

ىلע عقوم ىلإ عقوم نم VPN ۆكپش نیوکت
نم ۆرادملاتانایپلا ۆھجاو FDM

تایوتیم

مددة

ملا طباطبائی اس سوچ

تامل طتملا

ةمدختس ملأ تانوكمل

ةي س، اس، أ تامولع

نیوکرک

تائیوکتلا

للانم قيقحتلا

احالص او عاطل افasherكتسرا

معلومات اذتاذ

ةمدقملا

ةيسيس ألا تابلطت ملأ

- عيضاً وملأ هذه الأسئلة:
 - ةزهجأ ريدم لبقة نم ۀرادمل Cisco نم FirePOWER (FTD) ديدهت دض عافدلا FirePOWER (FDM).
 - نم (ASA) ۀلدعممل ناماًلا ةزهجأ Cisco.
 - طيسبلاتاكبشلا ۀرادإ لوكوتورب (SNMP).
 - ةيرهاظللا ظصالخلا ۀكبشلا (VPN).
 - FTD و ASA ۀزهجأ ىلإ ۀرادإ لوصولـا.
 - رمأ يأـل لمـتحـملـا رـيـثـأتـلـا مـهـفـتـو ۀـرـشـ، اـبـمـ كـتـكـبـشـ نـأـ نـمـ دـكـأـتـ.

تالیف ملک

ةمـدـخـتـسـمـلـا تـانـوـكـمـلـا

ةـيـلـاتـلـا ةـيـدـامـلـا تـانـوـكـمـلـا وجـمـارـبـلـا تـارـادـصـا ئـلـا دـنـتـسـمـلـا اـذـه يـف ةـدـرـاـوـلـا تـامـوـلـعـمـلـا دـنـتـسـتـ

- Cisco Firepower Threat Defense (FTD) FirePOWER Device Manager (FDM)، رادص إلأ 7.2.7.
- Cisco Adaptive Security Appliance (ASA)، 9.1.6.
- SNMP مـدـاخـجـمـانـرـبـيـا (سـاـيـقـ)

ةـصـاخـ ةـيـلـمـعـمـ ةـيـيـبـ يـف ةـدـوـجـوـمـلـا ةـزـهـجـأـلـا نـم دـنـتـسـمـلـا اـذـه يـف ةـدـرـاـوـلـا تـامـوـلـعـمـلـا عـاـشـنـا مـتـ
تنـاـكـ اـذـاـ. (يـصـارـتـفـاـ) حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـا اـذـه يـف ةـمـدـخـتـسـمـلـا ةـزـهـجـأـلـا عـيـمـجـ تـأـبـ
رمـأـ يـأـلـ لـمـتـحـمـلـا رـيـثـأـتـلـلـ كـمـهـفـ نـم دـكـأـتـفـ، لـيـغـشـتـلـا دـيـقـ كـتـكـبـشـ.

