

اهحال صا و هئا طخا فاشك ت سا و SNMP ني وكت ىل ع FirePOWER FDM

تا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س اس ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ة ي س اس ا ت ا م و ل ع م](#)

[ن ي و ك ت ل ا](#)

[SNMP v3](#)

[SNMP v2c](#)

[SNMP ن ي و ك ت ة ل ا ن ا](#)

[ة ح ص ل ا ن م ق ق ح ت ل ا](#)

[SNMP v3 ن م ق ق ح ت ل ا](#)

[SNMP v2c ن م ق ق ح ت ل ا](#)

[اهحال صا و ا ط خ ا ل ا فاشك ت سا](#)

[ة ب و ج ا و ة ل ي س ا](#)

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

ة م د ق م ل ا

ة ر ا د ا ي ل ع (SNMP) ط ي س ب ل ا ة ك ب ش ل ا ة ر ا د ا ل و ك و ت و ر ب ن ي ك م ت ة ي ف ي ك د ن ت س م ل ا ا ذ ه ح ض و ي REST ت ا ق ي ب ط ت ة ح م ر ب ة ه ج ا و م ا د خ ت س ا ب 6.7 ر ا د ص ا ل ا ي ل ع FirePOWER ة ز ه ج ا

ة ي س اس ا ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ة ي ل ل ا ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت:

- ل ع FirePOWER (FDM) ز ا ه ج ة ر ا د ا ل ب ق ن م ه ت ر ا د ا م ت ت Firepower (FTD) د ي د ه ت د ض ع ا ف د ل ا 6.7 ر ا د ص ا ل ا
- REST API ة ف ر ع م
- SNMP ة ف ر ع م

ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ل ع FirePOWER (FDM) ة ز ه ج ا ة ر ا د ا ل ب ق ن م ه ت ر ا د ا م ت ت Firepower (FTD) د ي د ه ت د ض ع ا ف د ل ا 6. 7. ر ا د ص ا ل ا

ةصاخ ةي لمعم ةئيب ي ف ةدوجوملا ةزهجال نم دنتسمل اذ ف ةدراول تامولعمل اشنم مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمل اذ ف ةمدختسمل ةزهجال عيمج تادب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا ديقتك تكبش


ةيساسا تامولعمل

6.7 ي ف ديدجال ام

تاعومجمو ني فيضملا او ني مدختسمل او SNMP م داخ ةرادو نيوكت FTD Device REST API م عدي 6.7 رادصلال ، FP ي ف SNMP FTD زاهجل تاقيبطتلا ةجمر ب ةهجاو معد عم . ةفيضملا ةزهجال

- ةرادال FTD REST API تاقيبطت ةجمر ب ةهجاو لال خ نم SNMP نيوكت مدختسمل ل نكمي ةكبشلا
- تاعومجمو ني مدختسمل او SNMP م داخ ةرادا و ا شي دحت/ ةفاضلا نكمي FTD زاهجل REST تاقيبطت ةجمر ب ةهجاو لال خ نم ني فيضملا/ ني فيضملا

ةطساوب اه داخا مت ي تال نيوكتلا تاوطخ دنتسمل ي ف ةنمضملا ةلثم ال ا فصت FDM ل (API) تاقيبطتلا ةجمر ب ةهجاو فشكتسم

 دنع REST تاقيبطت ةجمر ب ةهجاو ربع ال SNMP لوكوتورب نيوكت نكمي ال : ةظحال م FDM ةطساوب هت رادو FTD لوكوتورب نم 6.7 رادصلال ليغشت

تاقيبطتلا ةجمر ب ةهجاو اول (API) تاقيبطتلا ةجمر ب ةهجاو معد - تازيمل ال ع ةماع ةرطن SNMP FTD زاهجل (REST)

- SNMP ب ةصاخ FDM ل ديدج URL ناو نع ةياهن طاقن ةزيمل ا هذ ف ي ضت
- تاعالطتسال SNMP نيوكتل هذ ةدي دجل تاقيبطتلا ةجمر ب تاهجاو مادختسا نكمي ةمظنالا ةبقارمل خا فل او يرال
- (API) تاقيبطتلا ةجمر ب تاهجاو ربع SNMP لوكوتورب دع ب ام نيوكت ريفوت متي صحفلا راطخال و اعارتقال تاي لمعل ، FirePOWER ةزهجا ال ع (MIB) ةرادال تامولعمل دع او قو NMS/SNMP لي مع ال ع

طاقن SNMP API/URL ةياهن

URL	بي لاس ال	ز رطلال
/devicesettings/default/snmpservers	راضا	SNMPServer
/devicesettings/default/snmpservers/{objId}	ذخ ، عض	SNMPServer
/object/snmphosts	ال ع لوصحل ، لاسرا	SNMPHost
/object/snmphosts/{objId}	لوصحل ، فذخ ، عضو ال ع	SNMPHost

/object/snmpusergroups	ىلع لوصحلا ، لاسرا	SNMPUserGroup
/object/snmpuserGroups/{objId}	لوصحلا ، فذح ، عضو ىلع	SNMPUserGroup
/object/snmpusers	ىلع لوصحلا ، لاسرا	SNMPUser
/object/snmpusers/{objId}	لوصحلا ، فذح ، عضو ىلع	SNMPUser

نيوكتلا

- ةيساسا تارادصا 3 ىلع SNMP فيضم يوتحي

- SNMP v1

- SNMP v2c

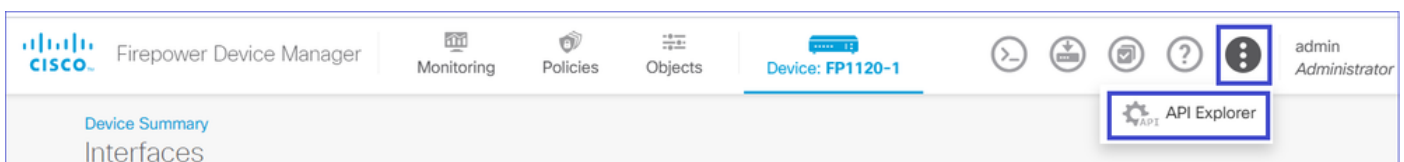
- SNMP v3

- "securityConfiguration" ل ددحم قيسنت ىلع رصانعلا هذه نم دحاولك يوتحي
- فرعي "عون" ل قحو "عمتجم ةلسلس" ىلع يوتحي: V1 و V2C ني رادصا ل ةبس نلاب
V1 و V2C ه نأ نيوكتلا
- فرعي "عون" ل قحو حلاص SNMP v3 مدختسم ىلع يوتحي: SNMP v3 ل ةبس نلاب
v3 ه نأ ىلع نيوكتلا

