Configure SNMP on Firepower NGFW Appliances

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Chassis (FXOS) SNMP on FPR4100/FPR9300
Configure FXOS SNMPv1/v2c via GUI
Configure FXOS SNMPv1/v2c via Command Line Interface (CLI)
Configure FXOS SNMPv3 via GUI
Configure FXOS SNMPv3 via CLI
FTD (LINA) SNMP on FPR4100/FPR9300
Configure LINA SNMPv2c
Configure LINA SNMPv3
SNMP in FPR2100
Chassis (FXOS) SNMP on FPR2100
Configure FXOS SNMPv1/v2c
Configure FXOS SNMPv3
FTD (LINA) SNMP on FPR2100
Verify
Verify FXOS SNMP for FPR4100/FPR9300
FXOS SNMPv2c Verifications
FXOS SNMPv3 Verifications
Verify FXOS SNMP for FPR2100
FXOS SNMPv2 Verifications
FXOS SNMPv3 Verifications
Verify FTD SNMP
Allow SNMP Traffic to FXOS on FPR4100/FPR9300
Configure Global Access-list via GUI
Configure Global Access-list via CLI
Verification
Use the OID Object Navigator
Related information

Introduction

This document describes how to configure Simple Network Management Protocol (SNMP) on the Next Generation Firewall (NGFW) Firepower Threat Defense (FTD) appliances.
Prerequisites

Requirements

This document requires basic knowledge of the SNMP protocol.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Firepower NGFW appliances can be split into 2 major subsystems:

- The Firepower Extensible Operative System (FX-OS) which controls the chassis hardware.
- The Firepower Threat Defense (FTD) which runs within the module.

FTD is a unified software which consists of 2 main engines, the Snort engine and the LINA engine. The current SNMP engine of the FTD derives from the classic ASA and it has visibility to the LINA-related features.

FX-OS and FTD have independent control planes and for monitoring purposes, they have different SNMP engines. Each of the SNMP engines provides different information and you might be interested in monitoring both for a more comprehensive view of the device status.

System-wide monitoring via SNMP over the FTD Management interface which includes both LINA and Snort information is not possible (Enhancement CSCvd12321).

From a hardware point of view, there are currently two major architectures for the Firepower NGFW appliances: the Firepower 2100 series and the Firepower 4100/9300 series.

Firepower 4100/9300 devices have a dedicated interface for the device management and this is the source and destination for the SNMP traffic addressed to the FXOS subsystem. On the other hand, the FTD application uses a LINA interface (data and/or diagnostic) for the SNMP configuration.
The SNMP engine on Firepower 2100 appliances uses the FTD management interface and IP. The appliance itself bridges the SNMP traffic received on this interface and forwards it to the FXOS software.

**Configure**

**Chassis (FXOS) SNMP on FPR4100/FPR9300**
Configure FXOS SNMPv1/v2c via GUI

Step 1. Open the Firepower Chassis Manager (FCM) UI and navigate to Platform Settings > SNMP tab. Check the SNMP enable box, specify the Community string to use on SNMP requests and Save.
Step 2. Configure the SNMP traps destination server.

**Note:** If the Community/Username field is already set, the text to the right of the empty field reads **Set: Yes.** If the Community/Username field is not yet populated with a value, the text to the right of the empty field reads **Set: No.**

![Add SNMP Trap](image)

**Note:** The community values for queries and trap host are independent and can be different.

The host can be defined as IP address or by name. Select **OK** and the configuration of the SNMP Trap server is saved automatically. There is no need to select the save button from the SNMP main page. The same occurs when you delete a host.

**Configure FXOS SNMPv1/v2c via Command Line Interface (CLI)**

```bash
ksec-fpr9k-1-A# scope monitoring  
ksec-fpr9k-1-A /monitoring# enable snmp  
ksec-fpr9k-1-A /monitoring* # set snmp community
Enter a snmp community:  
ksec-fpr9k-1-A /monitoring* # enter snmp-trap 192.168.10.100
ksec-fpr9k-1-A /monitoring/snmp-trap* # set community
Community:  
ksec-fpr9k-1-A /monitoring/snmp-trap* # set version v2c
ksec-fpr9k-1-A /monitoring/snmp-trap* # set notificationtype traps
ksec-fpr9k-1-A /monitoring/snmp-trap* # set port 162
ksec-fpr9k-1-A /monitoring/snmp-trap* # exit
ksec-fpr9k-1-A /monitoring* # commit-buffer
```
Configure FXOS SNMPv3 via GUI

Step 1. Open FCM and navigate to **Platform Settings > SNMP** tab.

