

ىلع عقوم ىلإ عقوم نم VPN ةكبش نيوكت FDM نم ةرادملا تانايبلا ةهجاو

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[تانوكتلا](#)

[ةحصلا نم ققحتلا](#)

[اهجالصاو عاخالل افاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

عقوم ىلإ عقوم نم VPN ةكبش لالخ نم ةديعب ةياهن ىلإ SNMP نيوكت دنتسملا اذه فصبي
FTD زاهج تانايب ةهجاو تانايب ةهجاو ىلع.

ةيساسألا تابلطتملا

ةيلاللا ةيساسألا تابلطتملا كيذل نأ نم دكأت، نيوكتلا ةعباتم لبق:

- عيضاوملا هذهل ةيساسألا مهفلا:
 - ةزهجأ ريديم لبق نم ةرادملا Cisco نم FirePOWER (FTD) ديهت دض عافدلا
FirePOWER (FDM).
 - Cisco نم (ASA) ةلدعمل نامألا ةزهجأ.
 - (SNMP) طيسبلا تاكبشلا ةرادلا لوكوتورب.
 - (VPN) ةيرهظلا ةصاخلا ةكبشلا.
- ASA و FTD ةزهجأ ىلإ يرادإلا لوصول.
- رمأ يأل لم تحملا ريثأتلا مهفتو ةرشابم كتكبش نأ نم دكأت.

تابلطتملا

- Cisco FTD رادصإلا، FDM ةطساوب رادملا 7.2.7
- Cisco ASA، رادصإلا 9.16
- (عمتجمللا ةلسلسو IP ناوئع كلذيف امب) SNMP مداخ ليصافت
- (كلذيف امب) عقوم ىلإ عقوم نم (VPN) ةيرهظلا ةصاخلا ةكبشلا نيوكت ليصافت
(اقبسم كرتشم حاتفم وريظنلل IP لوكوتورب)
- SNMP نيوكتلا REST API مادختسال لقالا ىلع 6.7 رادصإلا FTD نوكتي نأ بجي.

ةمدختسمل اتانوكمل

ةيلالتل ةيدامل اتانوكمل او جماربل اتارادصلل دل دن تسمل اذف ةدراول تامولعمل دن تس

- Cisco Firepower Threat Defense (FTD) ةمدصلل FirePOWER Device Manager (FDM)، رادصلل 7.2.7.
- Cisco Adaptive Security Appliance (ASA)، رادصلل 9.16.
- (سلسل ق SNMP مداخل جم انرب لل) SNMP مداخل

ةصاخ ةيلعمل ةئبل لل ةدوومل ةزهألل نل دن تسمل اذف لل ةدراول تامولعمل ءاشنل مل تنال اذل. (سلسل رتفلا) حوسمل نل وكتبل دن تسمل اذف لل ةمدختسمل ةزهألل ءل ممل ءادبل رمل لل لم حملل رل ءائلل كمهل نل دل ءافل، لسل شلل دل ق كلكل بل ش