SNMP v3

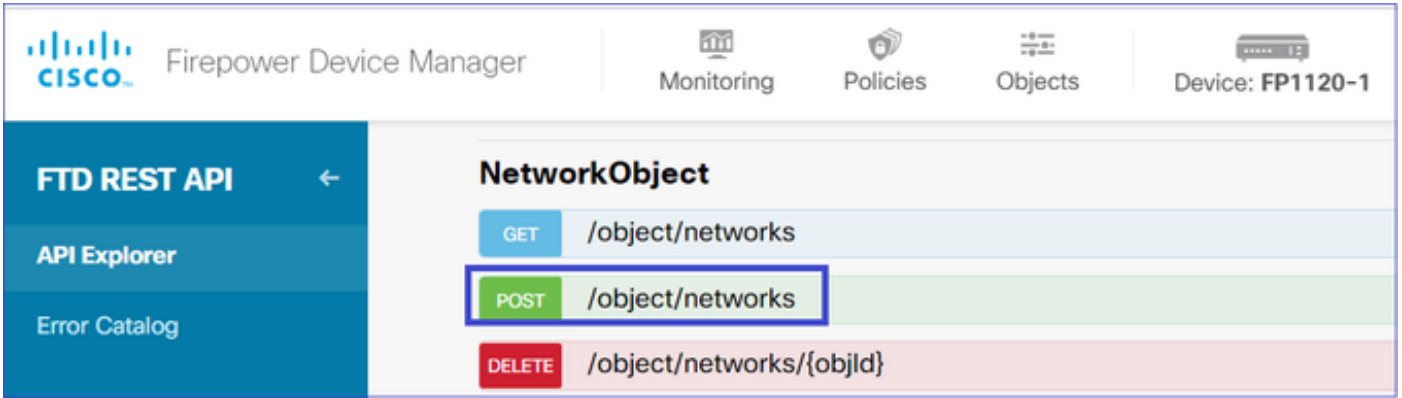
1. FDM ل (API) تاقىب طتلا ةجمر ب ةهجاو فشكتسم ىل لوصولا

مدختسم ل ةهجاو نم FDM REST ل (API) تاقىب طتلا ةجمر ب ةهجاو فشكتسم ىل لوصولا
(API) تاقىب طتلا ةجمر ب ةهجاو فشكتسم م ثال ثال طاقنلا دح، FDM ل (GUI) ةيموسرلا
URL https://FDM_IP/#/api-explorer ناو نع ىل لقتنا ، لكذ نم ال د ب



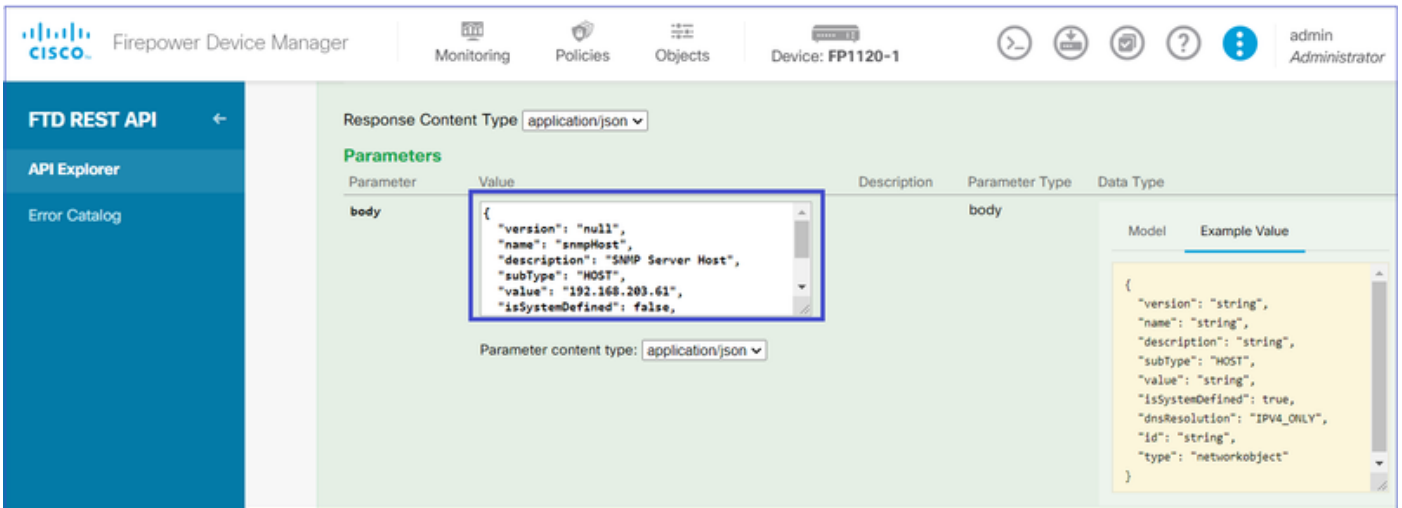
2. ةكبش ل نئاك نيوكت

POST مث NetworkObject دح FDM API Explorer ىلع: SNMP فيضم ل ديدج ةكبش نئاك عاشن
/object/networks:



رېيغتو يې ساسا ل ص ن ل م س ق ي ف JSON اذه ق ص ل ا . اذه وه SNMP ف ي ض م ل JSON ق ي س ن ت
 SNMP ف ي ض م ل IP ن ا و ن ع ة ق ب ا ط م ل " ة م ي ق " ل ع IP ن ا و ن ع

```
{
  "version": "null",
  "name": "snmpHost",
  "description": "SNMP Server Host",
  "subType": "HOST",
  "value": "192.168.203.61",
  "isSystemDefined": false,
  "dnsResolution": "IPV4_ONLY",
  "type": "networkobject"
}
```



ء ة م ر ب ة ه ا و ء ا ع د ت س ا ذ ي ف ن ت ل ! " ة م ي ق " ر ز ل ا د د ح و ل ف س ا ل ا ر ي ر م ت ل ا ب م ق
 200 ة ب ا ج ت س ا ل ا ز م ر ع ا ج ر ا ب ة ح ج ا ن ة م ل ا م م و ق ت . (API) ت ا ق ي ب ط ت ل ا

TRY IT OUT!