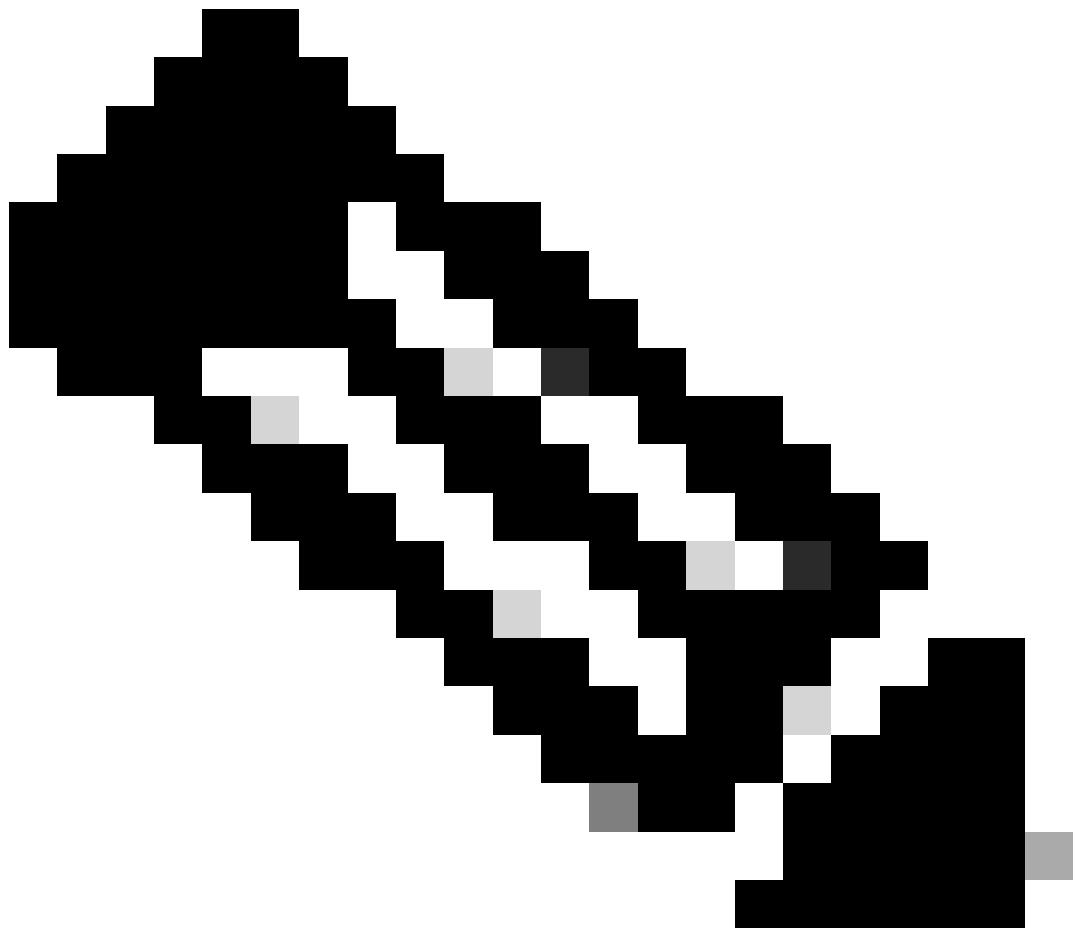
ةـيـسـاسـأـ تـامـوـلـعـمـ

مـهـبـ صـاخـلـا ةـكـبـشـلـا زـاهـجـ ةـبـقـارـمـ نـاـمـضـ ةـكـبـشـلـا يـلـوـؤـسـمـلـا، تـاوـطـخـلـا هـذـهـ حـيـضـوـتـ عـمـوـ
دعـبـ نـعـ.

اـذـهـ يـفـ. اـهـتـبـقـارـمـ وـةـكـبـشـلـا ةـرـاـدـاـلـ (طـيـسـبـلـا ةـكـبـشـلـا ةـرـاـدـاـلـ لـوـكـوـتـورـبـ) مـاـدـخـتـسـاـ مـتـيـ
نـمـ VPN ةـكـبـشـلـا لـالـخـ نـمـ دـيـعـبـ SNMP مـدـاخـلـا FTD نـمـ SNMP رـوـرـمـ ةـكـرـحـ لـاـسـرـاـ مـتـيـ، دـادـعـإـلـاـ
مـاـدـخـتـسـاـبـ اـهـؤـاشـنـاـ مـتـ عـقـوـمـ يـلـاـ عـقـوـمـ ASA.

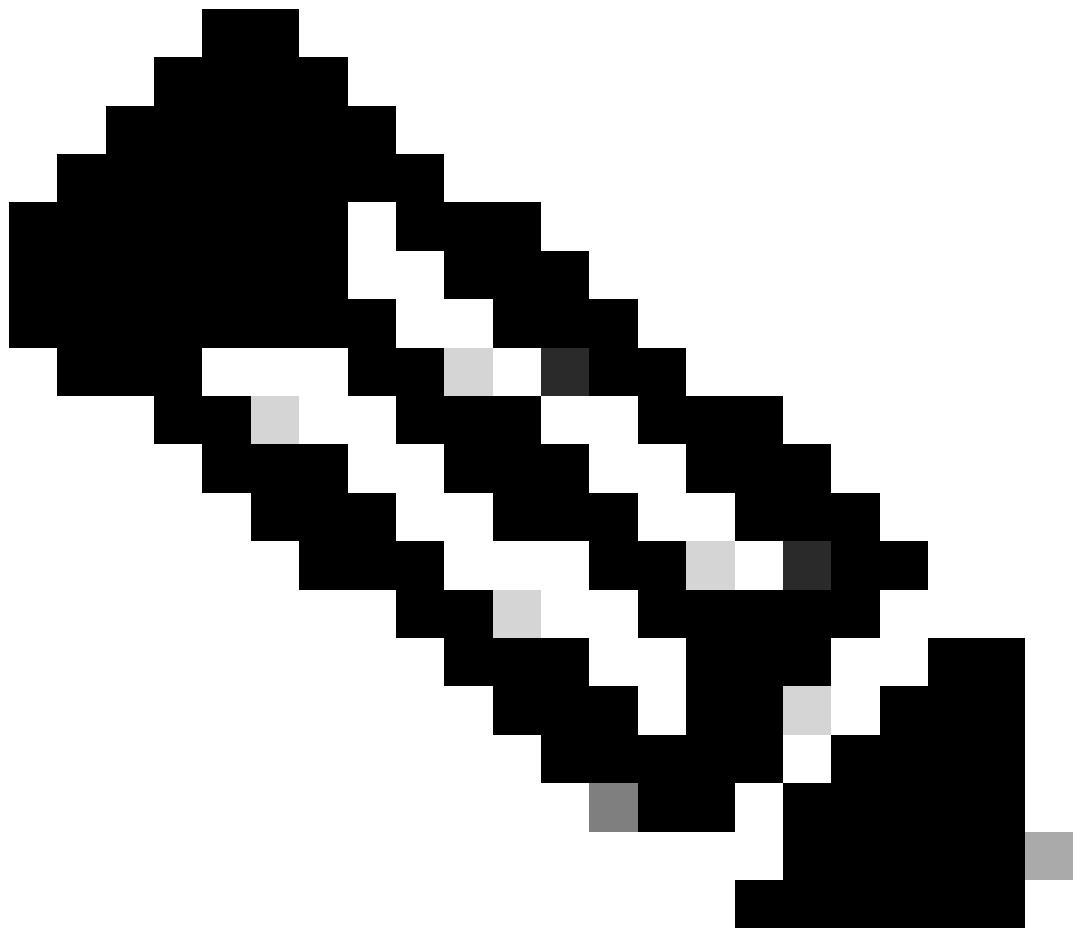
