

SSH 액세스를 제한하도록 SD-WAN cEdge 라우터 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[토폴로지](#)

[SSH 액세스 제한 절차](#)

[연결 확인](#)

[액세스 제어 목록 검증](#)

[액세스 제어 목록 컨피그레이션](#)

[vManage GUI의 컨피그레이션](#)

[확인](#)

[관련 정보](#)

[Cisco SD-WAN 정책 컨피그레이션 가이드, Cisco IOS XE 릴리스 17.x](#)

소개

이 문서에서는 Cisco IOS-XE® SD-WAN 라우터에 대한 SSH(Secure Shell) 연결을 제한하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

적절한 테스트를 수행하려면 vManage와 cEdge 간의 컨트롤 연결이 필요합니다.

사용되는 구성 요소

이 절차는 Cisco Edge 또는 vManage 디바이스의 소프트웨어 릴리스로 제한되지 않으므로 모든 릴리스를 이 단계에 사용할 수 있습니다. 그러나 이 문서는 cEdge 라우터에서만 제공됩니다. 구성하려면 다음이 필요합니다.

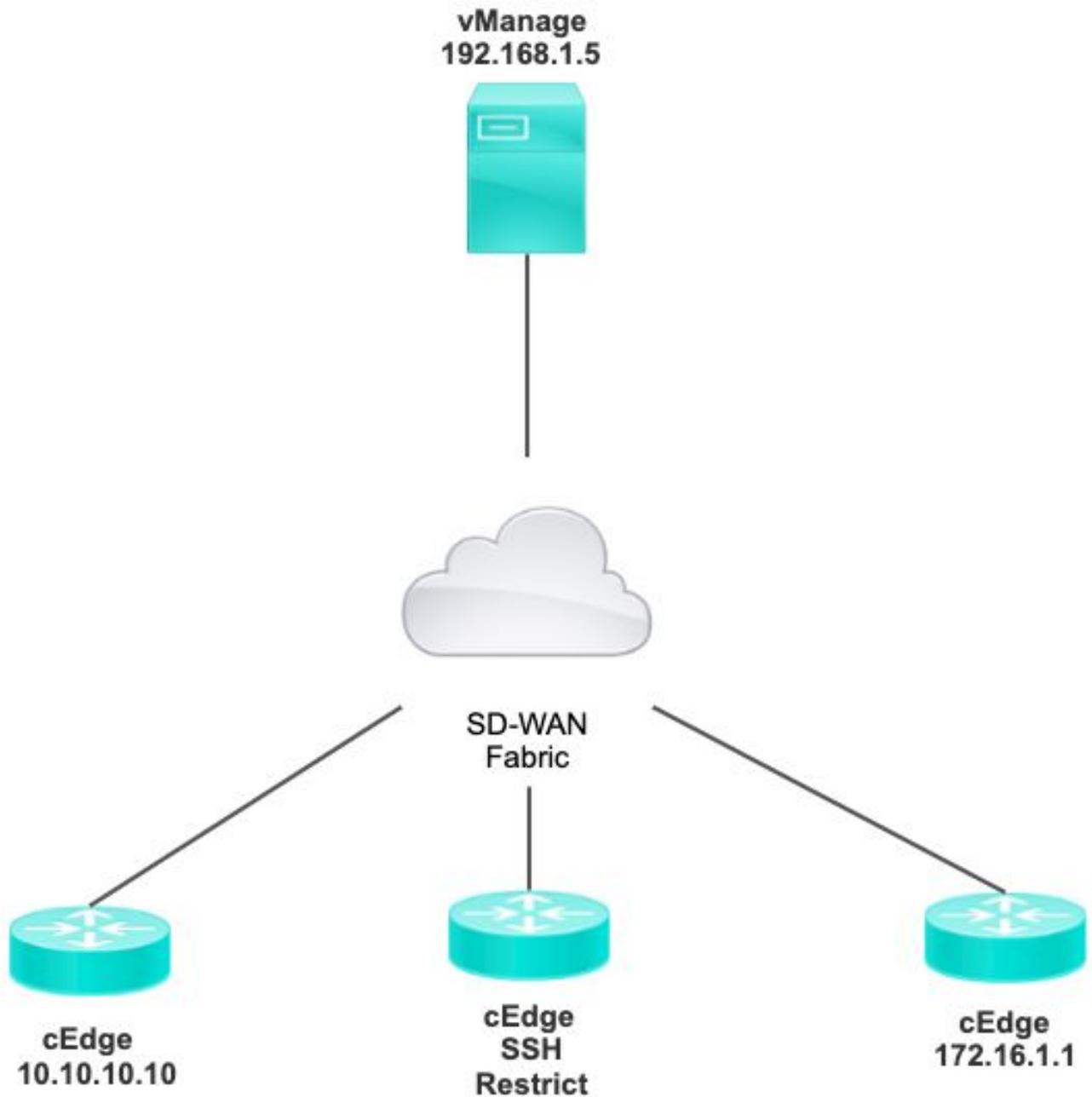
- Cisco cEdge 라우터(가상 또는 물리적)
- Cisco vManage

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 데모의 목적은 cEdge 172.16.1.1에서 SSH 액세스를 제한하지만 cEdge 10.10.10.10 및 vManage를 허용하도록 cEdge의 컨피그레이션을 표시하는 것입니다.

