

Configurar e solucionar problemas de SNMP no Firepower FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[SNMP v3](#)

[SNMP v2c](#)

[Remoção da configuração do SNMP](#)

[Verificar](#)

[Verificação SNMP v3](#)

[Verificação SNMP v2c](#)

[Troubleshooting](#)

[Perguntas e respostas](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como habilitar o SNMP (Simple Network Management Protocol) no Firepower Device Management na versão 6.7 com a API REST.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense (FTD) gerenciado pelo Firepower Device Management (FDM) na versão 6.7
- Conhecimento da API REST
- Conhecimento de SNMP

Componentes Utilizados

Firepower Threat Defense (FTD) gerenciado pelo Firepower Device Management (FDM) na versão 6.7.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.


Informações de Apoio

Novidades no 6.7

A API REST do dispositivo FTD oferece suporte à configuração e ao gerenciamento de servidores, usuários, hosts e grupos de hosts SNMP. Com o suporte à API REST do dispositivo SNMP FTD no FP 6.7:

- Um usuário pode configurar o SNMP através da API REST do dispositivo FTD para gerenciar a rede
- O servidor SNMP, os usuários e os grupos de host/host podem ser adicionados/atualizados ou gerenciados por meio da API REST do dispositivo FTD.

Os exemplos incluídos no documento descrevem as etapas de configuração executadas pelo FDM API Explorer.

 Observação: o SNMP só pode ser configurado via API REST quando o FTD executa a versão 6.7 e é gerenciado pelo FDM

Visão geral do recurso - Suporte à API REST do dispositivo SNMP FTD

- Este recurso adiciona novos pontos de extremidade de URL do FDM específicos ao SNMP.
- Essas novas APIs podem ser usadas para configurar o SNMP para votações e interceptações para monitorar sistemas.
- A configuração pós-SNMP através de APIs, as Bases de Informações de Gerenciamento (MIBs - Management Information Bases) nos dispositivos Firepower, estão disponíveis para sondagens ou notificação de interceptação no Cliente NMS/SNMP.

Terminais SNMP API/URL

| URL | Métodos | Modelos |
|---|----------------|--------------|
| /devicesettings/default/snmpservers | GET | ServidorSNMP |
| /devicesettings/default/snmpservers/{objId} | COLOCAR, OBTER | ServidorSNMP |
| /object/snmphosts | POSTAR, OBTER | SNMPHost |
| /object/snmphosts/{objId} | COLOCAR, | SNMPHost |

| | | |
|--------------------------------|----------------------------|---------------|
| | EXCLUIR, OBTER | |
| /object/snmpusergroups | POSTAR, OBTER | SNMPUserGroup |
| /object/snmpusergroups/{objId} | COLOCAR, EXCLUIR, OBTER | SNMPUserGroup |
| /object/snmpusers | POSTAR, OBTER | SNMPUser |
| /object/snmpusers/{objId} | COLOCAR, EXCLUIR, OBTER | SNMPUser |

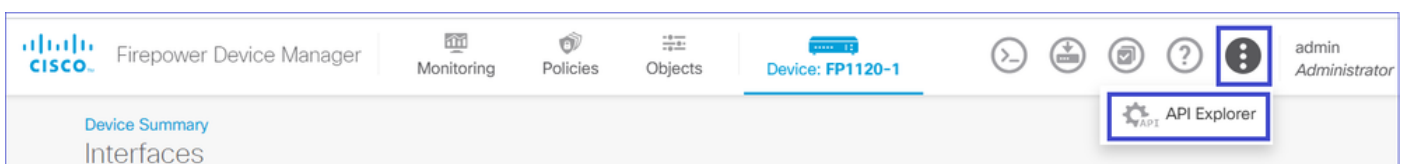
Configurar

- O host SNMP tem 3 versões principais
 - SNMP V1
 - SNMP V2C
 - SNMP V3
 - Cada um deles tem um formato específico para "securityConfiguration".
 - Para V1 e V2C: contém um campo "Community String" e um campo "type" que identifica a configuração como V1 ou V2C.
 - Para SNMP V3: contém um usuário SNMP V3 válido e um campo "type" que identifica a configuração como V3.