لـالـخـ نـمـ دـيـعـبـ فـرـطـ يـلـاـ SNMP نـيـوـكـتـلـا يـلـوـؤـسـمـ ةـدـعـاـسـمـ يـلـاـ لـيـلـدـلـاـ اـذـهـ فـدـهـيـ
ةـبـقـارـمـلـ اـدـيـفـمـ دـادـعـإـلـاـ اـذـهـ دـعـيـ. زـاهـجـلـ تـانـاـيـبـ ةـهـجـاـوـ يـلـعـ عـقـوـمـ يـلـاـ عـقـوـمـ نـمـ VPN ةـكـبـشـ
لـاـسـرـاـ مـتـيـوـ v2 SNMP لـوـكـوـتـورـبـ مـاـدـخـتـسـاـ مـتـيـ، دـادـعـإـلـاـ اـذـهـ يـفـ. دـعـبـ نـعـ اـهـتـرـاـدـاـوـ ةـكـبـشـلـا ةـزـهـجـأـ
نـمـ VPN ةـكـبـشـلـا لـالـخـ نـمـ دـيـعـبـ SNMP مـدـاخـلـا FTD تـانـاـيـبـ ةـهـجـاـوـ نـمـ SNMP تـانـاـيـبـ رـوـرـمـ ةـكـرـحـ
مـاـدـخـتـسـاـبـ اـهـؤـاشـنـاـ مـتـ عـقـوـمـ يـلـاـ عـقـوـمـ ASA.