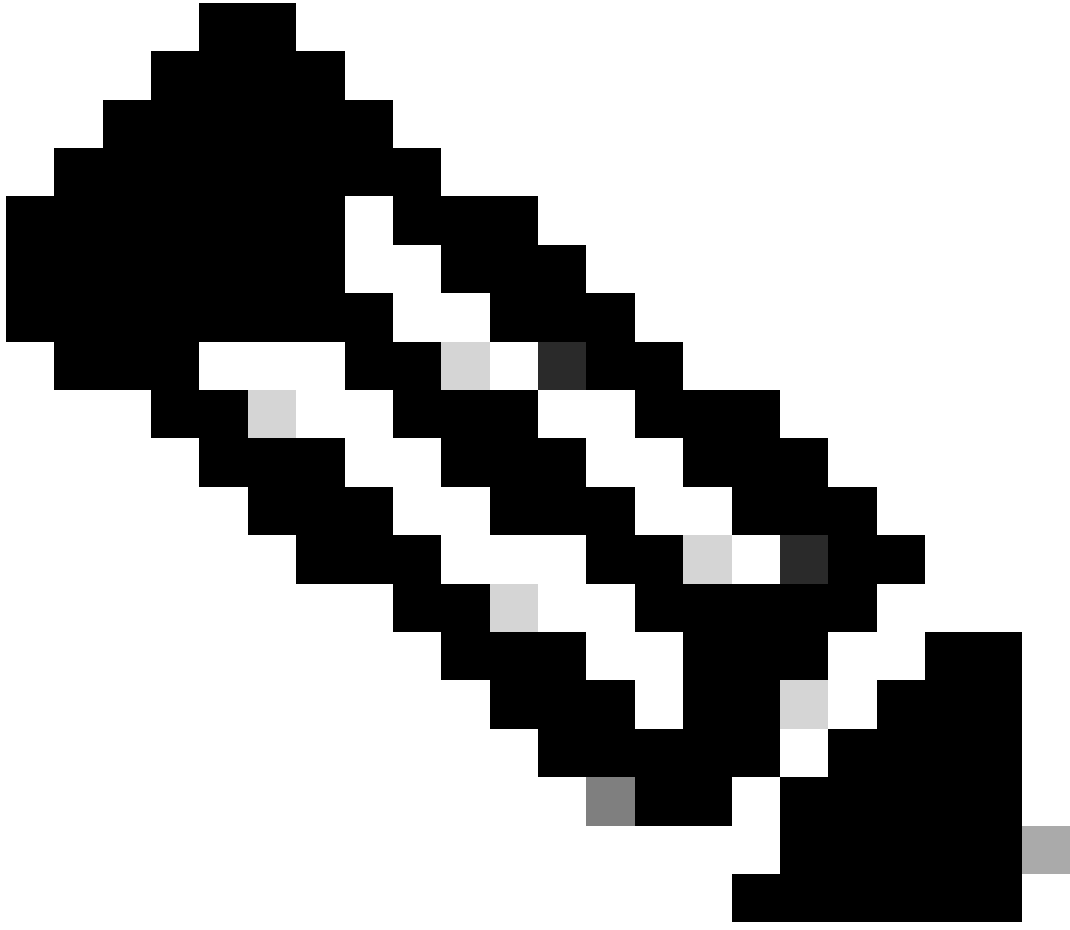
ةلسلسل تامولعمل

مهل صاخلل ةكبلشلل زاهل ةبل قارم نامصل ةكبلشلل لل ووسمل نكم لل، اتاوطخلل هذه حل صول ءوم ءعب نل.

اذف لل. اهلب قارم و ةكبلشلل ةرادلل (طلسبلل ةكبلشلل ةرادل لوكل ووربل) SNMP ماخلتسل مل لل نل VPN ةكبلشلل لال نل نل لل ب SNMP مداخل لل FTD نل SNMP رورم ةكل لل لاسرل مل لل، ءاءلل ل ASA ماخلتسل اب اهؤالشنل مل ءقووم لل ءقووم