تمامولعملاءلمىلإجاحتحت، اقحال. تاطحالمرتفدىلإباجتسالأهجنمJSONتانايبخسنا
SNMP فيضم لوح.

The screenshot displays the FTD REST API Explorer interface. The left sidebar contains the following menu items: "FTD REST API", "API Explorer", and "Error Catalog". The main content area shows the URL `https://10.62.148.231/api/fdm/v6/object/networks`. Below the URL, the "Response Body" is displayed as a JSON object:

```
{
  "version": "bsha3bhghu3vm",
  "name": "snmpHost",
  "description": "SNMP Server Host",
  "subType": "HOST",
  "value": "192.168.203.61",
  "isSystemDefined": false,
  "dnsResolution": "IPV4_ONLY",
  "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
  "type": "networkobject",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/networks/1d10ce6d-49de-11eb-a432-e320cd56d5af"
  }
}
```

Below the response body, the "Response Code" is shown as 200.

3. دي دج SNMPv3 مدختسم عاشنإ.

فديك/اليجرتب مق مث SNMP دح، FDM API Explorer.

Firepower Device Manager

Monitoring Policies Objects Device: FP1120-1

FTD REST API

API Explorer

Error Catalog

SNMP

- GET /devicesettings/default/snmpservers
- GET /devicesettings/default/snmpservers/{objId}
- PUT /devicesettings/default/snmpservers/{objId}
- GET /object/snmpusers
- POST /object/snmpusers

لثالث، لاي بس ىلع) كمهت يتل ماسقالا لي دع تب مقو ةركفم ىل هذه JSON تانايب خسن ا،
 "authenticationPassword" و "encryptionPassword" و "type": "snmpuser":

```
{
"version": null,
"name": "snmpUser",
"description": "SNMP User",
"securityLevel": "PRIV",
"authenticationAlgorithm": "SHA",
"authenticationPassword": "cisco123",
"encryptionAlgorithm": "AES128",
"encryptionPassword": "cisco123",
"id": null,
"type": "snmpuser"
}
```

⚠ في . طقف يحيضوتلا ضرعلا ضارغال يه ةلثمألا يف ةمدختسملا رورملا تاملك ريذحت
 ةيوق رورم تاملك مادختسا نم دكأت، جاتنا ةئييب

يساسألا صنلا مسق ىل ةلدعمل JSON تانايب خسن ا:

Firepower Device Manager

Monitoring Policies Objects Device: FP1120-1 admin Administrator

FTD REST API

API Explorer

Error Catalog

Response Content Type: application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type				
body	<pre>{ "version": null, "name": "snmpUser", "description": "SNMP User", "securityLevel": "PRIV", "authenticationAlgorithm": "SHA", "authenticationPassword": "cisco123", }</pre>		body	<table border="1"> <thead> <tr> <th>Model</th> <th>Example Value</th> </tr> </thead> <tbody> <tr> <td></td> <td> <pre>{ "version": "string", "name": "string", "description": "string", "securityLevel": "AUTH", "authenticationAlgorithm": "SHA", "authenticationPassword": "string", "encryptionAlgorithm": "AES128", "encryptionPassword": "string", "id": "string", "type": "snmpuser" }</pre> </td> </tr> </tbody> </table>	Model	Example Value		<pre>{ "version": "string", "name": "string", "description": "string", "securityLevel": "AUTH", "authenticationAlgorithm": "SHA", "authenticationPassword": "string", "encryptionAlgorithm": "AES128", "encryptionPassword": "string", "id": "string", "type": "snmpuser" }</pre>
Model	Example Value							
	<pre>{ "version": "string", "name": "string", "description": "string", "securityLevel": "AUTH", "authenticationAlgorithm": "SHA", "authenticationPassword": "string", "encryptionAlgorithm": "AES128", "encryptionPassword": "string", "id": "string", "type": "snmpuser" }</pre>							

Parameter content type: application/json

(API) تاقىب طتلا ةجر رب ةه جاو ءاعدتسإ ذى فنن تل ! ةل و احملا رزلا ددحو لفسأ ىلإ رىرمتلاب مق ىلإ ةباجتسالا ةه ج نم JSON تاناىب خسنا . 200 ةباجتسالا زمرع ارب ةحجان ةملاكم موقت SNMP مدختسم لوح تامولعملال علم ىلإ جاتحت ، اقحال . تاظحالم رتفد

The screenshot shows the Firepower Device Manager interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FP1120-1'. The left sidebar has 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main content area displays the 'Request URL' as 'https://10.62.148.231/api/fdm/v6/object/snmpusers'. Below it, the 'Response Body' is shown as a JSON object:

```
{
  "version": "bmwz4iw7php7",
  "name": "snmpUser",
  "description": "SNMP User",
  "securityLevel": "PRIV",
  "authenticationAlgorithm": "SHA",
  "authenticationPassword": "cisco123",
  "encryptionAlgorithm": "AES128",
  "encryptionPassword": "cisco123",
  "id": "65da6c50-49df-11eb-a432-e7823944dabc",
  "type": "snmpuser",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmpusers/65da6c50-49df-11eb-a432-e7823944dabc"
  }
}
```

The 'Response Code' is 200.

4. ةه جاوالا تامولعملال ىلإ لوصحال

ىلإ جاتحت . /default/interfaces/ ةزهجأل/ ىلإ لصحالم ةه جاوالا دىدحتب مق ، FDM API Explorer ىلإ جاتحت SNMP مداخلب لصتت ىلإ ةه جاوالا نم تامولعملال عىمجت

The screenshot shows the Firepower Device Manager interface. The top navigation bar includes 'Monitoring' and 'Policies'. The left sidebar has 'FTD REST API'. The main content area displays the 'GET /devices/default/interfaces' endpoint.