عـاـونـأـ يـلـعـ نـيـوـكـتـلـاـ اـذـهـ قـيـبـطـتـ نـكـمـيـ نـكـلـوـ، "لـخـاـدـلـا" مـسـاـ ةـمـدـخـتـسـمـلـا ةـهـجـاـوـلـاـ يـلـعـ قـلـطـيـوـ
يـتـلـاـ ةـهـجـاـوـلـاـ تـسـيـلـ ةـيـاـمـحـلـاـ رـاـدـجـلـ ةـهـجـاـوـيـأـ مـدـخـتـسـيـ نـأـ نـكـمـيـوـ "عـبـرـمـلـاـ يـلـاـ" رـوـرـمـ ةـكـرـحـ نـمـ يـرـخـأـ
(VPN).



دنس REST تاقيب طت ةجمرب هجأو رب عالا SNMP لوكوت ورب نيكوت نكمي عال : ظحالم ةطس او ب هترادا متت امك ، ثدح عالا تارادص عالا او 6.7 رادص عالا FDM. ليغشت

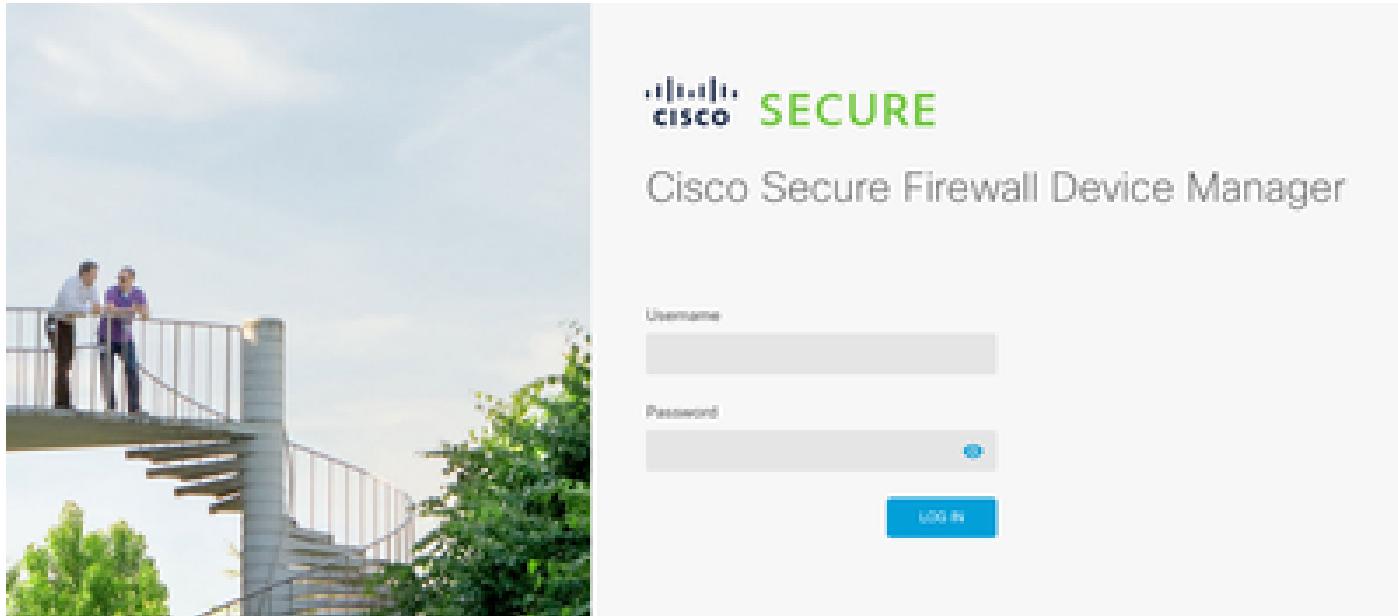
نيوكتل



ةزهجألا نيب لعفلاب نوكم VPN عقوم ىلإ عقوملا نأ نيوكتل اذه ربتعي :ةظحالم
صحفا VPN عقوم ىلإ عقوملا نيوكت ئيفيك لوح ئيفاضا ليصافت ىلع لوصحلل
ةطساوب ۋارادملار FTD ىلع عقوم ىلإ عقوم نم [VPN ۋېب شەنى يوكت](#). نيوكتل الىد
[FDM](#)

تانيوكتلار

1. كېنارلاردا FTD ىلإ لوط دىلا لجس.



2. تاقيب طتلـا ةـجـمـرـب ةـهـجـاو فـشـكـتـسـمـ ىـلـا لـقـتـنـا زـاهـجـلـا ىـلـع ـمـاع ـرـظنـنـ تـحـتـ.

A screenshot of the API Explorer interface. At the top, there are five circular icons with symbols: a right arrow, a download, a checkmark, a question mark, and three dots. To the right, it shows a user session for "admin" (Administrator). Below this, there's a section for "services" with tabs for "Registered" (highlighted) and "Register", and another for "Not Configured". In the center, there's a "API Explorer" section with a gear icon and an "API" label. To the right, there's a "CONFIGURE" button with a question mark icon. The background has a light blue gradient.

3. SNMPv2 ىـلـع FTD

- ةـهـجـاوـلا تـامـوـلـعـمـ ىـلـعـ لـصـحـاـ.

A screenshot of the Interface API endpoint details. It shows a "GET" method and the URL "/devices/default/interfaces". The background has a light blue gradient.

4. مـوقـتـ .تاـقيـبـ طـتـلـا ةـجـمـرـبـ ةـهـجـاوـ ءـاعـدـتـسـاـ ءـارـجـالـ إـكـلـذـ ةـبـرـجـتـ رـزـلـاـ دـدـحـوـ لـفـسـأـلـ رـيـرـمـتـلـاـبـ مـقـ

[TRY IT OUT!](#)[Hide Response](#)

Curl

```
curl -X GET --header 'Accept: application/json' 'https://192.168.1.1/api/fdm/v6/devices/default/interfaces/inside'
```

Request URL

https://192.168.1.1/api/fdm/v6/devices/default/interfaces/inside

Response Body

```
{
  "version": "mqjiiipiswsgsx",
  "name": "inside",
  "description": null,
  "hardwareName": "GigabitEthernet0/1",
  "monitorInterface": false,
  "ipv4": {
    "ipType": "STATIC",
    "defaultRouteUsingDHCP": false,
    "dhcpRouteMetric": null,
    "ipAddress": {
      "ipAddress": "10.57.58.1",
      "netmask": "255.255.255.0",
      "standbyIpAddress": null,
      "type": "haipv4address"
    },
    "dhcp": false,
    "addressNull": false,
    "type": "interfaceipv4"
  }
}
```

Response Code

200

- فیضمل ةكبش نئاک نیوکت عاشناب مق SNMP.

NetworkObject

GET

/object/networks

POST

/object/networks

- دیدج SNMPv2c فیضم نئاک عاشنایا.

SNMP

GET	/devicesettings/default/snmpservers
GET	/devicesettings/default/snmpservers/{objId}
PUT	/devicesettings/default/snmpservers/{objId}
GET	/object/snmpusers
POST	/object/snmpusers
DELETE	/object/snmpusers/{objId}
GET	/object/snmpusers/{objId}
PUT	/object/snmpusers/{objId}
GET	/object/snmpusergroups
POST	/object/snmpusergroups
DELETE	/object/snmpusergroups/{objId}
GET	/object/snmpusergroups/{objId}
PUT	/object/snmpusergroups/{objId}
GET	/object/snmphosts
POST	/object/snmphosts
DELETE	/object/snmphosts/{objId}
GET	/object/snmphosts/{objId}
PUT	/object/snmphosts/{objId}

فاشكتس او SNMP لوكوتورب نيوكتب مق ،نيوكتلا ليلد نم ققحت ،ليصافتلا نم ديزمل
FirePOWER FDM ايلع امحالص او هئاطخأ

مدقتملـا نـيوكتـلا مـسـق يـف زـاهـجـلـا إـلـا لـقـتـنـا ،زـاهـجـلـا إـلـعـ SNMP لـوكـوتـورـبـ نـيوـكـتـ درـجـمـبـ .
نيـوـكـتـلا ضـرـعـ دـدـحـ وـ.