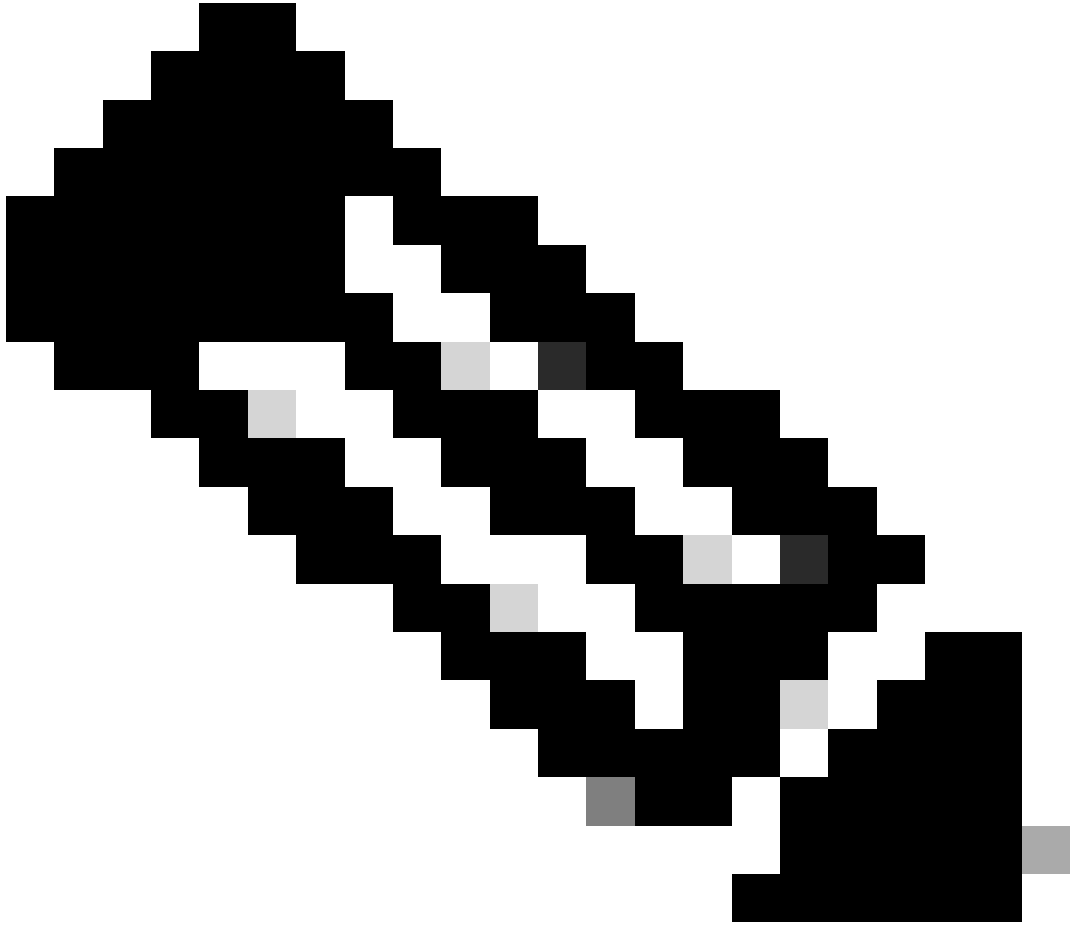
لال نل نل لل فرط لل SNMP نل وكتل لل ءل ءكبلشلل لل ووسم ءءءاسم لل لل لل لل اذف فءل لل ءبل قارم ل اءل فم ءاءلل اذف ءل. FTD زاهل اتانابل ءهءووم لل ءقووم لل ءقووم نل VPN ءكبلشلل لاسرل مل لل و SNMP لوكل ووربل ماخلتسل مل لل، ءاءلل اذف لل. ءعب نل اهتراءووم ءكبلشلل ءزهءووم نل VPN ءكبلشلل لال نل نل لل ب SNMP مداخل لل FTD اتانابل ءهءووم نل SNMP اتانابل رورم ءكل لل ل ASA ماخلتسل اب اهؤالشنل مل ءقووم لل ءقووم

ءاونل لل نل وكتل اذف قل بل طل نكم لل نكلو، "لخلل" ملسا ءمدختسمل ءهءووم لل لل قل لل و لل ءهءووم للسل ءل ءل راءل ءهءووم لل مءختسل نل نكم لل و "ءبرمل لل" رورم ءكل نل نل رل (VPN). ءل رهائلل ءصاخلل ءكبلشلل اهءنل ءهءنل



دنع REST تاقيب طت ةجم رب ةهجاو ربع ال SNMP لوكوتورب نيوك ت نكمي ال :ةظحالم
FDM ةطساوب هترادا متت امك ،ثدحال ا تارادص ال او 6.7 رادص ال FTD ليغشت

