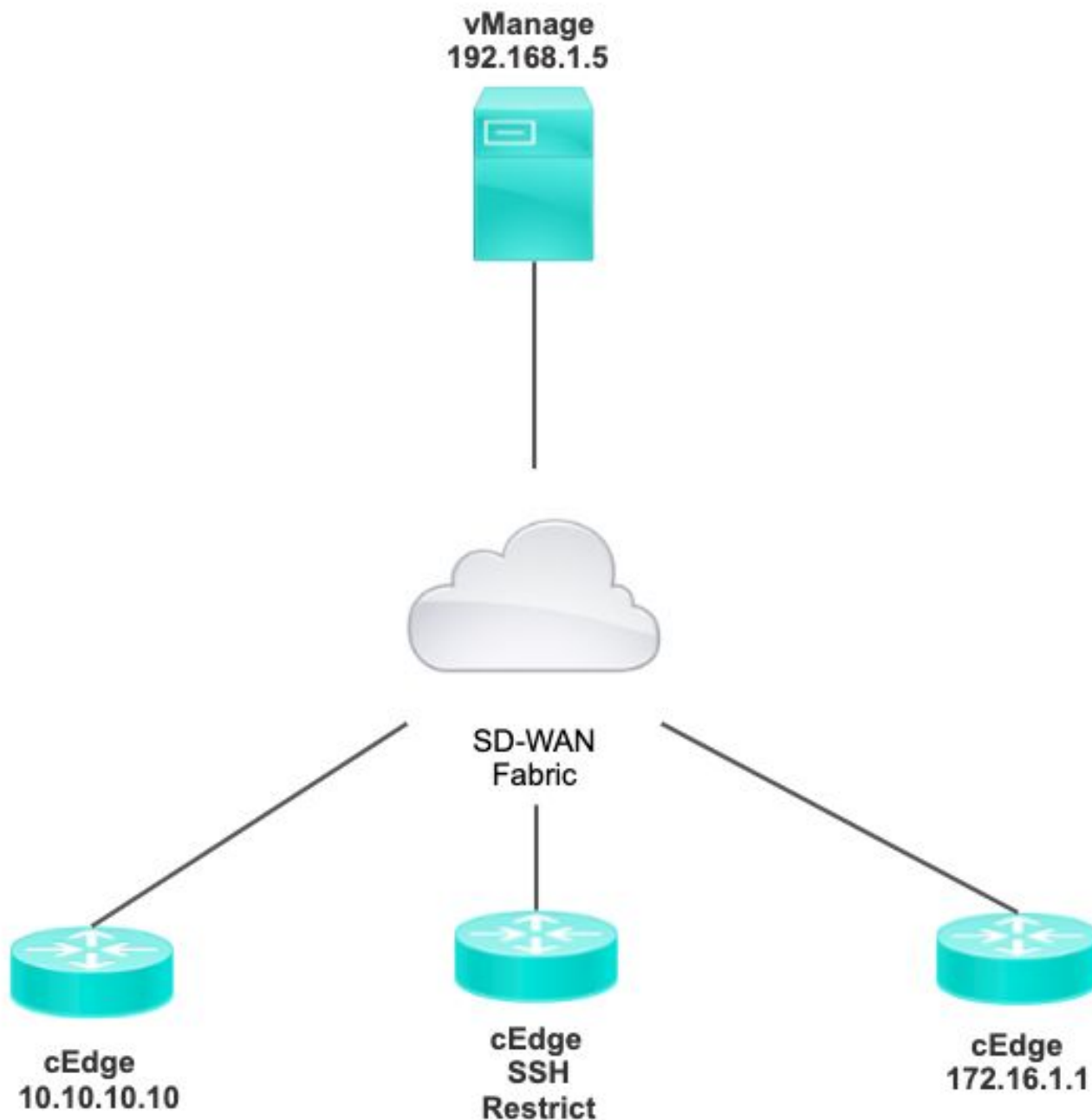
- Roteador Cisco cEdge (virtual ou físico)
- Cisco vManage

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

A finalidade desta demonstração é mostrar a configuração no cEdge para restringir o acesso SSH a partir do cEdge 172.16.1.1, mas permitir o cEdge 10.10.10.10 e o vManage.