SNMP v3

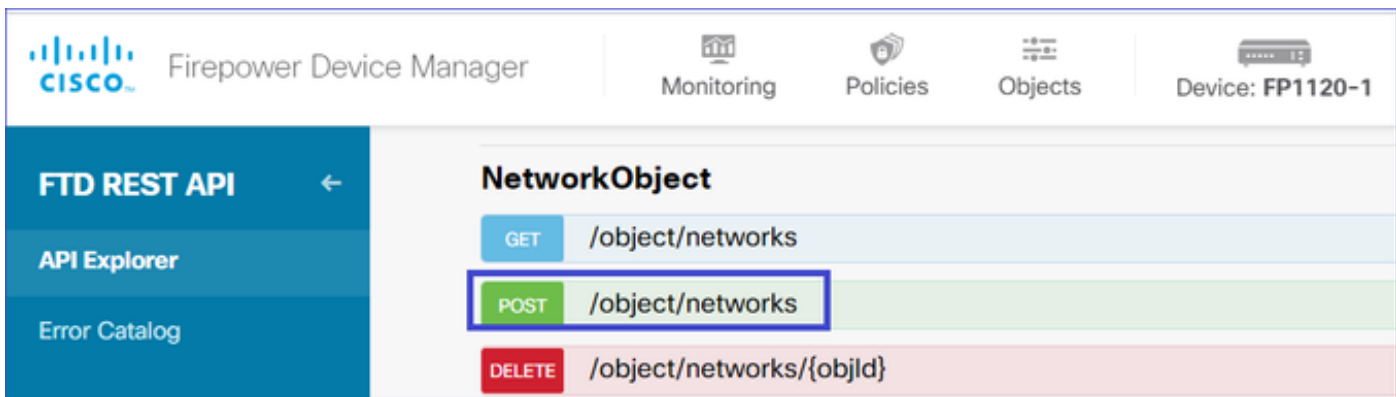
1. Acesse o API Explorer do FDM

Para acessar o Explorador da API REST do FDM na GUI do FDM, selecione os 3 pontos e, em seguida, Explorador da API. Como alternativa, navegue até a URL https://FDM_IP/#!/api-explorer:



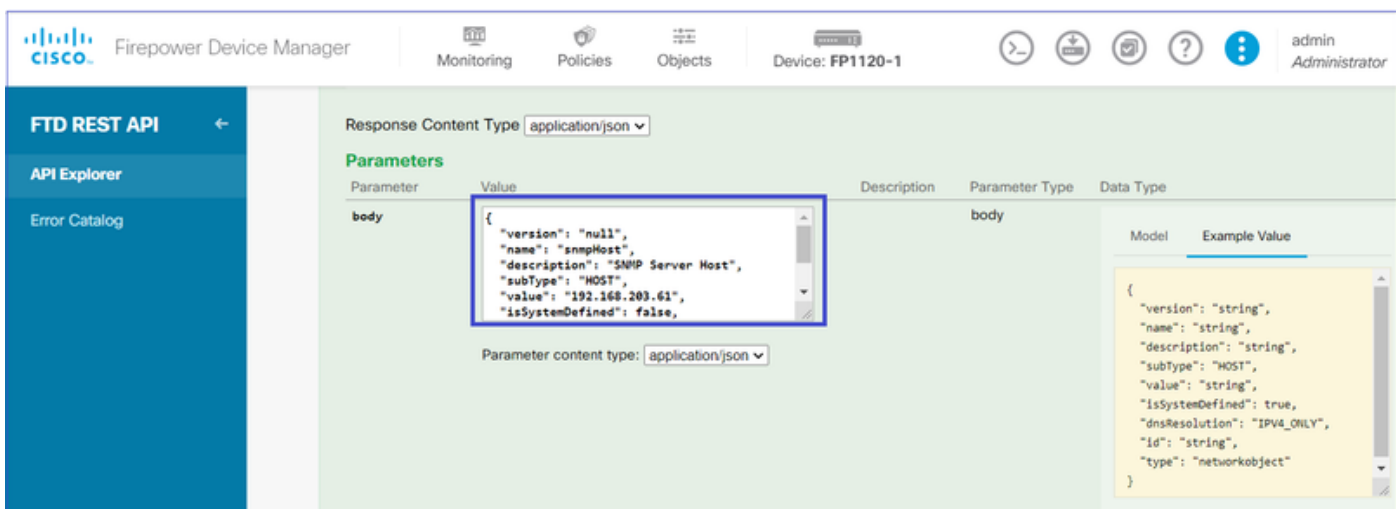
2. Configuração de Objetos de Rede

Crie um novo objeto de rede para o host SNMP: no FDM API Explorer, selecione NetworkObject e depois POST /object/networks:



O formato SNMP Host JSON é este. Cole esse JSON na seção do corpo e altere o endereço IP no "valor" para corresponder ao endereço IP do host SNMP:

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



Role para baixo e selecione o botão TRY IT OUT! para executar a chamada à API. Uma chamada bem-sucedida retorna o código de resposta 200.

TRY IT OUT!

Copie os dados JSON do corpo da resposta para um bloco de notas. Mais tarde, você precisa preencher as informações sobre o host SNMP.



The screenshot shows the FTD REST API Explorer interface. On the left, there is a sidebar with the following items: "FTD REST API" (with a back arrow), "API Explorer", and "Error Catalog". The main area displays the details of an API call to the endpoint `https://10.62.148.231/api/fdm/v6/object/networks`. The "Response Body" section contains the following JSON data:

```
{
  "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"
  }
}
```

The "Response Code" section shows a status of 200.

3. Criar um novo usuário SNMPv3


No FDM API Explorer, selecione SNMP e depois POST `/object/snmpusers`

The screenshot shows the Cisco Firepower Device Manager interface. On the left, there is a navigation menu with 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area displays the 'SNMP' section with a list of REST API endpoints:

- GET /devicesettings/default/snmpservers
- GET /devicesettings/default/snmpservers/{objId}
- PUT /devicesettings/default/snmpservers/{objId}
- GET /object/snmpusers
- POST /object/snmpusers** (highlighted with a blue box)

Copie esses dados JSON para um bloco de notas e modifique as seções de seu interesse (por exemplo, "authenticationPassword", "encryptionPassword" ou os algoritmos):

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

 Cuidado: as senhas usadas nos exemplos são apenas para fins de demonstração. Em um ambiente de produção, certifique-se de usar senhas fortes

Copie os dados JSON modificados para a seção do corpo:

The screenshot shows the Cisco Firepower Device Manager interface for configuring a REST API endpoint. The 'Parameters' section is visible, with a table showing the 'body' parameter. The 'body' field is highlighted with a blue box and contains the following JSON payload:

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

Below the 'body' field, there is a dropdown menu for 'Parameter content type' set to 'application/json'. To the right, there is a 'Model' section with an 'Example Value' field containing a JSON schema definition:

```
{
"version": "string",
"name": "string",
"description": "string",
"securityLevel": "AUTH",
"authenticationAlgorithm": "SHA",
"authenticationPassword": "string",
"encryptionAlgorithm": "AES128",
"encryptionPassword": "string",
"id": "string",
"type": "snmpuser"
}
```

Role para baixo e selecione o botão TRY IT OUT! para executar a chamada à API. Uma chamada bem-sucedida retorna o código de resposta 200. Copie os dados JSON do corpo da resposta para um bloco de notas. Posteriormente, você precisará preencher as informações sobre o usuário SNMP.

The screenshot shows the Cisco Firepower Device Manager REST API interface. The top navigation bar includes the Cisco logo, the text "Firepower Device Manager", and icons for "Monitoring", "Policies", and "Objects". The device name "Device: FP1120-1" is displayed on the right. The left sidebar contains "FTD REST API" (selected), "API Explorer", and "Error Catalog". The main content area is divided into three sections: "Request URL" with the value "https://10.62.148.231/api/fdm/v6/object/snmpusers", "Response Body" containing a JSON object, and "Response Code" with the value "200". The JSON object in the response body is:

```
{
  "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"
  }
}
```

4. Obter informações da interface

No FDM API Explorer, selecione Interface e, em seguida, GET /devices/default/interfaces. Você precisa coletar informações da interface que se conecta ao servidor SNMP.