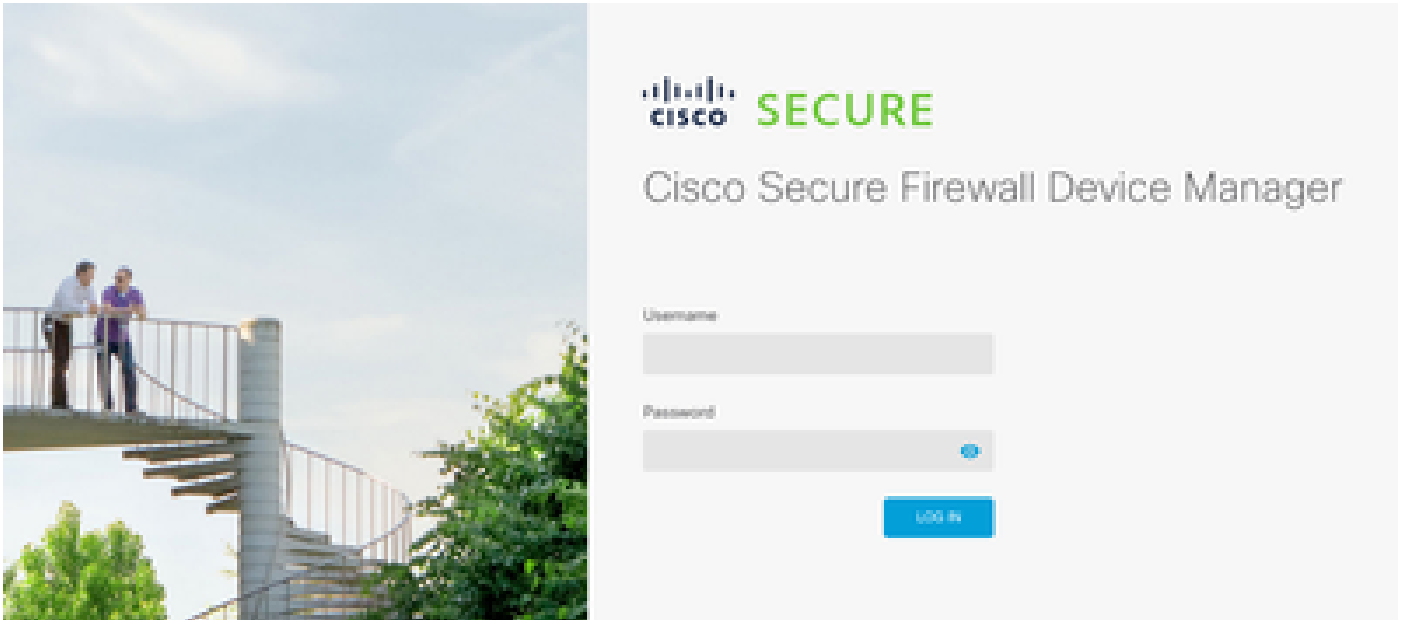
نيوك ت ال



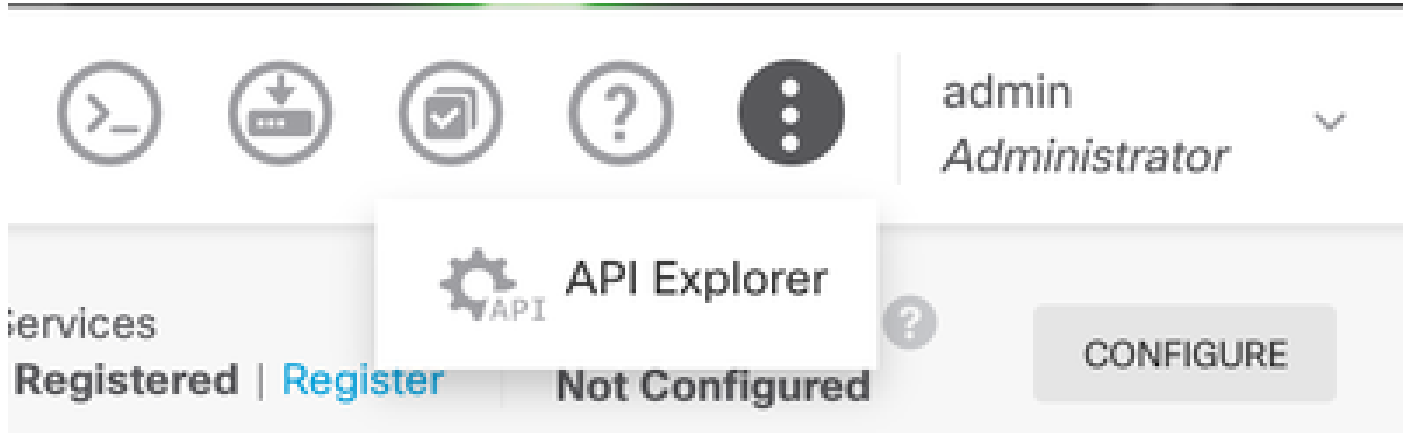
ةزهجالا ني ب لعفالاب نوكم VPN عقوم ىلإ عقوملا نأ نيوكتلا اذه ربتعي :ةظحالم
صحفا VPN عقوم ىلإ عقوملا نيوكت ةيفيك لوح ةيفاضا ليصافت ىلع لوصحلل
ةطساوب ةرادملا FTD ىلع عقوم ىلإ عقوم نم VPN ةكبش نيوكت . نيوكتلا ليلد
[FDM](#)

تانيوكتلا

1. ك ب صاخال FTD ىلإ لوخدلا لجس .