Advanced Configuration

Includes: FlexConfig, Smart CLI

[View Configuration](#)



هتيمستب مق، ديدج نئاك عاشناب مقو FlexConfig تانئاك ددح، FlexConfig مسق يف. عزج يف رمألا عاغلإا فضأو ةهجاولأا ددحو، بلاقلا مسق يف management-access رمألا ةفاضأو بلاقلا ضفر.

FlexConfig

FlexConfig Objects

FlexConfig Policy

Edit FlexConfig Object



Name

Description

This command gives mgmt access to the Inside Interface



Variables

There are no variables yet.

Start with adding a new variable.

ADD VARIABLE

Template

Expand Reset

1	management-access Inside
---	--------------------------

Negate Template

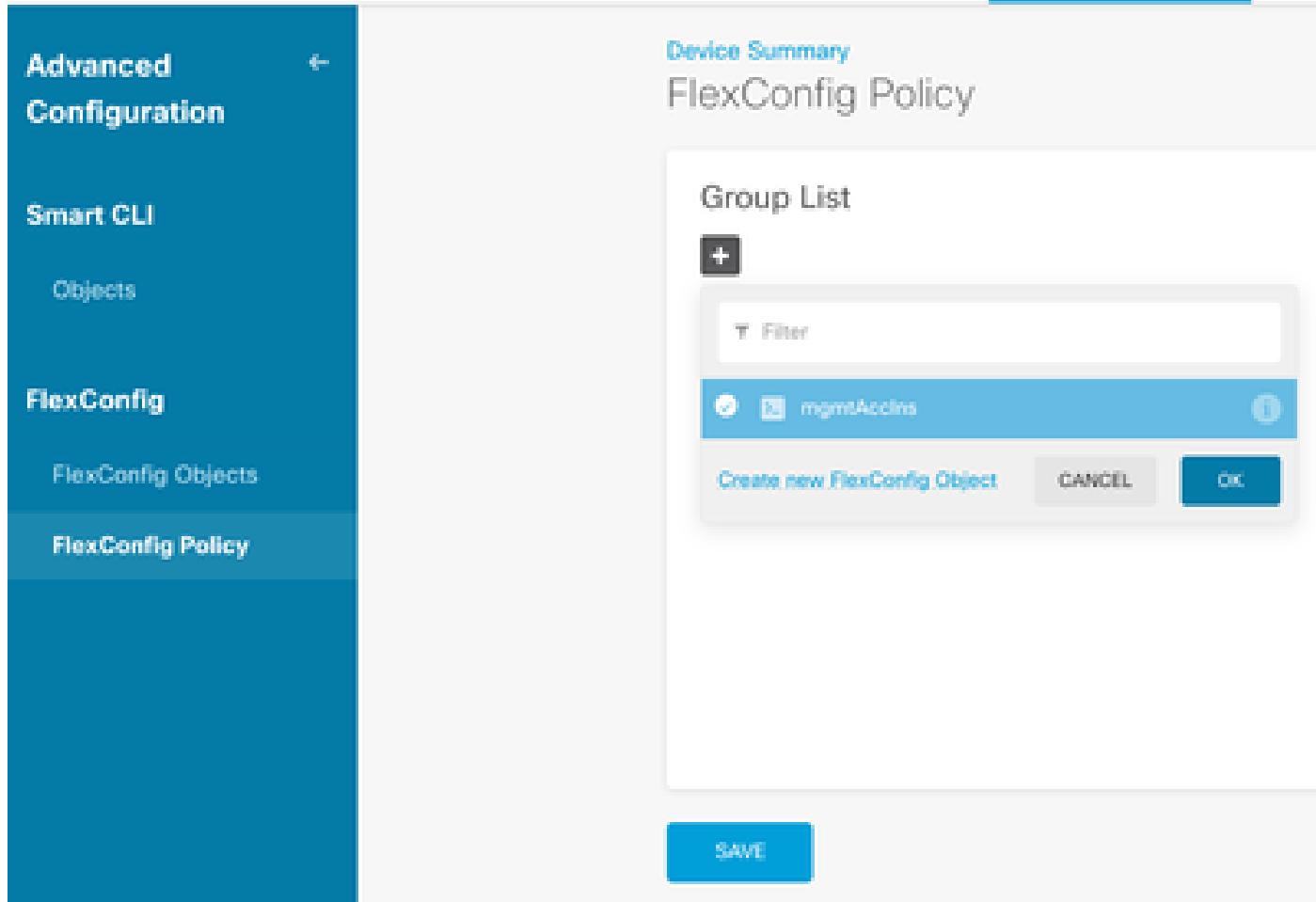