Step 2. For SNMP v3 there is no need to set any community string in the upper section. Every user created is able to successfully run queries to the FXOS SNMP engine. The first step is to enable SNMP in the platform. Once done you can create the users and destination trap host. Both, SNMP Users and SNMP Trap hosts are saved automatically.

Step 3. As shown in the image, add the SNMP user. The authentication type is always SHA but you can use AES or DES for encryption.
Step 4. Add the SNMP trap host, as shown in the image.

Configure FXOS SNMPv3 via CLI
FTD (LINA) SNMP on FPR4100/FPR9300

Configure LINA SNMPv2c

Step 1. On FMC UI, navigate to Devices > Platform Settings > SNMP. Check the option ‘Enable SNMP Servers’ and configure the SNMPv2 settings as follows.
Step 2. On Hosts tab select the Add button and specify the SNMP server settings.
Configure LINA SNMPv3
Step 1. On FMC UI navigate to **Devices > Platform Settings > SNMP**. Check the option **Enable SNMP Servers** and configure the SNMPv3 User and Host.

Step 2. Configure the host also to receive traps.
Step 3. The traps that you want to receive can be selected under **SNMP Traps** Section.

**SNMP in FPR2100**

On FPR2100 systems, there is no FCM. The only way to configure SNMP is via FMC.

**Chassis (FXOS) SNMP on FPR2100**
Configure FXOS SNMPv1/v2c

Open FMC UI and navigate to Choose Devices > Device Management. Select the device and select SNMP.
Configure FXOS SNMPv3

Open FMC UI and navigate to Choose Devices > Device Management. Select the device and select SNMP.
FTD (LINA) SNMP on FPR2100

LINA FTD SNMP configuration on FTD FPR2100 appliance is identical to an FTD on Firepower 4100 or 9300 appliance.
Verify

Verify FXOS SNMP for FPR4100/FPR9300

FXOS SNMPv2c Verifications

CLI configuration verification

```
  ksec-fpr9k-1-A /monitoring # show snmp
  Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact:
    Sys Location:
  ksec-fpr9k-1-A /monitoring # show snmp-trap

  SNMP Trap                Port     Community  Version V3 Privilege Notification Type
  ------------------------ -------- ---------- ------- ------------ -----------------
  192.168.10.100           162                 V2c     Noauth       Traps

  From the FXOS mode.

  ksec-fpr9k-1-A(fxos)# show run snmp

  !Command: show running-config snmp
  !Time: Mon Oct 16 15:41:09 2017

  version 5.0(3)N2(4.21)
  snmp-server host 192.168.10.100 traps version 2c cisco456
  snmp-server enable traps callhome event-notify
  snmp-server enable traps callhome smtp-send-fail
  ... All traps will appear as enable ...
  snmp-server enable traps flexlink ifStatusChange
```
snmp-server context mgmt vrf management
snmp-server community cisco123 group network-operator

ksec-fpr9k-1-A(fxos)# show snmp host
-------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Host</th>
<th>Port</th>
<th>Version</th>
<th>Level</th>
<th>Type</th>
<th>SecName</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.100</td>
<td>162</td>
<td>v2c</td>
<td>noauth</td>
<td>trap</td>
<td>cisco456</td>
</tr>
</tbody>
</table>
-------------------------------------------------------------------

ksec-fpr9k-1-A(fxos)# show snmp
Community            Group / Access      context    acl_filter
---------            --------------      -------    ----------
cisco123              network-operator

Test SNMP Requests:

Perform an SNMP request from a valid host.

root@kali:~# snmpgetnext -v2c -ccisco123 10.62.148.35 1.3.6.1.2.1.2.1.2.1.2.83886080 = STRING: "mgmt0"

Confirm Trap Generation:

You can use flap an interface with ethanalyzer enabled to confirm that SNMP traps are being generated and sent to the trap hosts defined

ksec-fpr9k-1-A(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 162"
Capturing on eth0
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0
2017-11-17 09:01:35.954624 10.62.148.35 --> 192.168.10.100 SNMP snmpv2-Trap 2017-11-17
09:01:36.054511 10.62.148.35 --> 192.168.10.100 SNMP snmpv2-Trap

Warning: Flapping an interface will cause a traffic outage. Do this test only in a lab environment or during a maintenance window