2. (API) تاقېبطلال ةجمرې ةهجاو فشككسم ىل لقتنا زاهجلا ىلع ةماع ةرطن تحت.



3. FTD ىلع SNMPv2 نېوكت.

- ةهجاولا تامولعم ىلع لصحا.



4. موقت. تاقېبطلال ةجمرې ةهجاو اعادتسا عارجال اكلذ ةبرجت رزلا ددحو لفسأل ريرمتلاب مق. 200 ةباجتسالال زمرعارجراب ةحجان ةملاك

TRY IT OUT!

Hide Response

Curl

```
curl -X GET --header 'Accept: application/json' 'https://
```

Request URL

```
https://10.57.58.1:443/api/fdm/v6/devices/default/interfaces
```

Response Body

```
{
  "version": "mqjiipiswsgsx",
  "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

- SNMP فيضمل ةكبش نئاك نيوكت عاشناب مق

NetworkObject

GET

/object/networks

POST

/object/networks

- دي دج SNMPv2c فيضم نئاك عاشناب

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](#) لي اعجالص او هئاطخأ

مدقتملا نيوكتلا مسق يف زاهجال الى لقتنا، زاهجال الى ع SNMP لوكوتورب نيوكت درجم 5. نيوكتلا ضرع دحو

Advanced Configuration

Includes: FlexConfig, Smart CLI

[View Configuration](#)



هتيمستب مق ،ديج نئك عاشناب مق و FlexConfig تانئك ددح ، FlexConfig مسق يف 6. عزج يف رمألا اغلإ فضأو هجاولا ددحو ، بلالاقلا مسق يف management-access رمألا ةفاضإو بلالاقلا 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

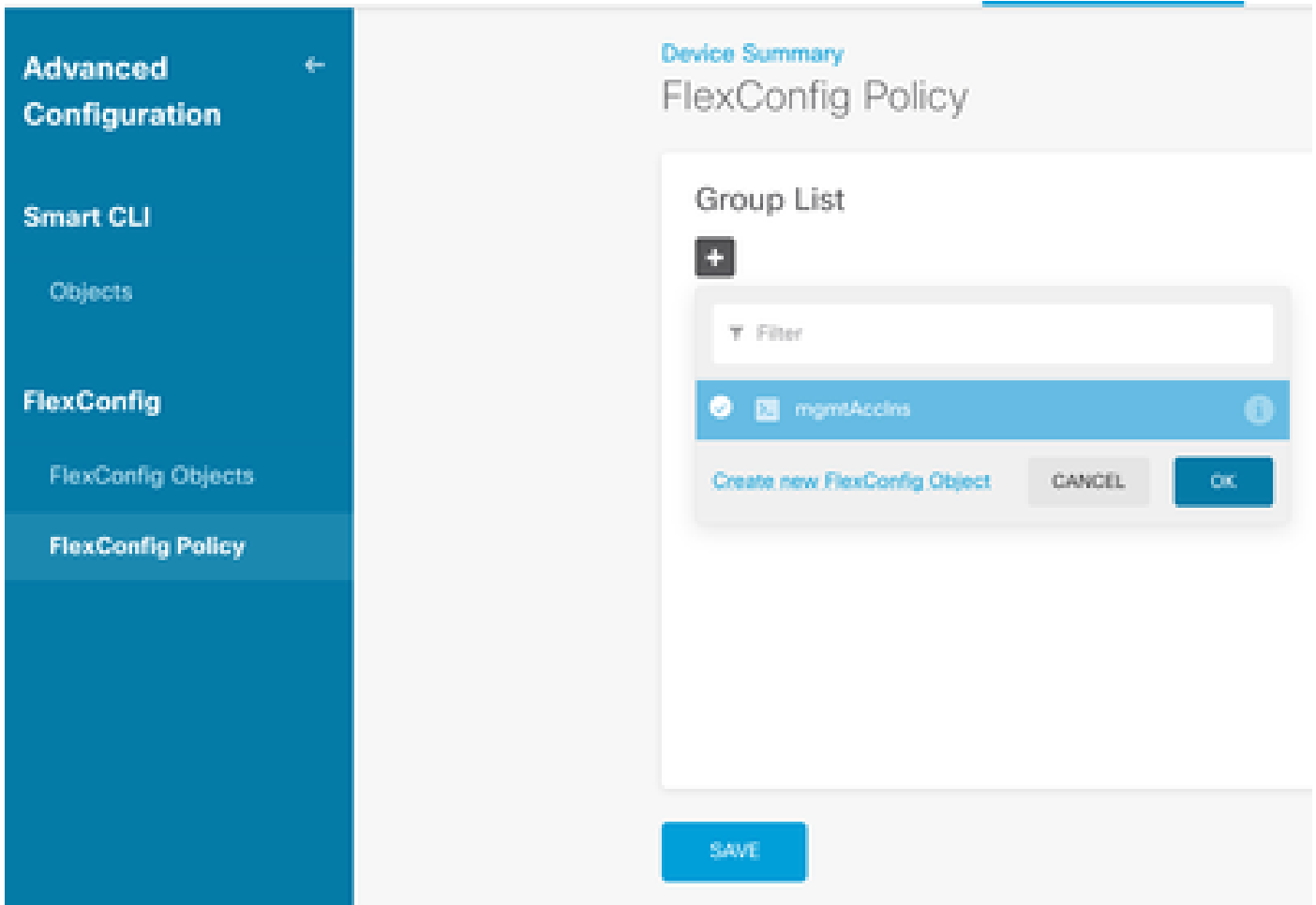
Expand | Reset

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

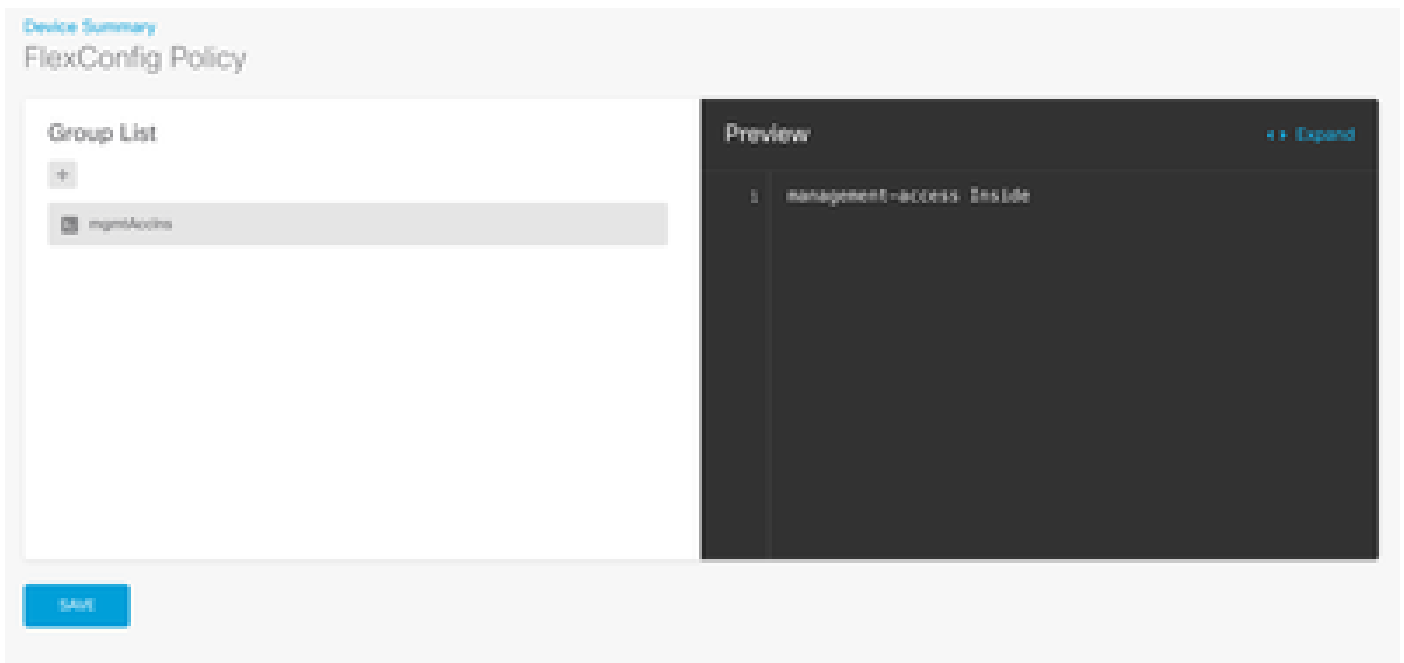
CANCEL

OK