(API) تاقىب طتلا ةجر رب ةه جاو ءاعدتسإ ذى فنن تل ! ةل و احملا رزلا ددحو لفسأ ىلإ رىرمتلاب مق ىلإ ةباجتسالا ةه ج نم JSON تاناىب خسنا . 200 ةباجتسالا زمرع ارب ةحجان ةملاكم موقت ةه جاوالا لوح تامولعملال ةئبعت ىلإ جاتحت ، اقحال . تاظحالم رتفد

FTD REST API ←

API Explorer

Error Catalog

https://10.62.148.231/api/fdm/v6/devices/default/interfaces

Response Body

```

"version": "kkpkibjlu6qro",
"name": "inside",
"description": null,
"hardwareName": "Ethernet1/2",
"monitorInterface": true,
"ipv4": {
  "ipType": "STATIC",
  "defaultRouteUsingDHCP": false,
  "dhcpRouteMetric": null,
  "ipAddress": {
    "ipAddress": "192.168.203.71",
    "netmask": "255.255.255.0",
    "standbyIpAddress": null,
    "type": "haipv4address"
  },
  "dhcp": false,
  "addressNull": false,
  "type": "interfaceipv4"
},
"ipv6": {
  "enabled": false,

```

Response Code

200

JSON تانايې ىل لاثم. JSON تانايې نم "type" و "id" و "name" و "version" ةه جاول لفسأ ظحال ةي لخال ةه جاول نم

<#root>

```

{
  "version": "kkpkibjlu6qro",
  "name": "inside",
  "description": null,
  "hardwareName": "Ethernet1/2",
  "monitorInterface": true,
  "ipv4": {
    "ipType": "STATIC",
    "defaultRouteUsingDHCP": false,
    "dhcpRouteMetric": null,
    "ipAddress": {
      "ipAddress": "192.168.203.71",
      "netmask": "255.255.255.0",
      "standbyIpAddress": null,
      "type": "haipv4address"
    },
    "dhcp": false,
    "addressNull": false,
    "type": "interfaceipv4"
  },
  "ipv6": {

```



```
"enabled": false,
"autoConfig": false,
"dhcpForManagedConfig": false,
"dhcpForOtherConfig": false,
"enableRA": false,
"dadAttempts": 1,
"linkLocalAddress": {
  "ipAddress": "",
  "standbyIpAddress": "",
  "type": "haipv6address"
},
"ipAddresses": [
  {
    "ipAddress": "",
    "standbyIpAddress": "",
    "type": "haipv6address"
  }
],
"prefixes": null,
"type": "interfaceipv6"
},
"managementOnly": false,
"managementInterface": false,
"mode": "ROUTED",
"linkState": "UP",
"mtu": 1500,
"enabled": true,
"macAddress": null,
"standbyMacAddress": null,
"pppoe": null,
"speedType": "AUTO",
"duplexType": "AUTO",
"present": true,
"tenGigabitInterface": false,
"gigabitInterface": false,
```

```
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
```

```
"type": "physicalinterface",
```

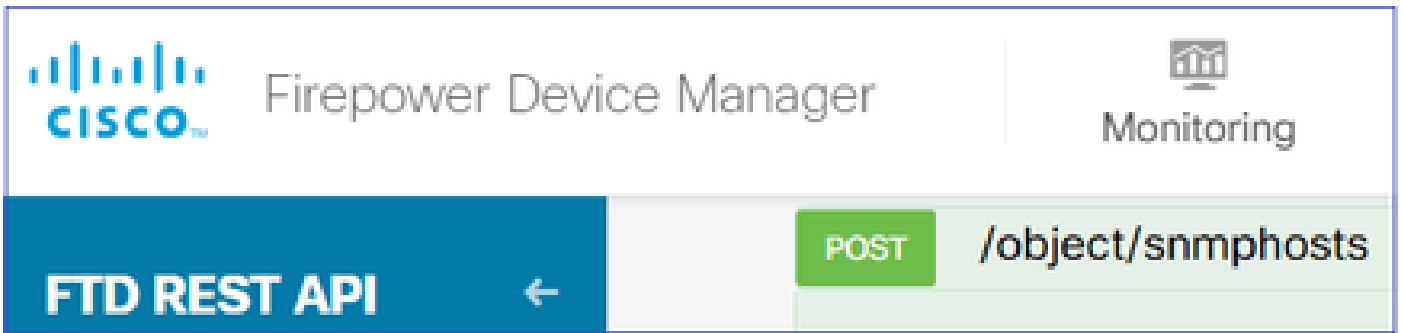
```
"links": {
  "self": "https://10.62.148.231/api/fdm/v6/devices/default/interfaces/fc3d07d4-49d2-11eb-85a8-65aec636a0fc"
},
```

مداخل اهنارق! مزلي يتل تانايبلا ىلع يوتحت 'لخاد' ةهجالا ةيؤر كنكمي، JSON تانايب نم SNMP:

- "version": "kkpkibjlu6qro"
- "لخادلا": "مسالا"،
- "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc".
- "type": "physicalInterface".

5. ديدج SNMpv3 فيضم ءاشنإ.

SNMP لفسأ/سئك/لحرتب مق مئ SNMP دح، FDM API Explorer لىع



اقفوبلاق لىل ةقباسلا تاوطخلال نم تانايا بلاق صل و خسن. بلاقك اذه JSON مدختسا لكذل:

```
{
  "version": null,
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpHost",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "authentication": {
      "version": "bmwz4iw7php7",
      "name": "snmpUser",
      "id": "65da6c50-49df-11eb-a432-e7823944dabc",
      "type": "snmpuser"
    },
    "type": "snmpv3securityconfiguration"
  },
  "interface": {
    "version": "kkpkibjlu6qro",
    "name": "inside",
    "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
    "type": "physicalinterface"
  },
  "id": null,
  "type": "snmpHost"
}
```

ةظحالم:

- يتلا تامولعم لابل مسالا و رادصلال او عونللا و ManagerAddress فرعم في ةميقلا لدبتسا 1 ةوطخلال نم اهتملتسا
- 2 ةوطخلال نم اهيلع تلصح يتلا تامولعم لابل ةقداصلال في ةميقلا لدبتسا

- 3 ةوطخلال نم اهتملتسإ يتل تانايب لابل ةهجالول يف ةميقلا لدبتسا
- وه عونلاو، ةقداصم دجوت ال، لوكوتوربل ةبسنلاب snmpV2csecurityConfiguration نم ال دب snmpv3securityConfiguration

يساسألا صنلا مسق ىلإ ةلدعمل JSON تانايب حسن

The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FP1120-1'. The left sidebar has 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main content area is titled 'Parameters' and shows a table with columns 'Parameter', 'Value', and 'Description'. A parameter named 'body' is highlighted with a blue box, and its value is a JSON object: {"version": null, "name": "snmpv3-host", "description": null, "managerAddress": {"version": "bsha3bhghu3vmk", "name": "snmpHost"}}. The 'Response Content Type' is set to 'application/json' and the 'Parameter content type' is also set to 'application/json'.

