

لوصو دييقتل SD-WAN cEdge هجوم نيوكت SSH

تايوتحمل

[عمدقمل](#)

[ةيساسأل تابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[ةيساسأ تامولعم](#)

[طاطخمل](#)

[SSH لوصول دييقت عارج](#)

[لاصتال نم ققحتل](#)

[لوصولاب مكحتل ةمئاق ةحص نم ققحتل](#)

[لوصولاب مكحتل ةمئاق نيوكت](#)

[vManage ةيموسرل مدختسمل ةهجاو لعل نيوكت](#)

[ققحتل](#)

[قلص تاذا تامولعم](#)

[17.x رادصل، Cisco SD-WAN، Cisco IOS XE، تاسايس نيوكت ليلد](#)

عمدقمل

Cisco IOS-XE® SD-WAN هجوم ب (SSH) نامأل ةقبط لاصتا دييقت ةيلمع دنتسمل اذه فصوي WAN.

ةيساسأل تابلطتمل

تابلطتمل

ةبسانمل تارابتخال عارجال cEdge و vManage ني ب مكحتل لاصتا رفوت مزلي

عمدختسمل تانوكمل

نكمي يلاتلابو، vManage و Cisco Edge ةزهجا ي جم انرب رادصل ي لعل عارجال اذه رصتقي ال cEdge تاهجوم ب صاخ دنتسمل اذه نإف، كلذ عم و. تاوطخل هذه عم تارادصلال عيمج مادختسإ يلي ام مزلي، نيوكتلل:

- (ي دام و يرهاظ) Cisco cEdge هجوم
- جم انرب Cisco vManage

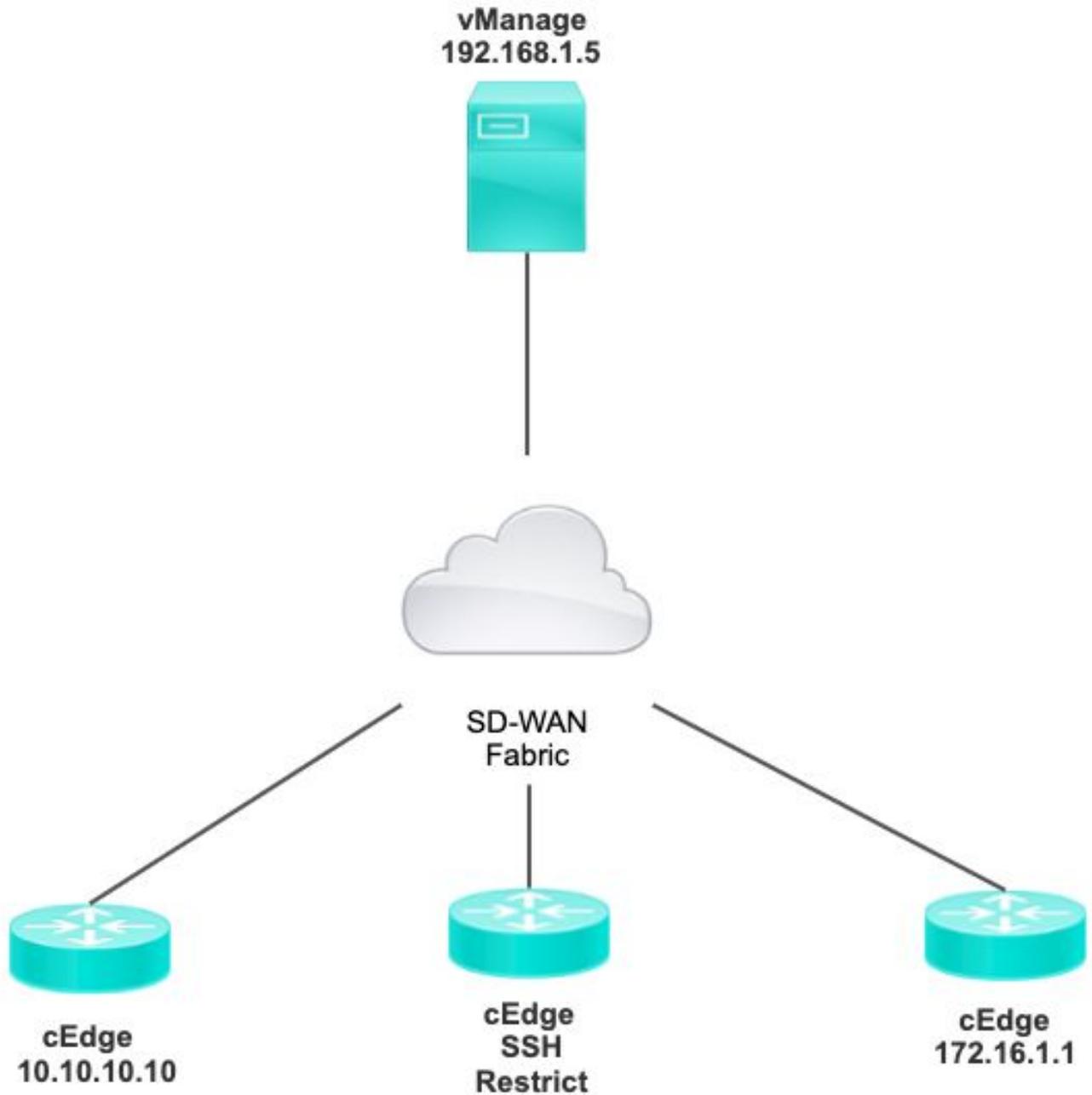
ةصاخ ةيلمعم ةئيب ي ةدوجومل ةزهجال نم دنتسمل اذه ي ةدراول تامولعمل عاشنإ م تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي عمدختسمل ةزهجال عيمج تادب