نئاك ددحو ةفاضإلا ةنوقبأ ىلع رقنا ، FlexConfig ةسايس ددح ، FlexConfig مسق ي ف 7. قفاوم ددحو ةقباسلا ةوطخلا ي ف هانأشنأ يذلا FlexConfig.



8. ظرفح ددح .زاهجالا ىلع اهقېب طت م تېس ي تالارم اوألل ةن ياع م رهظت ،كلذ دعب .



9. نأالا "رشن" قوف رقنا ورشنالارم ددح م ت ،نېوك تالارشن ب مق .



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 ▾

كلذ ديكأتل ماهملا ةمئاق نم ققحتلا كنكمي ،ضرم لكشب هلامكإ نم دكأت :ةظحالم

ةحصل نم ققحتلا

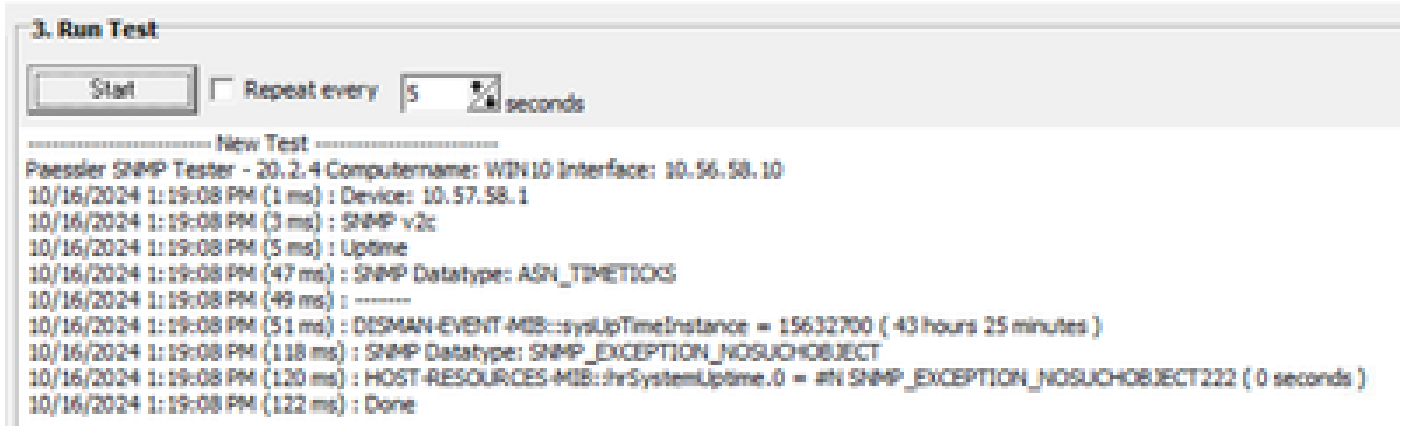
ةدحو و SSH ربع FTD لىل لوخدلا لجسو ،تارابتخالا هذه ءارجإ مق ،نيوكتلا نم ققحتلل رم اوألا هذه لىغشتب مق مث ،مكحتلا

- اهانيرجأ يتلا تاريخيتلا لىل عيوتحي زاهلل هليغشت يراجلا نيوكتلا نأ نم ققحت