## Topologia



## Restringir o procedimento de acesso SSH

### Verificação de conectividade

A verificação de conectividade é necessária para validar se o roteador cEdge pode acessar o

vManage. Por padrão, o vManage usa o IP 192.168.1.5 para fazer login em dispositivos cEdge.

Na GUI do vManage, abra o SSH para o cEdge e verifique se o IP conectado tem a próxima saída:

```
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
```

Certifique-se de que o vManage não use o túnel, o sistema ou o endereço ip público para fazer login no cEdge.

Para confirmar o IP usado para fazer login no cEdge, você pode usar a próxima lista de acesso.

```
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.
```

## Validação da Lista de Controle de Acesso

Lista de acesso aplicada na linha VTY

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

Depois que a ACL foi aplicada, você pode abrir o SSH novamente do vManage para o cEdge e ver a próxima mensagem gerada nos logs.

Essa mensagem pode ser vista com o comando: **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
```

No registro anterior, você pode ver a porta local 22. Isso significa que 192.168.1.5 tentou abrir o SSH para o cEdge.

Agora que você confirmou que o IP de origem é 192.168.1.5, você pode configurar a ACL com o IP correto para permitir que o vManage possa abrir a sessão SSH.

## Configuração da Lista de Controle de Acesso

Se o cEdge tiver várias sequências, certifique-se de adicionar a nova sequência na parte superior

da ACL.

Antes:

```
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
```

Exemplo de configuração:

```
cEdge#config-transaction
cEdgeconfig)# 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
cEdgeconfig-ext-nacl)# commit
Commit complete.
```

Nova sequência:

```
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
```

Aplice a ACL na linha 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
```

## Configuração na GUI do vManage

Se o dispositivo cEdge tiver um modelo anexado, você poderá usar o próximo procedimento.

### Etapa 1. Crie uma ACL

Navegue até **Configuration > Custom Options > Access Control List > Add Device Access Policy > Add ipv4 Device Access Policy**

Adicione o nome e a descrição da ACL, clique em **Add ACL Sequence** e selecione **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

Selecione **Device Access Protocol >SSH**

Em seguida, selecione a **Lista de prefixos de dados de origem**.

**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

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

Clique em **Ações**, selecione **Aceitar** e clique em **Save Match And Actions**.

Finalmente, você pode selecionar **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](#)

## Etapa 2. Criar Política Localizada

Navegue até **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				

Selecione a **ACL** anterior e clique em **Importar**.

### Import Existing Device Access Control List Policy

Policy

SDWAN\_CEDGE\_ACCESS

Adicione o Nome da política e a Descrição da política e clique em **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: How often packet flows are logged (maximum 2147483647) i

FNF IPv4 Max Cache Entries: Enter the cache size (range 16 - 2000000) i

FNF IPv6 Max Cache Entries: Enter the cache size (range 16 - 2000000) i

Preview Save Policy Changes Cancel

**Etapa 3.** Anexar a política localizada ao modelo do dispositivo

Navegue para **Configuration > Template > Device > Select the Device** e clique em **> ... > 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 Choose...

CLI Add-On Template Choose...

**Policy SDWAN\_CEDGE**

Antes de enviar o modelo, você pode verificar a Diferença de configuração.

**Nova configuração de ACL**

```

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 aplicada à linha 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
		224	transport input ssh
		225	.

## Verificação

Agora você pode testar novamente o acesso SSH ao cEdge com filtros anteriores do vManage com este caminho: **Menu > Ferramentas > Terminal SSH**.

O roteador tentou usar SSH para 192.168.10.114m

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

Router#
```

Se você verificar os contadores da ACL, poderá confirmar se Seq 30 tem 1 correspondência e se a conexão SSH foi negada.

```
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)
```

## Informações Relacionadas

[Guia de configuração de políticas de SD-WAN da Cisco, Cisco IOS XE versão 17.x](#)



## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.