رمأ يأل لم تحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديقتك بش

ةيساسأ تامولعم

SSH لوصو ديقتل cEdge ىلع دوجوملا نيوكتلا ضرع وه يحيضوتلا ضرعلا اذه نم ضرغلا vManage و cEdge 10.10.10.10 ل حامسلا عم نكلو cEdge 172.16.1.1 نم

ططخملا



SSH ىلا لوصولا ديقت ءارجا

لاصتالال نم ققحتال

ىل cEdge هجوم لوصو ةي ناكم ا ةحص نم ققحتال ل لاصتالال نم ققحتالال مزلي ةزهجأ ىل ل لوخدال ليجستل IP 192.168.1.5 vManage مدختسي، يضارتفا لكش ب vManage. cEdge.

لوكوتورب نأ نم دكأتو cEdge ىل SSH حتفا، vManage ةي موسرلا مدختس مالا ةهجاو نم يلاتال جارخالال ىل ع يوتحي هلي صوت مت يذالال تنرتنالال:

```
<#root>
```

```
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

ىل ل لوخدال ليجستل ماعال IP ناو نع وأ ماظنالال وأ قفنلال مدختسي ال vManage نأ نم دكأت cEdge.

لوصولال ةمئاق مادختس ا كنكمي، cEdge ىل ل لوخدال ليجستل همادختس ا متي يذالال IP دي كأتال ةي لالال.

```
<#root>
```

```
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

لوصولال م كحتالال ةمئاق ةحص نم ققحتالال

طخ ىل ع ةق ب طملا لوصولال ةمئاق

```
<#root>
```

```
cEdge#
```

```
show sdwan running-config | section vty
```

```
line vty 0 4
```

```
access-class VTY_FILTER_SSH in vrf-also
transport input ssh
```

على vManage من ىرخ أةرم SSH حتف كنىمى (ACL) لوصول فى مكحتل ةمئاق قىببط دعب
تالجلسل ىلع اهؤاشنإ مت ىتلا ةىلاتلا ةلاسرلا ةىورو cEdge.

رمألا مادختساب ةلاسرلا هذة ةىورنىمى: show logging.

```
*Jul 13 15:05:47.781: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Tadmin] [Source: 192.168.1.5] [1
```

192.168.1.5 رادصلال أنىنعى اذهو. 22 ءانىم ىلحم تىأر عىطتسى تنأ، قىباسلال لجلسلال ىلع
cEdge ىلع SSH حتف لواح.