The screenshot shows the Cisco Firepower Device Manager REST API interface. The top navigation bar includes the Cisco logo, the text "Firepower Device Manager", and icons for "Monitoring" and "Policies". The left sidebar contains "FTD REST API" (selected). The main content area shows the endpoint "GET /devices/default/interfaces".

Role para baixo e selecione o botão TRY IT OUT! para executar a chamada à API. Uma chamada bem-sucedida retorna o código de resposta 200. Copie os dados JSON do corpo da resposta para um bloco de notas. Mais tarde, você precisa preencher as informações sobre a interface.

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

Anote a interface "version", "name", "id" e "type" a partir dos dados JSON. Exemplo de um dado JSON da interface interna:

<#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-85a8-65aec636a0"
}
},

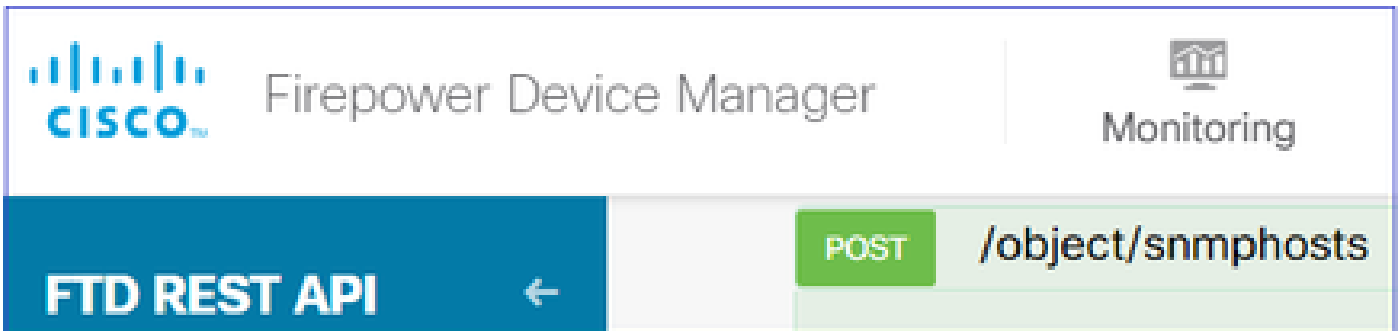
```

A partir dos dados JSON, você pode ver que a interface 'inside' tem estes dados que precisam ser associados ao servidor SNMP:

- "versão": "kpkibjlu6qro"
- "nome": "dentro",
- "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
- "type": "physicalinterface",

5. Criar um novo host SNMPv3

No FDM API Explorer, selecione SNMP e depois POST /object/snmphosts/em SNMP



Use este JSON como um modelo. Copie e cole os dados das etapas anteriores no modelo de acordo:

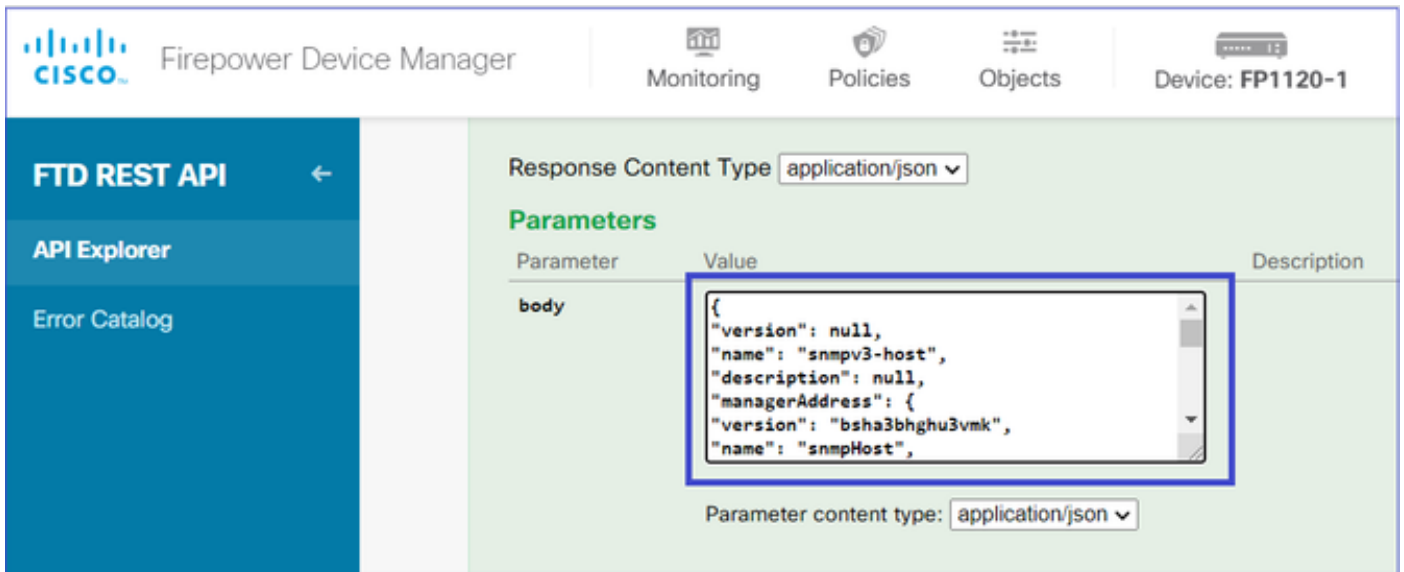
```
{
  "version": null,
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpHost",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "authentication": {
      "version": "bmwzw4iw7php7",
      "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"
}
```

Note:

- Substitua o valor em managerAddress id, type, version e name pelas informações recebidas da Etapa 1
- Substitua o valor na autenticação pelas informações recebidas da Etapa 2

- Substitua o valor na interface pelos dados recebidos da Etapa 3
- Para SNMP2, não há autenticação e o tipo é snmpv2csecurityconfiguration em vez de snmpv3securityconfiguration

Copiar os dados JSON modificados para a seção do corpo



The screenshot displays the Cisco Firepower Device Manager (FDM) REST API interface. The top navigation bar includes the Cisco logo, the text 'Firepower Device Manager', and several icons for 'Monitoring', 'Policies', 'Objects', and 'Device: FP1120-1'. On the left, a sidebar shows 'FTD REST API' with sub-links for 'API Explorer' and 'Error Catalog'. The main content area is titled 'Parameters' and features a table with columns for 'Parameter', 'Value', and 'Description'. A single parameter named 'body' is listed, with its value field containing a JSON object:

```
{
  "version": null,
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpHost",
  }
}
```

. The 'Response Content Type' dropdown is set to 'application/json', and the 'Parameter content type' dropdown is also set to 'application/json'.

Role para baixo e selecione o botão TRY IT OUT! para executar a chamada à API. Uma chamada bem-sucedida retorna o código de resposta 200.

The screenshot displays the FTD REST API interface. On the left is a blue sidebar with the following menu items: "FTD REST API" (with a back arrow), "API Explorer", and "Error Catalog". The main content area is divided into three sections:

- Request URL:** `https://10.62.148.231/api/fdm/v6/object/snmphosts`
- Response Body:** A JSON object representing the configuration of an SNMP host:

```
{
  "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": "bmwz4iw7php7",
      "name": "snmpUser",
      "id": "65da6c50-49df-11eb-a432-e7823944dabc",
      "type": "snmpuser"
    }
  }
},
```
- Response Code:** 200

Navegue até a GUI do FDM e Implante as alterações. Você pode ver a maior parte da configuração SNMP:

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 |
|--|-------------------------------|
| + Network Object Added: snmpHost | |
| - | subType: Host |
| - | value: 192.168.203.61 |
| - | isSystemDefined: false |
| - | dnsResolution: IPV4_ONLY |
| - | description: SNMP Server Host |
| - | name: snmpHost |
| + snmpHost Added: snmpv3-host | |
| - | udpPort: 162 |
| - | pollEnabled: true |
| - | trapEnabled: true |
| - | name: snmpv3-host |
| snmpInterface: | inside |
| managerAddress: | snmpHost |
| securityConfiguration.authentication: | snmpUser |

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

SNMP v2c

Para o v2c, você não precisa criar um usuário, mas ainda precisa:

1. Criar uma configuração de objeto de rede (como descrito na seção SNMPv3)
2. Obter informações de interface (as mesmas descritas na seção SNMPv3)
3. Criar um novo objeto de host SNMPv2c

Este é um exemplo de um payload JSON que cria um objeto SNMPv2c:

```
{
  "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": "snmpghost"
}

```

Use o método POST para implantar o payload JSON:

The screenshot shows the Cisco Firepower Device Manager interface. The left sidebar is titled "FTD REST API" and includes "API Explorer" and "Error Catalog". The main area is titled "Parameters" and shows a table with columns "Parameter", "Value", and "Description". A row is defined for the parameter "body" with a JSON payload in the "Value" column. The "Response Content Type" is set to "application/json" and the "Parameter content type" is also set to "application/json".

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

Role para baixo e selecione o botão TRY IT OUT! para executar a chamada à API. Uma chamada bem-sucedida retorna o código de resposta 200.

The screenshot shows the results of the API call. The "Request URL" is "https://10.62.148.231/api/fdm/v6/object/snmpghosts". The "Response Body" is a JSON object containing configuration details for an SNMP host and its interface. The "Response Code" is 200.

```

Request URL
https://10.62.148.231/api/fdm/v6/object/snmpghosts

Response Body
{
  "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": "snmpghost",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmpghosts/1bfbdf1f0-4ac6-11eb-a432-e76cd376bca7"
  }
}

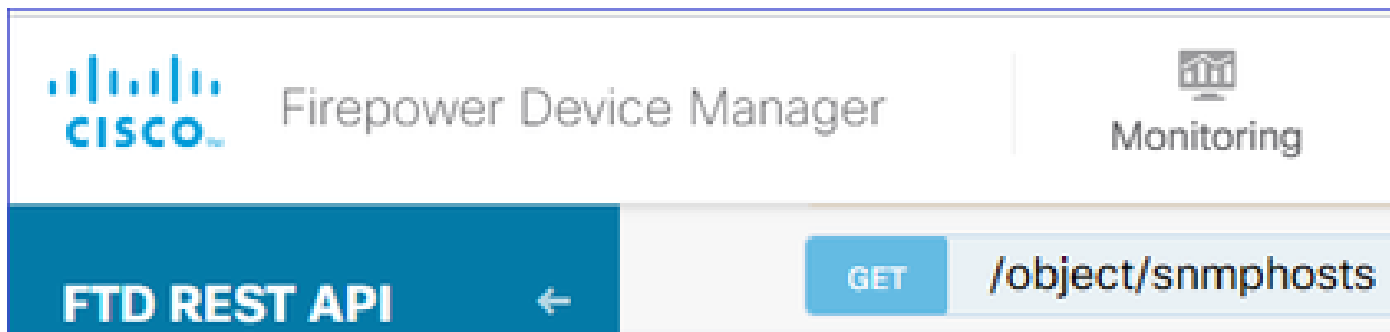
Response Code
200

```

Remoção da configuração do SNMP

Etapa 1.

Obtenha as informações do host SNMP (SNMP > /object/snmphosts):



Role para baixo e selecione o botão TRY IT OUT! para executar a chamada à API. Uma chamada bem-sucedida retorna o código de resposta 200.

Você obtém uma lista de objetos. Anote o id do objeto snmphost que você deseja remover:

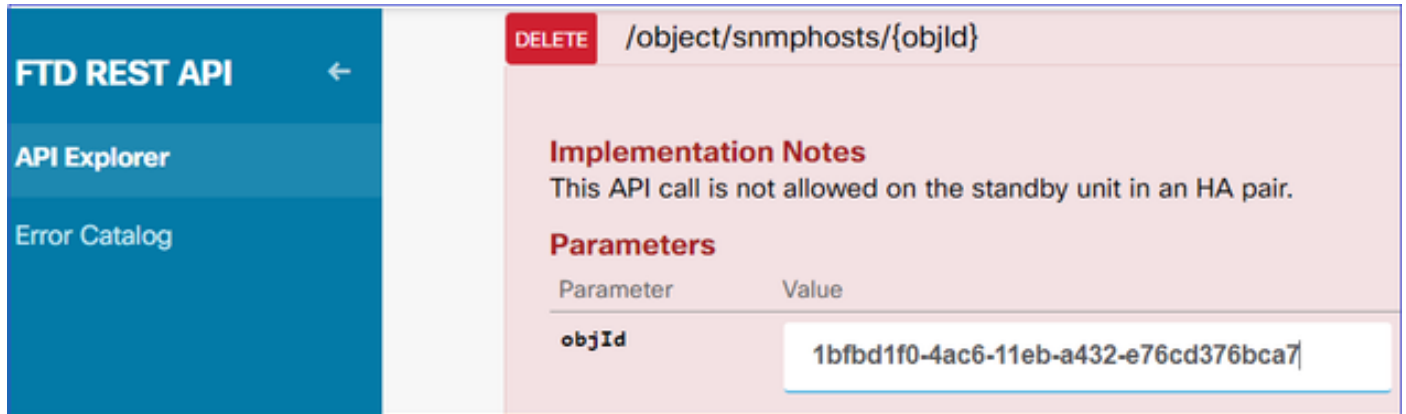
```
<#root>
```

