

配置SD-WAN cEdge路由器以限制SSH訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[拓撲](#)

[限制SSH訪問過程](#)

[連線驗證](#)

[訪問控制清單驗證](#)

[訪問控制清單配置](#)

[vManage GUI上的配置](#)

[驗證](#)

[相關資訊](#)

[Cisco SD-WAN策略配置指南, Cisco IOS XE版本17.x](#)

簡介

本檔案介紹限制與Cisco IOS-XE® SD-WAN路由器的安全殼層(SSH)連線的程式。

必要條件

需求

需要在vManage和cEdge之間進行控制連線，才能進行正確的測試。

採用元件

此過程不限於Cisco Edge或vManage裝置中的任何軟體版本，因此可以使用所有版本執行這些步驟。但是，本文檔僅適用於cEdge路由器。要進行配置，需要執行以下操作：

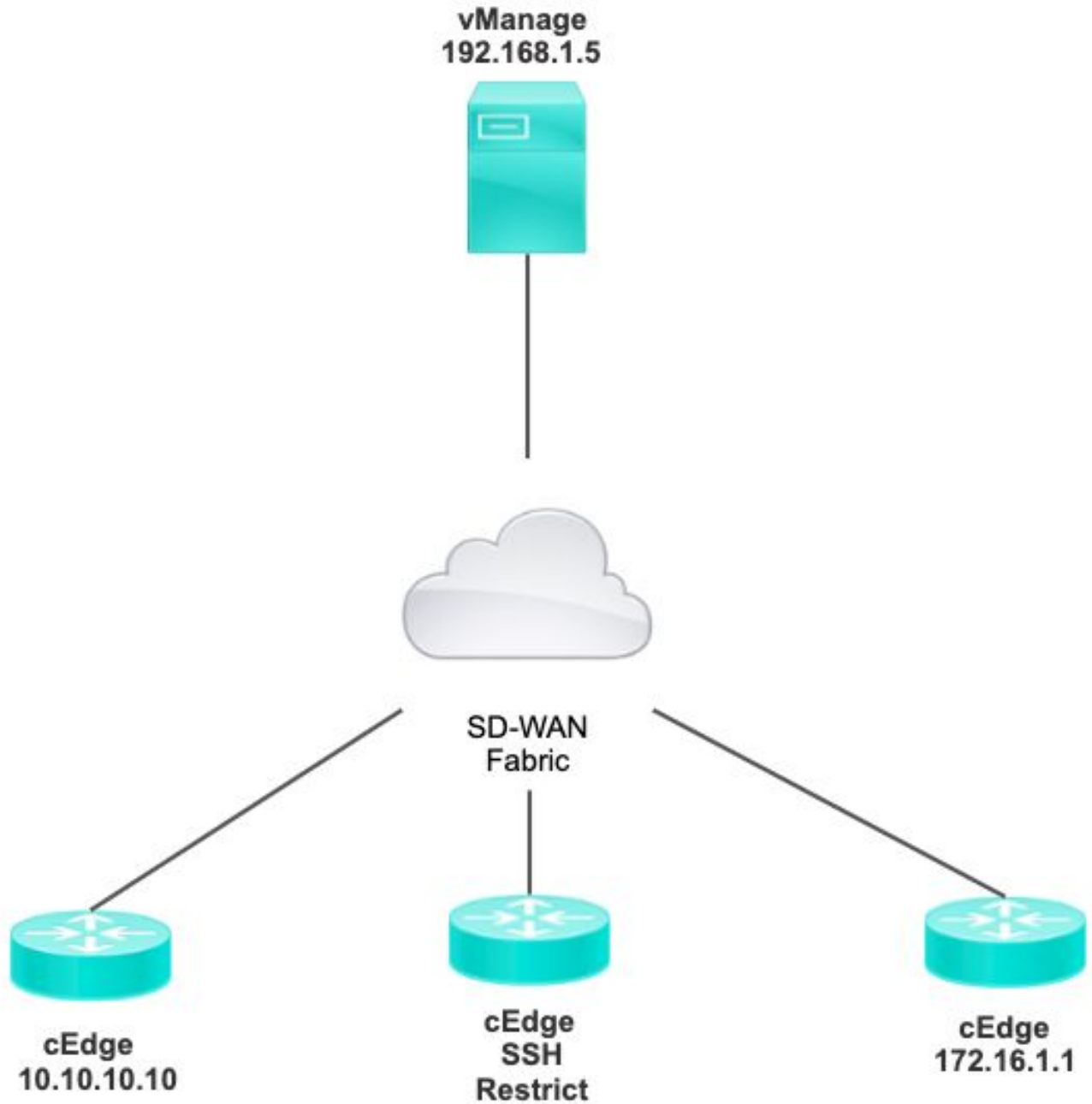
- Cisco cEdge路由器 (虛擬或物理)
- Cisco vManage