Expand Reset

1	no management-access Inside
---	-----------------------------

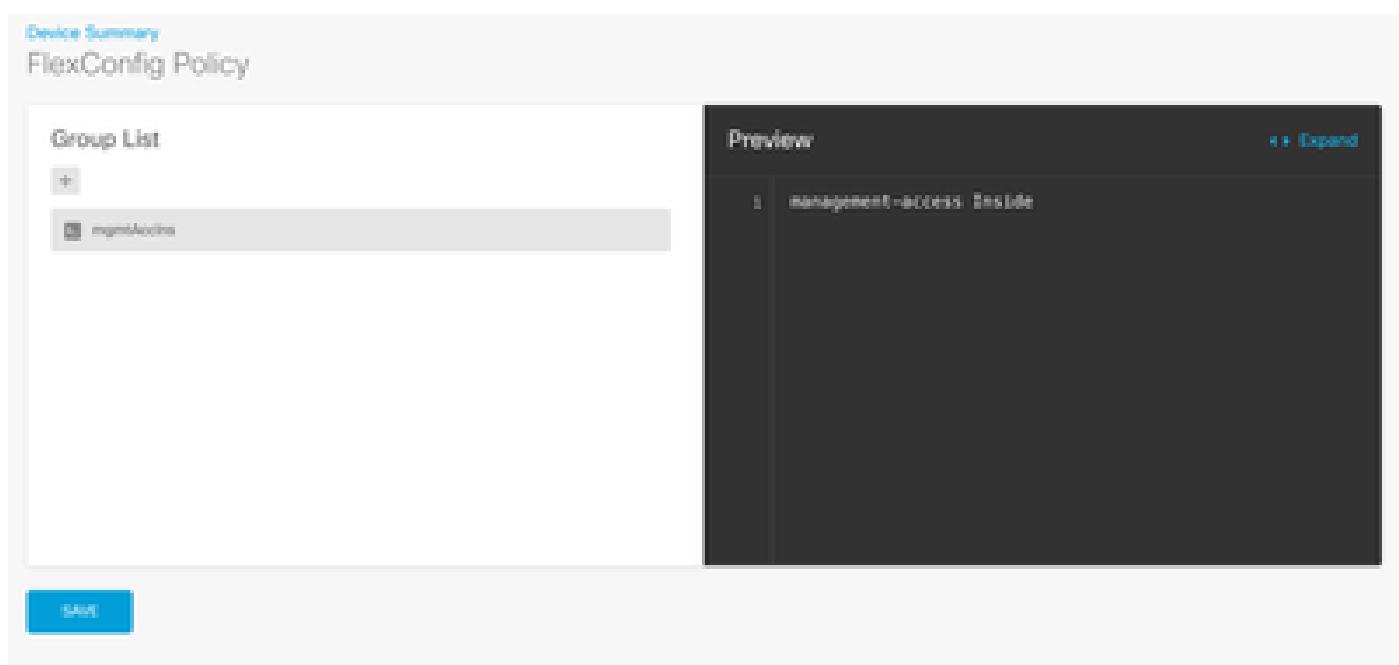
CANCEL

OK

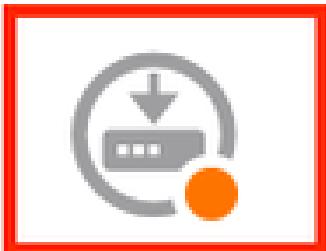
نئاك ددحو ةفاضالا ٓنوقيأ ىلع رقنا، ئاسيس ددح، ئاسيس FlexConfig، ئاسيس FlexConfig، مسق يف FlexConfig ددحو ةقباسلا ٓوطخلا يف هانأشنأ يذلا قفاوم.



8. ظفح ددح زاهجلا ىلع اهقيبطة متييس يتلا رماوألل ۋەنیاعم رەھەت، كىلذ دعب.



9. نآلا "رشن" قوف رقنا او رشنلار زمر ددح مىث، نىوكتىلا رشنب مۇق.



Pending Changes



- Last Deployment Completed Successfully
15 Oct 2024 08:06 PM. [See Deployment History](#)

Deployed Version (15 Oct 2024 08:06 PM)