(API) تاقيبطتلا ةجرمرب ةهجاو ءاعدتسإ ذيفنتل! ةلواحمل رزلا دجولفسأ ىلإ يرمتلاب مق 200 ةباجتسالال زمرعاجراب ةحجان ةملالم موقت

FTD REST API ←

API Explorer

Error Catalog

Request URL

```
https://10.62.148.231/api/fdm/v6/object/snmphosts
```

Response Body

```
{
  "version": "gneswdadd3isp",
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vm",
    "name": "snmpHost",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "udpPort": 162,
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "authentication": {
      "version": "bmwzw4iw7php7",
      "name": "snmpUser",
      "id": "65da6c50-49df-11eb-a432-e7823944dabc",
      "type": "snmpuser"
    }
  },
}
```

Response Code

```
200
```

عاطالال كنكمي .تاريغتلال رشنب مقو FDM ل (GUI) ةيموسرللا مدختسمللا ةهجاو ىللا لقتنا
مظعم SNMP نيوكت ىلع:

Pending Changes ? ×

✓ **Last Deployment Completed Successfully**
29 Dec 2020 02:32 PM. [See Deployment History](#)

Deployed Version (29 Dec 2020 02:32 PM)	Pending Version																				
<p>+ Network Object Added: <i>snmpHost</i></p> <table border="1"> <tr><td>-</td><td>subType: Host</td></tr> <tr><td>-</td><td>value: 192.168.203.61</td></tr> <tr><td>-</td><td>isSystemDefined: false</td></tr> <tr><td>-</td><td>dnsResolution: IPV4_ONLY</td></tr> <tr><td>-</td><td>description: SNMP Server Host</td></tr> <tr><td>-</td><td>name: snmpHost</td></tr> </table>		-	subType: Host	-	value: 192.168.203.61	-	isSystemDefined: false	-	dnsResolution: IPV4_ONLY	-	description: SNMP Server Host	-	name: snmpHost								
-	subType: Host																				
-	value: 192.168.203.61																				
-	isSystemDefined: false																				
-	dnsResolution: IPV4_ONLY																				
-	description: SNMP Server Host																				
-	name: snmpHost																				
<p>+ snmpHost Added: <i>snmpv3-host</i></p> <table border="1"> <tr><td>-</td><td>udpPort: 162</td></tr> <tr><td>-</td><td>pollEnabled: true</td></tr> <tr><td>-</td><td>trapEnabled: true</td></tr> <tr><td>-</td><td>name: snmpv3-host</td></tr> <tr><td colspan="2">snmpInterface:</td></tr> <tr><td>-</td><td>inside</td></tr> <tr><td colspan="2">managerAddress:</td></tr> <tr><td>-</td><td>snmpHost</td></tr> <tr><td colspan="2">securityConfiguration.authentication:</td></tr> <tr><td>-</td><td>snmpUser</td></tr> </table>		-	udpPort: 162	-	pollEnabled: true	-	trapEnabled: true	-	name: snmpv3-host	snmpInterface:		-	inside	managerAddress:		-	snmpHost	securityConfiguration.authentication:		-	snmpUser
-	udpPort: 162																				
-	pollEnabled: true																				
-	trapEnabled: true																				
-	name: snmpv3-host																				
snmpInterface:																					
-	inside																				
managerAddress:																					
-	snmpHost																				
securityConfiguration.authentication:																					
-	snmpUser																				

MORE ACTIONS ▼ CANCEL DEPLOY NOW ▼

SNMP v2c

يحتاج لارت ال نك لو مدخست سم عاشن إىل جاتحت ال v2c ل قس نلاب

1. SNMPv3 مسق يف فوصوم ل لثم) ةكبش نئاك نيوكت عاشن إىل.
2. SNMPv3 مسق يف حضوم وه امك) ةه جاولا تامول عم يلع لوصح ل.
3. دي ج SNMPv2c فيض نئاك عاشن إىل.

SNMPv2c نئاك ئشنن يت ال JSON ةلومح نم ةنيغ هذو

```
{
  "version": null,
  "name": "snmpv2-Host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpv4hostgrp",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "community": "cisco123",
    "type": "snmpv2csecurityconfiguration"
  }
}
```

```

},
"interface": {
"version": "kkpkibjlu6qro",
"name": "inside",
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
"type": "physicalinterface"
},
"id": null,
"type": "snmpHost"
}

```

JSON قىلومىچ رىشنىل POST بولسا مۇدخىتسا:

The screenshot shows the Cisco Firepower Device Manager interface. On the left, there is a navigation menu with 'FTD REST API' selected. The main area displays the configuration for a REST API endpoint. The 'Response Content Type' is set to 'application/json'. Under the 'Parameters' section, a table lists the parameters for the 'body' parameter. The 'body' parameter is highlighted with a blue box and contains a JSON object:

Parameter	Value	Description
body	<pre> { "version": null, "name": "snmpv2-Host", "description": null, "managerAddress": { "version": "bsha3bhghu3vmk", "name": "snmpv4hostgrp", } } </pre>	

Below the table, the 'Parameter content type' is also set to 'application/json'.

قۇمىر بىر قەدەر ئادەتتە سىزنىڭ ئىنتىڭىڭىزنىڭ! "جورخىللا بىرچىت" رىزىلا دىجىتال سىستېمىسىدا رىمىتلا بىر قەدەر 200 نەپەسلىك زىمىنغا رىبەتتە (API) تاقىيىپتەتتە.