```
> 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 outouts are ommitted>
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
```

- حاجة نب هلامك نم دكات و SNMP ربتخم نم رابتخا اناج اب مق



اهحالص او ااطخال فاشك تسا

ةةلاتل تاوطخال ي ف لمأت ف ، لكاشم يا تهجا وا اذا:

- قف ن ققحتل رمال اذ له لىغشت كنكم ي ، ه لىغشت و VPN قف ن لىغشت 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
```

ةةفك : انه IKEv2 قاقفنا ااطخال انا صت ةةففك لوح لى لى صفت لى لى ع روثل كنكم ي

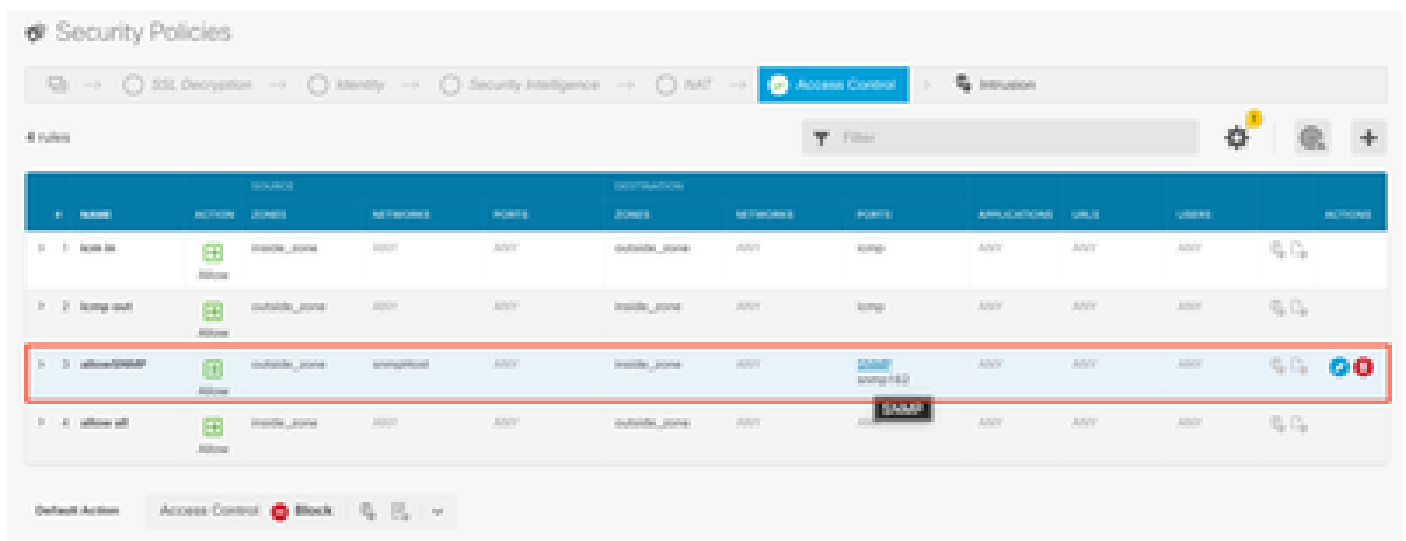
[IKEv2 VPNs](#) اطخأ حيصت

- لوصول ايف مكحتلاو عم تجملا ةلسلس تادادع| ةحص نم دكأتو SNMP نيوكت نم ققحت نيتيهاهنا لك ىلع

```
Firepower# sh mdax snmp
2c رادصا **** عم تجم 10.56.58.10 لخد SNMP مداخل فيضم
لخد snmp مداخل عقوم
ةيلاخ snmp مداخل لاصتا ةهج
snmp مداخل عم تجم *****
```

- FTD لالخد نم SNMP رورم ةكرحب حامسلا نم دكأت

SNMP رورم ةكرحب حيتت ةدعاق رفوت نم ققحتو لوصول ايف مكحتلا > تاسايسلا ىلا لقتنا



#	name	action	source	ref. policies	ports	destination	ref. policies	ports	applications	url	users	actions
1	block in	Block	inside_zone	ANY	ANY	outside_zone	ANY	snmp	ANY	ANY	ANY	
2	block out	Block	outside_zone	ANY	ANY	inside_zone	ANY	snmp	ANY	ANY	ANY	
3	allow SNMP	Allow	outside_zone	snmpHost	ANY	inside_zone	ANY	snmp, snmp161	ANY	ANY	ANY	
4	allow all	Allow	inside_zone	ANY	ANY	outside_zone	ANY	snmp	ANY	ANY	ANY	

- لكاشم يا ىلع فرعتلاو SNMP رورم ةكرحب قارمل ةمزحلا طاقثلا مدختسا

ةيامحلا رادج ىلع عبتتلاب طاقثلال نيكمت:

```
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

[SNMP نېوكټې مق](#)، SNMP نېوكټ لېلډ نم ققحت، ةي فاضا لېصافت ىل ع لوصحلل
[FirePOWER FDM](#) ىل ع اهجالص او هئاطخأ فاشكتس او

ةلص تاذا تامولعم

- [Cisco Secure Device Manager](#) نېوكټ لېلډ
- [Cisco](#) نم [ASA](#) تانېوكټ لېلډ
- [Cisco](#) ةزهجأ ىل ع [SNMP](#) نېوكټ

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 ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا 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 ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح 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 ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج 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 ج ن ا ل ا دن ت س م ل ا