토폴로지



SSH 액세스 제한 절차

연결 확인

cEdge 라우터가 vManage에 연결할 수 있는지 확인하려면 연결을 확인해야 합니다. 기본적으로 vManage는 IP 192.168.1.5를 사용하여 cEdge 디바이스에 로그인합니다.

vManage GUI에서 cEdge에 대한 SSH를 열고 연결된 IP에 다음 출력이 있는지 확인합니다.

```
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

vManage에서 cEdge에 로그인하는 데 터널, 시스템 또는 공용 ip 주소를 사용하지 않는지 확인합니다.

cEdge에 로그인하는 데 사용되는 IP를 확인하려면 다음 access-list를 사용할 수 있습니다.

```
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.
```

액세스 제어 목록 검증

VTY 라인에 적용된 액세스 목록

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

ACL이 적용된 후 vManage에서 cEdge로 SSH를 다시 열고 로그에 생성된 다음 메시지를 확인할 수 있습니다.

이 메시지는 show logging 명령을 통해 확인할 수 있습니다.

```
*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
```

이전 로그에서 Local port 22를 볼 수 있습니다. 이는 192.168.1.5에서 cEdge에 대한 SSH를 열려고 시도했음을 의미합니다.

소스 IP가 192.168.1.5임을 확인했으므로 vManage에서 SSH 세션을 열 수 있도록 올바른 IP로 ACL을 구성할 수 있습니다.

액세스 제어 목록 컨피그레이션

cEdge에 여러 시퀀스가 있는 경우 ACL의 맨 위에 새 시퀀스를 추가해야 합니다.

공격 전:

```
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
```

컨피그레이션 예시:

```
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.
```

새 시퀀스:

```
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
```

VTY 라인에 ACL을 적용합니다.

```
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 GUI의 컨피그레이션

cEdge 디바이스에 템플릿이 연결된 경우 다음 절차를 사용할 수 있습니다.

1단계. ACL을 생성합니다

Configuration(컨피그레이션) > Custom Options(맞춤형 옵션) > Access Control List(액세스 제어 목록) > Add Device Access Policy(디바이스 액세스 정책 추가) > Add ipv4 Device Access Policy(ipv4 디바이스 액세스 정책 추가)로 이동합니다

ACL의 이름과 설명을 추가하고 Add ACL Sequence(ACL 시퀀스 추가)를 클릭한 다음 Sequence Rule(시퀀스 규칙)을 선택합니다

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

Device Access Protocol > SSH를 선택합니다

그런 다음 소스 데이터 접두사 목록을 선택합니다.

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	

Actions(작업)를 클릭하고 Accept(수락)를 선택한 다음 Save Match And Actions.

마지막으로, 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 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

2단계. 지역화된 정책 생성

Configuration(컨피그레이션) > Localized Policy(현지화된 정책) > Add Policy(정책 추가) > Configure Access Control List(액세스 제어 목록 구성) > Add Device Access Policy(디바이스 액세스 정책 추가) > Import Existing(기존 가져오기)으로 이동합니다.

Localized Policy > Add Policy

Create Groups of Interest
 Configure Forwarding Classes/QoS
 Configure Access Control Lists

Search

Add Access Control List Policy v Add Device Access Policy v (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				

이전 ACL을 선택하고 Import(가져오기)를 클릭합니다.

x

Import Existing Device Access Control List Policy

Policy SDWAN_CEDGE_ACCESS

Cancel Import

Policy Name(정책 이름) 및 Policy Description(정책 설명)을 추가하고 Save Policy Changes.

Policy Overview Forwarding Class/QoS Access Control Lists Route Policy

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) ⓘ

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

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

Preview Save Policy Changes Cancel

3단계. 장치 템플릿에 현지화된 정책 첨부

Configuration(컨피그레이션) > Template(템플릿) > Device(디바이스) > Select the Device(디바이스 선택)로 이동하고 >> ... > Edit(편집) > Additional Templates(추가 템플릿) > Policy(정책) > SDWAN_CEDGE > Update(업데이트)를 클릭합니다.

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

템플릿을 푸시하기 전에 컨피그레이션 차이를 확인할 수 있습니다.

새 ACL 컨피그레이션

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	!

ACL이 라인 vty에 적용됨

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

확인

이제 vManage의 이전 필터를 사용하여 cEdge에 대한 SSH 액세스를 다시 테스트할 수 있습니다 (Menu(메뉴) > Tools(툴) > SSH Terminal(SSH 터미널)).

라우터가 192.168.10.114에 대한 SSH를 시도했습니다.

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

Router#
```

ACL 카운터를 확인할 경우 시퀀스 30에 1개의 일치가 있고 SSH 연결이 거부되었음을 확인할 수 있습니다.

```
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)
```

관련 정보

[Cisco SD-WAN 정책 컨피그레이션 가이드, Cisco IOS XE 릴리스 17.x](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.