The screenshot shows the Cisco Firepower Device Manager interface displaying the details of a REST API request and response. The 'Request URL' is 'https://10.62.148.231/api/fdm/v6/object/snmpHosts'. The 'Response Body' is a JSON object:

```

{
  "udpPort": 162,
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "community": "*****",
    "type": "snmpv2csecurityconfiguration"
  },
  "interface": {
    "version": "kkpkibjlu6qro",
    "name": "inside",
    "hardwareName": "Ethernet1/2",
    "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
    "type": "physicalinterface"
  },
  "id": "1bfbdf1f0-4ac6-11eb-a432-e76cd376bca7",
  "type": "snmpHost",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmpHosts/1bfbdf1f0-4ac6-11eb-a432-e76cd376bca7"
  }
}

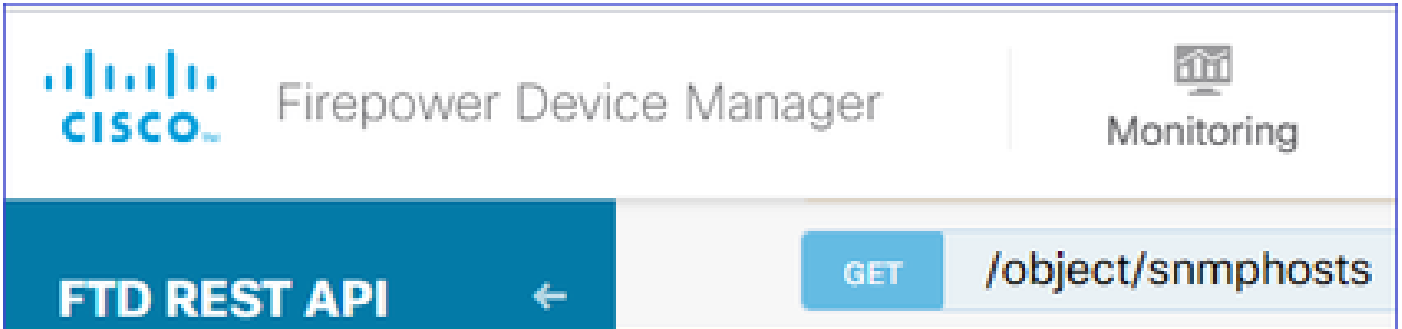
```

The 'Response Code' is 200.

SNMP نيوكت ةلازا

1. ةوطخلال

SNMP (SNMP > /object/snmpHost): تامولعم ىلع لوصحلل



ةجمرب ةهجاو ءاعدتسا ذيفنتل "!جورخلال ةبرجت" رزلا ددحو لفسأ ىلإ ريرمتلاب مق ةباجتسالال زمرع اجراب ةحجان ةملاك موقت (API) تاقيبطتلال

هتلازا ديرت يذال snmpHost نئاكلال فرعم ظحال .تانئاكلال ةمئاق ىلع لصحت

```
<#root>
```

```
{
  "items": [
    {
      "version": "ofaasthu26u1x",
      "name": "snmpv2-Host",
      "description": null,
      "managerAddress": {
        "version": "bsha3bhghu3vm",
        "name": "snmpHost",
        "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
        "type": "networkobject"
      },
      "udpPort": 162,
      "pollEnabled": true,
      "trapEnabled": true,
      "securityConfiguration": {
        "community": "*****",
        "type": "snmpv2csecurityconfiguration"
      },
      "interface": {
        "version": "kkpkibjlu6qro",
        "name": "inside",
        "hardwareName": "Ethernet1/2",
        "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
        "type": "physicalinterface"
      },
      "id": "
1bfb1f0-4ac6-11eb-a432-e76cd376bca7
",
      "type": "snmpHost",
      "links": {
        "self": "https://10.62.148.231/api/fdm/v6/object/snmpHosts/1bfb1f0-4ac6-11eb-a432-e76cd376bca7"
```

```
}  
},
```

2. عوطخال

1: عوطخال يف هتعمج يذلا فرع عمل ق صلا. SNMP > /object/snmphost{objId} يف فذحل رايف رتخأ

The screenshot shows the FTD REST API interface. On the left is a sidebar with 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area displays a DELETE request for the endpoint `/object/snmphosts/{objId}`. Below the endpoint, there are 'Implementation Notes' stating 'This API call is not allowed on the standby unit in an HA pair.' and 'Parameters' section with a table:

Parameter	Value
objId	1bfbd1f0-4ac6-11eb-a432-e76cd376bca7

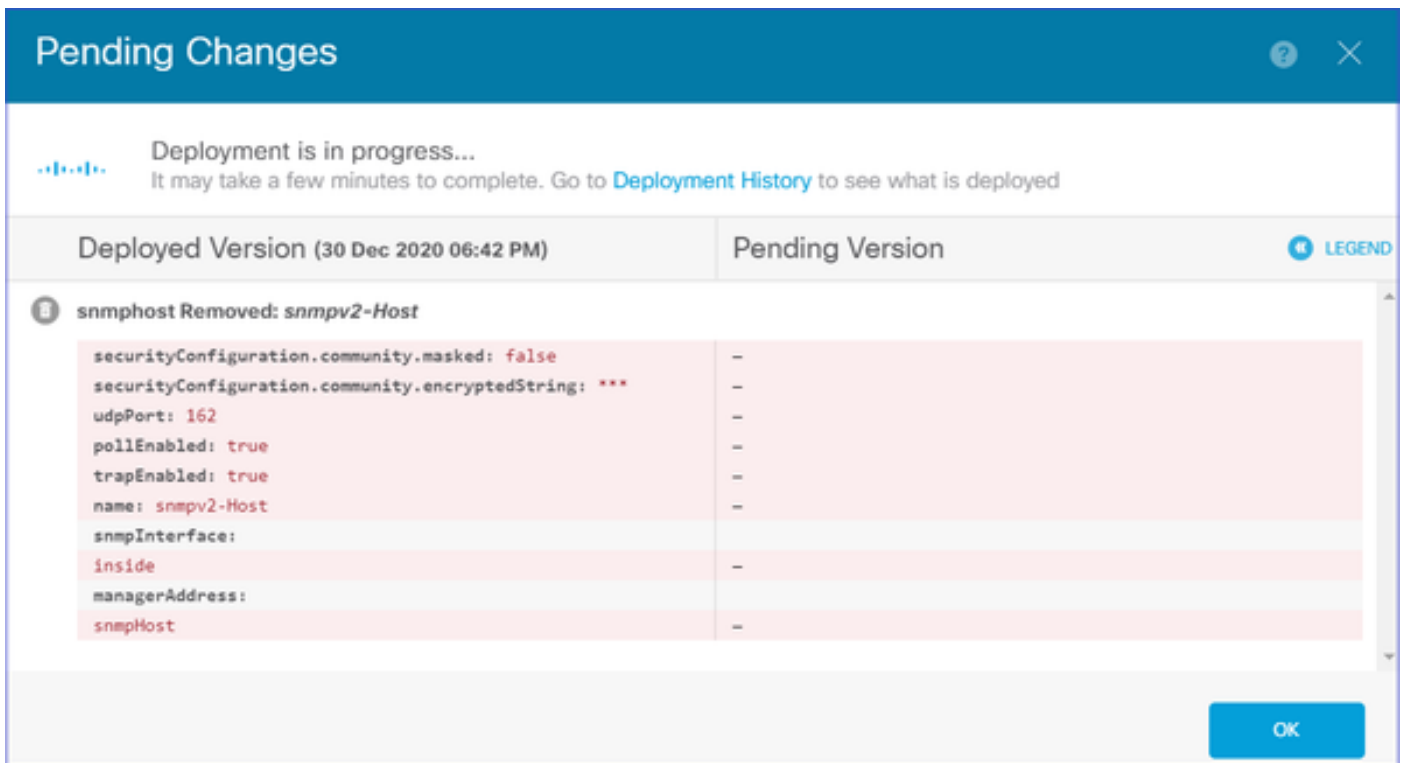
ةجمرب ههجاو عاعدتس اذيفنتل "جورخال ةبرجت" رزلا ددحو لفسأ ىل ايرمرتلاب مق
400 ةباجتسالا زمرة مل كمل اعجت. (API) تاقيبطتلا