FXOS SNMPv3 Verifications

Step 1. Open FCM UI Platform Settings > SNMP > User shows if there is any password and privacy password configured.
Step 2. In CLI you can verify the SNMP configuration under scope **monitoring**.

```bash
ksec-fpr9k-1-A /monitoring # show snmp
Name: snmp
   Admin State: Enabled
   Port: 161
   Is Community Set: No
   Sys Contact:
   Sys Location:

ksec-fpr9k-1-A /monitoring # show snmp-user
SNMPv3 User:
   Name                     Authentication type
   ------------------------ -------------------
   user1                     Sha

ksec-fpr9k-1-A /monitoring # show snmp-user detail
SNMPv3 User:
   Name: user1
   Authentication type: Sha
   Password: ****
   Privacy password: ****
   Use AES-128: Yes

ksec-fpr9k-1-A /monitoring # show snmp-trap
SNMP Trap:
   SNMP Trap                Port     Community  Version V3 Privilege Notification Type
   ------------------------ -------- ---------- ------- ------------ -------------------
   192.168.10.100 162 V3 Priv Traps
```

Step 3. Under FXOS mode you can expand the SNMP configuration and details.

```bash
ksec-fpr9k-1-A(fxos)# show running-config snmp all
```
snmp-server user user1 network-operator auth sha 0x022957ee4690a01f910f1103433e4b7b07db5fc priv aes-128 0x022957ee4690a01f910f1103433e4b7b07db5fc localizedkey
snmp-server host 192.168.10.100 traps version 3 priv user1

ksec-fpr9k-1-A(fxos)# show snmp user

<table>
<thead>
<tr>
<th>User</th>
<th>Auth</th>
<th>Priv(enforce)</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>sha</td>
<td>aes-128(yes)</td>
<td>network-operator</td>
</tr>
</tbody>
</table>

NOTIFICATION TARGET USERS (configured for sending V3 Inform)

ksec-fpr9k-1-A(fxos)# show snmp host

<table>
<thead>
<tr>
<th>Host</th>
<th>Port</th>
<th>Version</th>
<th>Level</th>
<th>Type</th>
<th>SecName</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.48.26.190</td>
<td>162</td>
<td>v3</td>
<td>priv</td>
<td>trap</td>
<td>user1</td>
</tr>
</tbody>
</table>

Test SNMP Requests:

You can verify the configuration and do an SNMP request from any device with SNMP capabilities.

```
root@kali:~# snmpgetnext -v3 -u user1 -A zaq12wsx -a SHA -X zaq12wsx -x AES -l Auth Priv 10.62.148.35 1.3.6.1.2.1.2.2.1.2.83886080 = STRING: "mgmt0"
```

To check how the SNMP request is processed you can use SNMP debug.

```
ksec-fpr9k-1-A(fxos)# debug snmp pkt-dump
```

Caution: A debug can impact the device performance.

Verify FXOS SNMP for FPR2100

FXOS SNMPv2 Verifications

Check the configuration via CLI

```
FP2110-4 /monitoring # show snmp
Name: snmp
```
Admin State: Enabled
Port: 161
Is Community Set: Yes
Sys Contact: Sys Location:

FP2110-4 /monitoring # show snmp-trap

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Port</th>
<th>Version</th>
<th>Privilege</th>
<th>Notification</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.48.26.190</td>
<td>162</td>
<td>V2c</td>
<td>Noauth</td>
<td>Traps</td>
<td></td>
</tr>
</tbody>
</table>

Confirm the SNMP Behavior:

You can verify that you are able to poll the FXOS and send an SNMP request from a host or any device with SNMP capabilities.

```
root@kali:~# snmpgetnext -v2c -ccisco123 10.62.148.180 1.3.6.1.2.1.2.2.1.2 iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"
```

Use the `capture-traffic` command to see the SNMP request and response.

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - management0

Selection? 0

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: udp port 161
H5_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes
  interfaces.ifTable.ifEntry.ifDescr
  interfaces.ifTable.ifEntry.ifDescr.1=|snmp|

^C
Caught interrupt signal

Exiting.

2 packets captured
2 packets received by filter
0 packets dropped by kernel

FXOS SNMPv3 Verifications

Check the configuration via CLI.