لوصول فى مكحتل ةمئاق نىوكت كنىمى، 192.168.1.5 وه IP ردىم أنأ تدكأنأ دعب نألا
SSH ةسلج حتف ىلع ةردقلااب vManage ل حامسلل لىحصلال IP مادختساب.

لوصول فى مكحتل ةمئاق نىوكت

ةمئاق ىلعأ فى دىدل لسلستلا ةفاصلإنم دكأتف، ةددعتم تالسلست cEdge ل ناك اذإ
(ACL) لوصول فى مكحتل.

لبق:

```
<#root>
```

```
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
```

نىوكتلا لاثم:

```
<#root>
```

```
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.

ديج لس لس ت:

```
<#root>
```

```
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
```

vtv طخ ىلع (ACL) لوصول في مكحتل ةمئاق قي بطت

```
<#root>
```

```
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 ةموسرلا مدختس ملة ةهجاو ىلع نيوكتل

يلال ءارجلال مادختس ل كنكمي، قفرم بلال cEdge زاهج ىدل ناك اذا

(ACL) لوصول في مكحتل ةمئاق ءاشن 1. ةوطخل

ةسايس ةفاض | > لوصول في مكحتل ةمئاق > ةصصخم تاراخي > نيوكتل ىل لقتنا
IPv4 ةزهجأ ىل لوصول ةسايس ةفاض | > ةزهجأ ىل لوصول

لس لس ةفاض قوف رقن او هفصوو (ACL) لوصول في مكحتل ةمئاق مسا ةفاض اب مق
لس لس ةفاض قوف رقن او هفصوو (ACL) لوصول في مكحتل ةمئاق

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

SSH > زاھجلا ىلا لوصول لوك وورب ددح
ردصملا تانايبلا تائداب ةمئاق ددح مث

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	

Save Match And Actions. رقنا مث ، لوبق ددح ، تاي لمع رقنا

Save Device Access Control List Policy. راتخت نأ ك نكمي ، اريخأ

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

محرتم جهن عاشن | 2. ةوطخل

> لوصولا يف مكحتلا ةمئاق نيوكت > ةسايس ةفاض | > محرتم جهن > نيوكتلا لىل لقتنا
> دوجوملا داريتس | > زاهجلا لىل لوصولا ةسايس ةفاض |

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				

داريتس | قوف رقناو ةقباسلا (ACL) لوصولا يف مكحتلا ةمئاق دح

Import Existing Device Access Control List Policy



Policy

SDWAN_CEDGE_ACCESS

Cancel

Import

Save Policy Changes. قوف رقنا مٲ جهنلا فصوو جهنلا مسا ةفاضاب مق

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

زاهجلا بللق مٲ جهنلا قافرا 3 ةوطخلا

> ةفاضاب لاق > ررحت > ... > قوف رقناو زاهجلا ددحت > زاهج > بللق > نيوكت للاق لقتنا
> SDWAN_CEDGE > ةسايس

Device

Feature

Basic Information

Transport & Management VPN

Service VPN

Cellular

Additional Templates

TrustSec

Choose...

CLI Add-On Template

Choose...

Policy

SDWAN_CEDGE

نيوكتلا فالتخاً نم ققحتلا كنكمي، بلالال لىل ع طغضلاب موقت نأ لب ق

ةديجالا (ACL) لوصولاي ف مكحتلا ةمئاق نيوك

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 طخ لىل ع قق ب ط م

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	.

ققحتلا

نم قق ب اسلا ةي فصتلا لم اوع مادختساب cEdge لىل SSH لوصولاي رابتخا رخأ ةرم كنكمي نألا SSH ةي فرطلا ةدحولا > تاودأ > ةمئاقلا: راسملا اذه مادختساب vManage.

SSH لىل 192.168.10.114 عم هجوملا ةلواجم تمت

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

Router#
```

يوتحي Seq 30 نأ ديكات كنكمي، لوصولاي ف مكحتلا ةمئاق تاداع نم ققحتلاب تمق اذا SSH لاصتا ضفر مت ودحاو قباطت لىل ع

```
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)
```

ةلص تاذا تامولعم

[17.x رادصلال، Cisco SD-WAN، Cisco IOS XE، تاسايس نيوكت ليلد](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل چ ن ا ل ا دن ت س م ل ا