The screenshot shows the response details for the failed request. It includes a 'Response Code' of 400 and a 'Response Headers' section with the following JSON data:

```
{  
  "accept-ranges": "bytes",  
  "cache-control": "no-cache, no-store",  
  "connection": "close",  
  "content-type": "application/json;charset=UTF-8",  
  "date": "Wed, 30 Dec 2020 18:00:41 GMT",  
  "expires": "0",  
  "pragma": "no-cache",  
  "server": "Apache",  
  "strict-transport-security": "max-age=63072000; includeSubdomains; preload, max-age=31536000; includeSubDomains",  
  "transfer-encoding": "chunked",  
  "x-content-type-options": "nosniff",  
  "x-frame-options": "SAMEORIGIN, SAMEORIGIN",  
  "x-xss-protection": "1; mode=block"  
}
```

3. عوطخال

ريغتلا رشن:



فيضم الامل تام ولعم ةلازا يلعل رشن اللمع:

```
<#root>
```

```
FP1120-1#
```

```
show run snmp-server
```

```
snmp-server group AUTH v3 auth
snmp-server group PRIV v3 priv
snmp-server group NOAUTH v3 noauth
snmp-server location null
snmp-server contact null
snmp-server community *****
```

لشف ل SNMPwalk ل v2c:

```
<#root>
```

```
root@kali2:~#
```

```
snmpwalk -v2c -c cisco123 -Os 192.168.203.71
```

```
Timeout: No Response from 192.168.203.71
```

ببترت ال اذهب تانئال فذح ببج، 3 رادصل ال ةبسن للاب.

1. (204 وه حجان ال عاجرال زمر) SNMP فيضم.

2. (204) SNMP لوكوتورب مدختسم

أطخالا اذه لىل ع لصحت، ئطاخلال بيترتلاب تانئاكلال فذح تلواح اذا:

```
<#root>
{
  "error": {
    "severity": "ERROR",
    "key": "Validation",
    "messages": [
      {
        "description": "You cannot delete the object because it contains SNMPHost: snmpv3-host2, SNMPHost: snmpv3-host1,
        You must remove the object from all parts of the configuration before you can delete it.",
        "code": "deleteObjWithRel",
        "location": ""
      }
    ]
  }
}
```

ةحصلال نم ققحتلال

SNMP v3 نم ققحتلال

SNMP نيوكت نم ققحتلال ل FTD ب ةصاخلال (CLI) رماوالا رطس ةهجاو لىل لقتنا، رشنال دعب ائاقلت engineID ةميق ءاشنل مت هنا طحال.

```
<#root>
FP1120-1#
connect ftd

>
system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

FP1120-1>
enable

Password:
FP1120-1#
show run all snmp-server
```

```
snmp-server group AUTH v3 auth
snmp-server group PRIV v3 priv
snmp-server group NOAUTH v3 noauth

snmp-server user snmpUser PRIV v3

engineID 80000009febdf0129a799ef469aba2d5fcf1bfd7e86135a1f8

  encrypted auth sha ca:1b:18:f3:62:b1:63:7e:92:34:92:b3:cf:54:86:f9:8e:2a:4c:fd priv aes 128 ca:1b:18:f3:62:b1:63:7e:92:34:92:b3:cf:54:86:f9:8e:2a:4c:fd

snmp-server listen-port 161

snmp-server host inside 192.168.203.61 version 3 snmpUser udp-port 162

snmp-server location null
snmp-server contact null
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
no snmp-server enable traps syslog
no snmp-server enable traps ipsec start stop
no snmp-server enable traps entity config-change fru-insert fru-remove fan-failure power-supply power-failure
no snmp-server enable traps memory-threshold
no snmp-server enable traps interface-threshold
no snmp-server enable traps remote-access session-threshold-exceeded
no snmp-server enable traps connection-limit-reached
no snmp-server enable traps cpu threshold rising
no snmp-server enable traps ikev2 start stop
no snmp-server enable traps nat packet-discard
no snmp-server enable traps config
no snmp-server enable traps failover-state
no snmp-server enable traps cluster-state
snmp-server enable oid mempool
snmp-server enable
```

يعارش ريس رابتخا

```
<#root>
```

```
root@kali2:~#
```

```
snmpwalk -v3 -l authPriv -u snmpUser -a SHA -A cisco123 -x AES -X cisco123 192.168.203.71
```

```
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Firepower Threat Defense, Version 6.7.0 (Build 65), ASA Version 9.8(2)K8"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.2663
iso.3.6.1.2.1.1.3.0 = Timeticks: (1616700) 4:29:27.00
iso.3.6.1.2.1.1.4.0 = STRING: "null"
iso.3.6.1.2.1.1.5.0 = STRING: "FP1120-1"
iso.3.6.1.2.1.1.6.0 = STRING: "null"
iso.3.6.1.2.1.1.7.0 = INTEGER: 4
...
```

نم ققحتلا SNMP v2c

```
<#root>
```

```
FP1120-1#
```

```
show run snmp-server
```

```
snmp-server host inside 192.168.203.61 community ***** version 2c
```

```
snmp-server location null
```

```
snmp-server contact null
```

```
snmp-server community *****
```