FP2110-4 /monitoring # show snmp
Name: snmp
  Admin State: Enabled
  Port: 161
  Is Community Set: No
Sys Contact:  
Sys Location:  
FP2110-4 /monitoring # show snmp-user detail

SNMPv3 User:  
  Name: user1  
  Authentication type: Sha  
  Password: ****  
  Privacy password: ****  
  Use AES-128: Yes  
FP2110-4 /monitoring # show snmp-trap detail

SNMP Trap:  
  Notification Type: Traps

Confirm the SNMP Behavior:

Send an SNMP request to verify that you are able to poll the FXOS.

```
root@kali:~# snmpgetnext -v 3 -u user1 -A Zaq12wsx! -a SHA -X Zaq12wsx! -x AES -l AuthPriv 10.62.148.180 1.3.6.1.2.1.2.2.1.2
iso.3.6.1.2.1.2.2.2.1 = STRING: "lo"
```

Additionally, you can capture the request.

```
> capture-traffic
```

Please choose domain to capture traffic from:

```
  0 - management0
```

Selection? 0

Please specify tcpdump options desired.  
(or enter '?' for a list of supported options)

Options: **udp port 161**  
H3_PACKET_BUFFER_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes  

**Verify FTD SNMP**

To verify the FTD LINA SNMP configuration.

```
Firepower-module1# show run snmp-server
snmp-server host OUTSIDE3 10.62.148.75 community ***** version 2c no snmp-server location no snmp-server contact snmp-server community *****
```

Additional verification.

```
Firepower-module1# show snmp-server host
host ip = 10.62.148.75, interface = OUTSIDE3 poll community ***** version 2c
```

From the SNMP Server CLI run a snmpwalk.
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 6.2.3.1 (Build 43), ASA
Version 9.9(2)4
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2313
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8350600) 23:11:46.00
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: Firepower-module1
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 4
IF-MIB::ifNumber.0 = INTEGER: 10
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.10 = INTEGER: 10
IF-MIB::ifIndex.11 = INTEGER: 11
...
Verification of the SNMP traffic statistics.

Firepower-module1# show snmp-server statistics
1899 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
1899 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
1899 Get-next PDUs
0 Get-bulk PDUs
0 Set-request PDUs (Not supported)
1904 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
1899 Response PDUs
5 Trap PDUs

Allow SNMP Traffic to FXOS on FPR4100/FPR9300

FXOS configuration on FPR4100/9300 can restrict SNMP access per source IP address. The Access List configuration section defines which networks/hosts are able to reach the device via SSH, HTTPS or SNMP. You need to ensure that SNMP queries from your SNMP server are allowed.

Configure Global Access-list via GUI
Configure Global Access-list via CLI

ksec-fpr9k-1-A# scope system
ksec-fpr9k-1-A /system # scope services
ksec-fpr9k-1-A /system/services # enter ip-block 0.0.0.0 0 snmp
ksec-fpr9k-1-A /system/services/ip-block* # commit-buffer

Verification

ksec-fpr9k-1-A /system/services # show ip-block

Permitted IP Block:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Prefix Length</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td>https</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td>snmp</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td>ssh</td>
</tr>
</tbody>
</table>

Use the OID Object Navigator

Cisco SNMP Object Navigator is an online tool where you can translate the different OIDs and get a short description.
Use the command `show snmp-server oid` from the FTD LINA CLI to retrieve the whole list of LINA OIDs that can be polled.

```
> system support diagnostic-cli
firepower# show snmp-server oid
---------------------------------------------------------------------
[0] 1.3.6.1.2.1.1.1. sysDescr [1] 1.3.6.1.2.1.1.2. sysObjectID [2] 1.3.6.1.2.1.1.3.
sysLocation [6] 1.3.6.1.2.1.1.7. sysServices [7] 1.3.6.1.2.1.1.8. sysORLastChange
... [1081] 1.3.6.1.6.3.16.1.4.1.9. vacmAccessStatus [1082] 1.3.6.1.6.3.16.1.5.1.
vacmViewSpinLock [1083] 1.3.6.1.6.3.16.1.5.2.1.3. vacmViewTreeFamilyMask [1084]
1.3.6.1.6.3.16.1.5.2.1.4. vacmViewTreeFamilyType [1085] 1.3.6.1.6.3.16.1.5.2.1.5.
vacmViewTreeFamilyStorageType [1086] 1.3.6.1.6.3.16.1.5.2.1.6. vacmViewTreeFamilyStatus -------
--------------------------------------------------------------------- firepower#
```

**Note:** The command is hidden.

**Related information**

- [Configure SNMP for Threat Defense](#)
- [Configuring SNMP on FXOS (UI)](#)
- [Technical Support & Documentation - Cisco Systems](#)