Pending Version

LEGEND

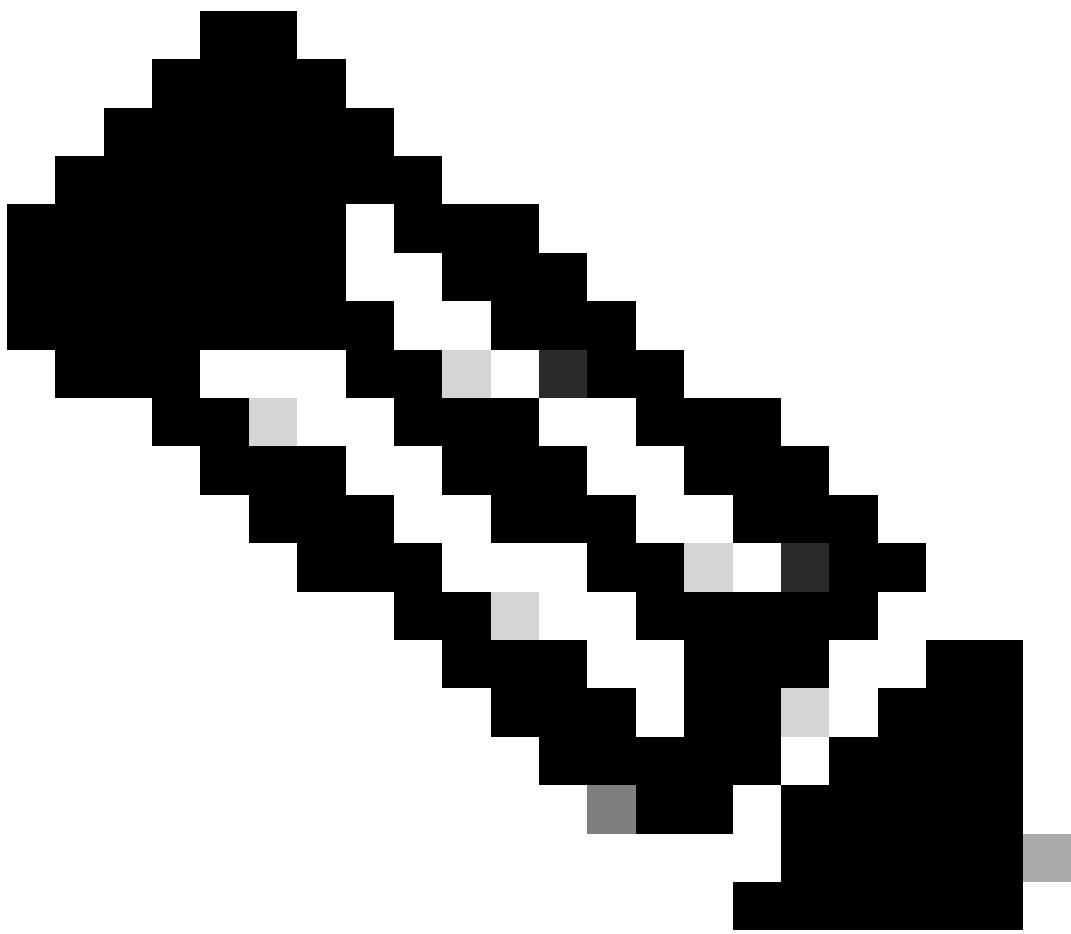
- FlexConfig Policy Edited: default-group

MORE ACTIONS ▾

CANCEL

DEPLOY NOW





كـل ذـيـكـأـتـلـ مـاهـمـلـا ظـمـئـاقـ نـمـ قـقـحـتـلـاـ كـنـكـمـيـ ،ـضـرـمـ لـكـشـبـ هـلـامـكـاـ نـمـ دـكـأـتـ :ـةـظـحـالـمـ

ةـحـصـلـاـ نـمـ قـقـحـتـلـاـ

ةـدـحـوـ وـأـ SSHـ رـبـعـ FTDـ ىـلـاـ لـوـخـدـلـاـ لـجـسـوـ ،ـتـارـابـتـخـالـاـ هـذـهـ عـارـجـاـبـ مـقـ ،ـنـيـوـكـتـلـاـ نـمـ قـقـحـتـلـلـ رـمـأـوـأـلـاـ هـذـهـ لـيـغـشـتـبـ مـقـ مـثـ ،ـمـكـحـتـلـاـ:

• اـهـانـيـرجـأـ يـتـلـاـ تـارـيـيـغـتـلـاـ ىـلـعـ يـوـتـحـيـ زـاهـجـلـلـ هـلـيـغـشـتـ يـرـاجـلـاـ نـيـوـكـتـلـاـ نـأـ نـمـ قـقـحـتـ.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password:
firepower# show running-config
<some outputs are omitted>
object network snmpHost
host 10.56.58.10
```

```

<some outputs are omitted>
snmp-server host inside 10.56.58.10 community ***** version 2c
snmp-server location null
snmp-server contact null
snmp-server community *****
<some outputs are omitted>
management-access inside

```

- حاجن ب هلامك! نم دكأت و SNMP رب تخم نم رابتخا عاجاب مق.

The screenshot shows the "Run Test" configuration window with the "Start" button highlighted. Below it is the log output from the test run:

```

Paessler SNMP Tester - 20.2.4 Computername: WHN10 Interface: 10.56.58.10
10/16/2024 1:19:08 PM (1 ms) : Device: 10.57.58.1
10/16/2024 1:19:08 PM (3 ms) : SNMP v3c
10/16/2024 1:19:08 PM (5 ms) : Uptime
10/16/2024 1:19:08 PM (47 ms) : SNMP Datatype: ASN_UTIMETicks
10/16/2024 1:19:08 PM (49 ms) : -----
10/16/2024 1:19:08 PM (51 ms) : DISMAN-EVENT-MIB::sysUpTimeInstance = 15632700 ( 43 hours 25 minutes )
10/16/2024 1:19:08 PM (118 ms) : SNMP Datatype: SNMP__EXCEPTION_NOSUCHOBJECT
10/16/2024 1:19:08 PM (120 ms) : HOST-RESOURCES-MIB::hrSystemUptime.0 = IN SNMP__EXCEPTION_NOSUCHOBJECT222 ( 0 seconds )
10/16/2024 1:19:08 PM (122 ms) : Done

```

اهحالص او عاطخألا فاشكتسا

:ةيلاتلا تاوطلخا يف لمأت ف ،لكاشم يأ تهج او اذا

- قفن نم ققحتلل رمألا اذه ليغشت كنكمي ،هليغشت و VPN قفن ليغشت نم دكأت VPN.

```

firepower# show crypto ikev2 sa

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf Status Role
442665449 10.197.225.82/500 10.197.225.81/500 READY RESPONDER
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/10 sec
Child sa: local selector 10.57.58.0/0 - 10.57.58.255/65535
remote selector 10.56.58.0/0 - 10.56.58.255/65535
ESP spi in/out: 0x3c8ba92b/0xf79c95a9

```

```
firepower# show crypto ikev2 stats
```

```

Global IKEv2 Statistics
Active Tunnels: 1
Previous Tunnels: 2

```

ةيفيك: انه IKEv2 قافنأ عاطخأ حيحيصت ةيفيك لوح يليصفت ليلد لىل روثعلا نكمي

IKEv2 VPNs حی حصت اسٹاک

- لوصول ایف مکاحتل او عمتجملا ۃلسس تادادع اۃحص نم دکأت و SNMP نیوکت نم ققحت نیتیاهنلا الک یلع.

Firepower# sh مداخل snmp لغشی **** رادصا 2c عمتجم 10.56.58.10 SNMP مداخل فیضم
لاخ snmp مداخل عقوم
ةيلاخ snmp مداخل لاصتا ٥ه
مداخل snmp ****

- لالخ نم SNMP رورم ڈکرچب حامسلانم دکأت FTD.

SNMP روم ڈکرچ حیت ت ڈعاق رفوت نم ققحت ول وصولا یف مکحتلا > تاس ایسلا یل ای لقتنا

Security Policies

→ SSL Decryption → Identity → Security Intelligence → NAT → Access Control > Inspection

4 rules

Filter

gear icon

refresh icon

plus icon

	ID	NAME	SOURCE	PROT	PORTS	DESTINATION	PROT	PORTS	APPLICATION	URL	PROTO	OPTIONS
1	1	Allow all	outside zone	any	any	outside zone	any	any	any	any	any	Block
2	2	Allow out	outside zone	any	any	inside zone	any	any	any	any	any	Block
3	3	allow inzone	inside zone	any	any	inside zone	any	any	any	any	any	Block
4	4	allow all	inside zone	any	any	outside zone	any	any	any	any	any	Block

- لـ كـ اـ شـ مـ يـ أـ يـ لـ عـ فـ رـ عـ تـ لـ اوـ SNMP رـ وـ رـ مـ ظـ كـ رـ حـ ظـ بـ قـ اـ رـ مـ لـ ظـ مـ زـ حـ لـ اـ طـ اـ قـ تـ لـ اـ مـ دـ خـ تـ سـ اـ

لاب طاق تل الـ اـ نـ يـ كـ مـ

```
capture snmp interface inside trace detail match udp any any eq snmp
```

```
firepower# show capture  
capture snmp type raw-data trace detail interface inside include-decrypted [Capturing - 405 bytes]  
match udp host 10.57.58.10 host 10.56.58.1 eq snmp
```

```
firepower# sh capture snmp  
4 packets captured
```

```
1: 17:50:42.271806 10.56.58.10.49830 > 10.57.58.1.161: udp 43  
2: 17:50:42.276551 10.56.58.10.49831 > 10.57.58.1.161: udp 43  
3: 17:50:42.336118 10.56.58.10.49832 > 10.57.58.1.161: udp 44  
4: 17:50:42.338803 10.56.58.10.49833 > 10.57.58.1.161: udp 43
```

4 packets shown

نیوکت مق SNMP نیوکت لیلد نم ققحت، ئیفاصا لیصافت ىلۇمۇچىلىك FirePOWER FDM او ەئاطخا فاشكتىس او

ۋەلصى تاذ تامولۇم

- [Cisco Secure Device Manager نیوکت لیلد](#)
- [Cisco ASA نم تانىيوكت لیلد](#)
- [Cisco SNMP ۆزىمۇجۇ ىلۇمۇچىلىك](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).