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本演示的目的是顯示cEdge上的配置，以限制從cEdge 172.16.1.1進行SSH訪問，但允許cEdge 10.10.10.10和vManage。

拓撲



限制SSH訪問過程

連線驗證

驗證連線性是驗證cEdge路由器可以訪問vManage所必需的。預設情況下，vManage使用IP 192.168.1.5登入到cEdge裝置。

在vManage GUI中，開啟SSH到cEdge，並確保連線的IP具有下一個輸出：

```
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
```

確保vManage不使用隧道、系統或公共IP地址登入cEdge。

要確認用於登入cEdge的IP，您可以使用下一個訪問清單。

```
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.
```

訪問控制清單驗證

在VTY線路上應用的訪問清單

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

應用ACL後，您可以從vManage再次開啟SSH到cEdge，並檢視日誌中生成的下一條消息。

此消息可通過命令show logging看到。

```
*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
```

在上一個日誌中，您可以看到本地埠22。這表示192.168.1.5嘗試開啟到cEdge的SSH。

現在您已確認源IP是192.168.1.5，現在可以使用正確的IP配置ACL以允許vManage能夠開啟SSH會話。

訪問控制清單配置

如果cEdge有多個序列，請確保在ACL的頂部新增新序列。

之前：

```
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
```

組態範例:

```
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.
```

新序列：

```
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
```

在VTY線路上應用ACL。

```
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
```

vManage GUI上的配置

如果cEdge裝置附加了模板，則可以使用下一過程。

步驟1.建立ACL

導航到Configuration > Custom Options > Access Control List > Add Device Access Policy > Add ipv4 Device Access Policy

新增ACL的名稱和說明，然後按一下Add ACL Sequence，然後選擇Sequence Rule

The screenshot displays the vManage configuration interface for adding an IPv4 ACL policy. The breadcrumb path is: Localized Policy > Access Control Lists Policy > Add Device IPV4 ACL Policy. A red box highlights the 'Name' and 'Description' fields, both containing the text 'SDWAN_CEDGE_ACCESS'. Below this, there is a button labeled '+ Add ACL Sequence'. To the right, under the heading 'Device Access Control List', there is a '+ Sequence Rule' button with the instruction 'Drag and drop to re-arrange rules'. At the bottom, a 'Device Access Control List' entry is visible with a drag handle and a menu icon.

選擇Device Access Protocol >SSH

然後選擇源數據字首清單。

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

Device Access Protocol (required) SSH

Source Data Prefix List ALLOWED x

Actions

Accept Enabled

按一下Actions，選擇Accept，然後按一下 Save Match And Actions.

最後，您可以選擇 Save Device Access Control List Policy.

Device Access Control List

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 x

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

步驟2.建立本地化策略

導航到Configuration > Localized Policy > Add Policy > Configure Access Control List > Add Device Access Policy > Import Existing。

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

選擇上一個ACL，然後按一下Import。

Import Existing Device Access Control List Policy

Policy

SDWAN_CEDGE_ACCESS

Cancel

Import

新增策略名稱和策略描述，然後按一下 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

步驟3.將本地化策略附加到裝置模板

導航到 Configuration > Template > Device > Select the Device , 然後點選 > ... > Edit > Additional Templates > Policy > SDWAN_CEDGE > Update。

Device

Feature

Basic Information

Transport & Management VPN

Service VPN

Cellular

Additional Templates

TrustSec

CLI Add-On Template

Policy

在推送模板之前，您可以驗證配置差異。

新ACL配置

```

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

```

應用於線路vty的ACL

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	!

驗證

現在，您可以使用此路徑：**Menu > Tools > SSH Terminal**，再次使用之前的vManage過濾器測試cEdge的SSH訪問。

路由器嘗試通過SSH連線到192.168.10.114m

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

Router#
```

如果檢查ACL計數器，可以確認Seq 30有1個匹配項，並且SSH連線被拒絕。

```
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)
```

相關資訊

[Cisco SD-WAN策略配置指南，Cisco IOS XE版本17.x](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。