```
{
  "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": "
1bfbd1f0-4ac6-11eb-a432-e76cd376bca7"
    },
    {
      "type": "snmphost",
      "links": {
        "self": "https://10.62.148.231/api/fdm/v6/object/snmphosts/1bfbd1f0-4ac6-11eb-a432-e76cd376bca7"
```

```
}  
},
```

Etapa 2.

Escolha a opção DELETE em SNMP > /object/snmphosts{objId}. Cole a ID que você coletou na etapa 1:



The screenshot shows the FTD REST API interface. On the left, there is a navigation menu with 'API Explorer' and 'Error Catalog'. The main area displays the endpoint `/object/snmphosts/{objId}` with a 'DELETE' method. Below this, there are sections for 'Implementation Notes' (stating the call is not allowed on the standby unit in an HA pair) and 'Parameters'. A table lists the parameter `objId` with its value `1bfd1f0-4ac6-11eb-a432-e76cd376bca7`.

| Parameter | Value |
|--------------------|--|
| <code>objId</code> | <code>1bfd1f0-4ac6-11eb-a432-e76cd376bca7</code> |

Role para baixo e selecione o botão TRY IT OUT! para executar a chamada à API. A chamada retorna o código de resposta 400.

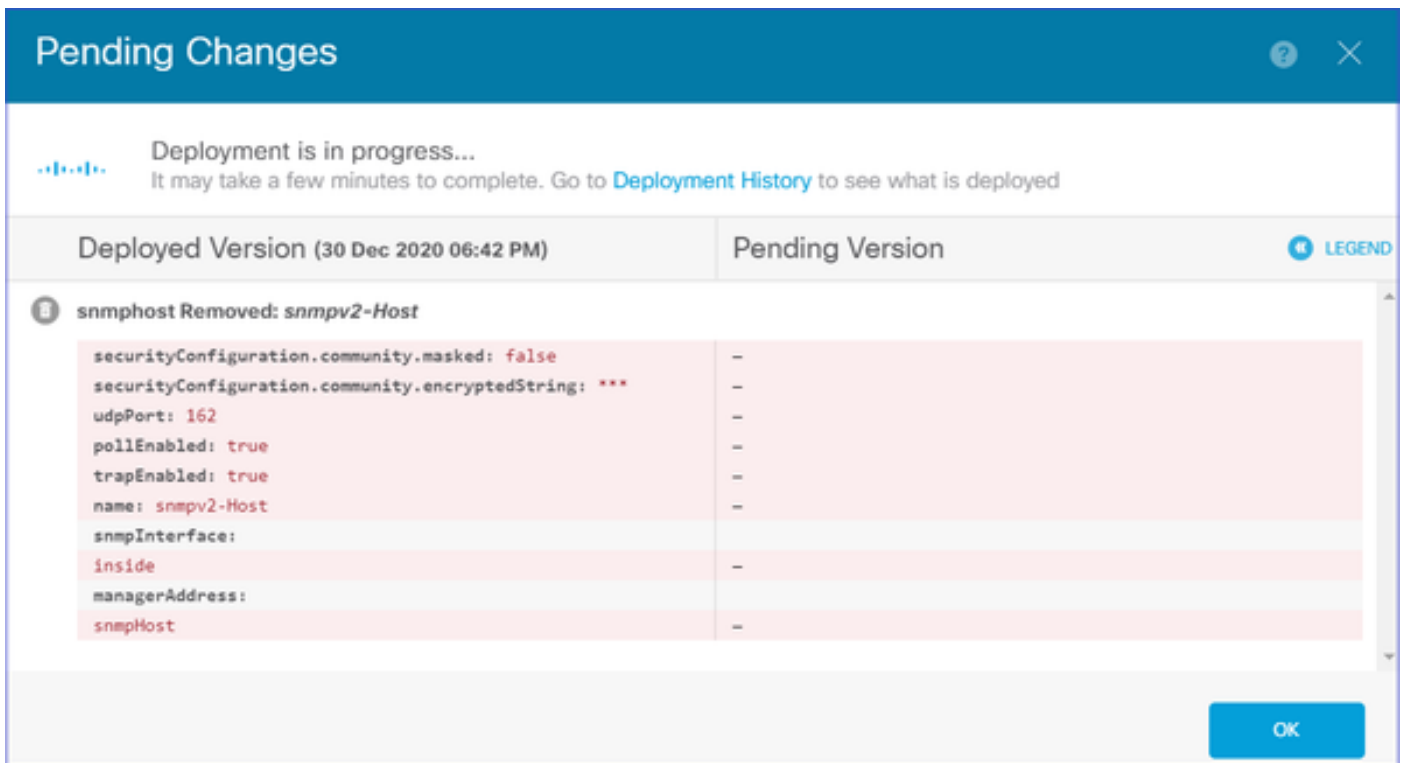


The screenshot shows the API response details. The 'Response Code' is 400. The 'Response Headers' are listed in a JSON object:

```
{  
  "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"  
}
```

Etapa 3.

Implante a alteração:



A implantação remove as informações do host:

```
<#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 *****
```

snmpwalk para v2c falha:

```
<#root>
```

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

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

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

Para v3, você deve excluir os objetos nesta ordem.

1. Host SNMP (o código de retorno bem-sucedido é 204)


```
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
```

teste snmpwalk

<#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
...
```

Verificação 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 para 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
```

Troubleshooting

Habilitar captura com rastreamento no firewall:

```
<#root>
```

```
FP1120-1#
```

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

Use a ferramenta snmpwalk e verifique se você pode ver os pacotes:

```
<#root>
```

FP1120-1#

show capture

capture CAPI type raw-data trace interface inside

[Capturing - 3137 bytes]

match udp any any eq snmp

O conteúdo da captura:

<#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 |

Verifique se os contadores de estatísticas do servidor SNMP mostram solicitações e respostas SNMP Get ou Get-next:

<#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

Rastreie um pacote de entrada. O pacote é UN-NAT para a interface NLP interna:

<#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

A regra NAT é implantada automaticamente como parte da configuração SNMP:

<#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

Na porta de back-end, o UDP 4161 escuta o tráfego SNMP:


```
<#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 :::*
```

Em um caso de configuração incorreta/incompleta, o pacote SNMP de entrada é descartado, já que não há fase UN-NAT:

```
<#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

Os syslogs de FTD LINA mostram que o pacote de entrada é descartado:

<#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.

Perguntas e respostas

P. Posso usar a interface de gerenciamento FTD para enviar mensagens SNMP?

Não, não há suporte para isso no momento.

Defeito de aprimoramento relacionado:

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

Informações Relacionadas

- [Guia de configuração do Cisco Firepower Threat Defense para Firepower Device Manager, versão 6.7](#)
- [Guia da API REST do Cisco Firepower Threat Defense](#)
- [Notas de versão do Cisco Firepower, versão 6.7.0](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.