SnmpWalk J v2c:

```
<#root>
```

```
root@kali2:~#
```

```
snmpwalk -v2c -c cisco123 -OS 192.168.203.71
```

```
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Firepower Threat Defense, Version 6.7.0 (Build 65), ASA Version 9.
```

```
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.2663
```

```
iso.3.6.1.2.1.1.3.0 = Timeticks: (10482200) 1 day, 5:07:02.00
```

```
iso.3.6.1.2.1.1.4.0 = STRING: "null"
```

```
iso.3.6.1.2.1.1.5.0 = STRING: "FP1120-1"
```

```
iso.3.6.1.2.1.1.6.0 = STRING: "null"
```

```
iso.3.6.1.2.1.1.7.0 = INTEGER: 4
```

اهحال صإو ءاطخأل فاشك تسأ

ةي امحلا رادج ىلع عبتتلاب طاقتلال نيكت مت

```
<#root>
```

```
FP1120-1#
```

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

مزاللة ةيؤر ىلع كتردق نم ققحتو طيسبلا لقننتلا ةادأ مدختسأ

```
<#root>
```

FP1120-1#

show capture

capture CAPI type raw-data trace interface inside

[Capturing - 3137 bytes]

match udp any any eq snmp

طاقات لال ااي و تحم:

<#root>

FP1120-1#

show capture CAPI

154 packets captured

1: 17:04:16.720131	192.168.203.61.51308 >	192.168.203.71.161:	udp 39
2: 17:04:16.722252	192.168.203.71.161 >	192.168.203.61.51308:	udp 119
3: 17:04:16.722679	192.168.203.61.51308 >	192.168.203.71.161:	udp 42
4: 17:04:16.756400	192.168.203.71.161 >	192.168.203.61.51308:	udp 51
5: 17:04:16.756918	192.168.203.61.51308 >	192.168.203.71.161:	udp 42

ىلع لوصح لال SNMP تاجت ساو تابلط رهظت SNMP م داخ تايئاصح ا تاداع نأ نم ققحت
ي: لال لوصح لال او SNMP تاجت ساو تابلط

<#root>

FP1120-1#

show snmp-server statistics

62 SNMP packets input

0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors

58 Number of requested variables

0 Number of altered variables
0 Get-request PDUs

58 Get-next PDUs

0 Get-bulk PDUs
0 Set-request PDUs (Not supported)

58 SNMP packets output

0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors

58 Response PDUs

0 Trap PDUs

نراق NLP يـلـخـادـلـا لـى un-nat طـبـرـلـا .لـخـدم ةـمـزـح عـبـتـت

<#root>

FP1120-1#

show capture CAPI packet-number 1 trace

30 packets captured

1: 17:04:16.720131 192.168.203.61.51308 > 192.168.203.71.

161

: udp 39
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3

Type: UN-NAT

Subtype: static
Result: ALLOW
Config:
Additional Information:
NAT divert to egress interface nlp_int_tap(vrfid:0)

Untranslate 192.168.203.71/161 to 169.254.1.3/4161

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1078, packet dispatched to next module

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:

Found next-hop 169.254.1.3 using egress ifc nlp_int_tap(vrfid:0)

Phase: 11

Type: ADJACENCY-LOOKUP

Subtype: Resolve Nexthop IP address to MAC

Result: ALLOW

Config:

Additional Information:

Found adjacency entry for Next-hop 169.254.1.3 on interface nlp_int_tap

Adjacency :Active

MAC address 3208.e2f2.b5f9 hits 0 reference 1

Result:

input-interface: inside(vrfid:0)

input-status: up

input-line-status: up

output-interface: nlp_int_tap(vrfid:0)

output-status: up

output-line-status: up

Action: allow

SNMP: نيوكت نم عزجك ايئاق لت NAT ةدعاق رشن متي

<#root>

FP1120-1#

show nat

Manual NAT Policies (Section 1)

1 (nlp_int_tap) to (inside) source dynamic nlp_client_0_192.168.203.61_intf4 interface destination stat
translate_hits = 0, untranslate_hits = 0

Auto NAT Policies (Section 2)

...

2 (nlp_int_tap) to (inside) source static nlp_server_0_snmp_intf4 interface service udp 4161 snmp

translate_hits = 0, untranslate_hits = 2

SNMP: رورم ةكرح ىلإ عامتس ال اب موقى UDP 4161 يف لخال ذفنم لاي

<#root>

>

expert

admin@FP1120-1:~\$

sudo netstat -an | grep 4161

Password:

udp 0 0 169.254.1.3:4161 0.0.0.0:*

udp6 0 0 fd00:0:0:1::3:4161 :::*

ارظن لخدم لابة صاخلا SNMP مزمح طاقسإ متي، لمكال ريغ/حيحصلال ريغ نيوكتلال ةلاحي في
unnat: ةلحرم دوجو مدعل

<#root>

FP1120-1#

show cap CAPI packet-number 1 trace

6 packets captured

1: 18:36:35.868485 192.168.203.61.50105 > 192.168.203.71.

161

: udp 42

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: No ECMP load balancing

Result: ALLOW

Config:

Additional Information:

Destination is locally connected. No ECMP load balancing.

Found next-hop 192.168.203.71 using egress ifc identity(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5

Type: ACCESS-LIST

Subtype:

Result: DROP

Config:
Implicit Rule
Additional Information:

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000557415b6347d flow

لهمه طبر لخدمال نأ FTDLINA syslogs رهظي:

<#root>

FP1120-1#

show log | include 161

Dec 30 2020 18:36:38: %FTD-7-710005: UDP request discarded from 192.168.203.61/50105 to inside:192.168.
Dec 30 2020 18:36:39: %FTD-7-710005: UDP request discarded from 192.168.203.61/50105 to inside:192.168.

ةبوجأوةلئسأ

س SNMP لئسر لاسرال FTD ةرادإ ةهجاوم ادختسإ يننكمي له .س

ال. ايلاح موعدم ريغ اذه ،

ةلصلال تاذ تانيسحتلال يف بيعلال

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu48012>

ةلص تاذا تامولعم

- [6.7 رادصلال، Firepower ةزهجأ ةرادال Cisco نم Firepower Threat Defense نيوكت ليلد](#)
- [Cisco Firepower ديدهت نع عافدلا تاقيبطت ةجمرب ةهجاو ليلد](#)
- [6.7.0 رادصلال، Cisco Firepower رادصل تاظالم](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ان أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 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 (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا