Creating Cacti FortiGate SNMP Graphs
Cacti 0.8.7.b

Corporate Headquarters
1090 Kifer Road,
Sunnyvale, Ca 94086
USA
http://www.fortinet.com
Tel: +1 408 235 7700
Fax: +1 408 235 7737
Documentation Written By: Minh Ly (Consulting Systems Engineer)

Some elements of the FortiGate configuration section were borrowed from an unknown writer on the Fortinet Knowledge Base.
Contents

About This Guide ........................................................................................................................................... xxi

Objectives.................................................................................................................................................. xxii
Related Publications................................................................................................................................... xxii
Intended Audience..................................................................................................................................... xxii
Organization............................................................................................................................................. xxxi

Part 1: Introduction......................................................................................................................................

Chapter 1: Overview.............................................................................................................................. 1-1
    Enabling SNMP on the FortiGate ........................................................................................................... 1-3
    Installing Cacti in Ubuntu .................................................................................................................... 1-6

Part 2: SNMP Data....................................................................................................................................

Chapter 2: Gathering SNMP Data ........................................................................................................... 2-1
    Installing the MIB File .......................................................................................................................... 2-2
    Obtaining OIDs ...................................................................................................................................... 2-3
    Using a MIB Browser ............................................................................................................................ 2-4

Chapter 3: Generating Graphs .................................................................................................................. 3-1
    Graphing Interface Traffic ................................................................................................................... 3-2
    Creating Data Templates ...................................................................................................................... 3-2
    Creating Graph Templates ................................................................................................................... 3-6
    Creating Host Templates ...................................................................................................................... 3-9
    Applying Host Templates to Devices ................................................................................................... 3-10
    Graphing Quick and Easy .................................................................................................................... 3-15
This preface includes the following sections:

- Objectives
- Related Publications
- Intended Audiences
- Organization

Objectives

This document describes the tasks and commands used to install Cacti, obtain SNMP data and create graphs on Ubuntu 7.10 for the purpose of monitoring FortiGate firewalls.

Related Publications

Refer to http://www.cacti.net and http://www.ubuntu.com for additional Cacti and Ubuntu resources. This document will not go into Cacti details. Of course as always, use Google for research as if you have the plague and your life depended on the answers.

Intended Audience

This publication is intended for engineering, SEs, support and training personnel experienced in Linux type OS administration and Fortinet FortiGate firewalls.
Organization

This guide is organized as follows:

- Part 1, “Cacti Installation”
  Describes how to install Cacti in the simplest form

- Part 2, “Generating Graphs”
  Describes all the necessary steps to generating SNMP graphs
This part provides an overview of installing Cacti and enabling SNMP on for a FortiGate firewall.

This part consists of the following chapters:

- Chapter 1, “Overview”
Overview

In the context of this document, SNMP graphs are created to show various historical usage statistics for a FortiGate firewall running at least the MR6 firmware build. Older versions may be used, but not all SNMP data shown in this document will be retrievable. It is the intention of this document to simplify the process of installing Cacti and generating SNMP graphs on an Ubuntu 7.10 operating system. Please refer to the applications website for a more manual approach of installation.

Some example graphs that can be generated after reading this document are shown below.
Enabling SNMP on the FortiGate

You must first configure the FortiGate unit to allow SNMP polling. There are three steps to enabling SNMP polling:

• Enable the SNMP agent
• Create a new Community
• Activate SNMP on the interface.

Enable the SNMP agent

To configure the FortiGate unit

1. Go to System > Config > SNMP v1/v2c.
2. Select Enable for the SNMP Agent.
3. Enter a Description, Location and Contact information.
4. Select Apply.

Figure 1: Enabling the SNMP Agent
Creating a new Community

To create a new Community

1. Go to **System > Config > SNMP v1/v2c**.
2. Select Create New.
3. Enter a Community Name.
   Leave the remainder of the settings as the default. To make a secure community, specify IP addresses that will be allowed to pool the FortiGate unit with SNMP. You can also define which interface the IP addresses will be allowed to communicate with the FortiGate unit.
4. To do this, enter the IP addresses, select the Interface and select Add.
5. Select OK.

Figure 2: Creating a Community
Activating SNMP on the Interface

If SNMP is allowed from only one Interface, you need to enable SNMP for the interface.

To activate SNMP

1. Go to System > Network > Interface.
2. For the interface allowing SNMP traffic, select Edit.
4. Select OK.

Figure 3: Activating SNMP for the Internal Interface
Installing Cacti in Ubuntu

In general, there’s only one command needed to install Cacti unless customization is required. Accept all the default values. Please refer to the Cacti website to verify hardware and additional software requirements. Cacti requires the Apache web server to already be installed.

root@monitor:/# sudo aptitude install cacti

This is it, a whole chapter dedicated to one line!
This part provides information on MIB files and the commands used to gather data from them.

This part consists of the following chapters:

- Chapter 2, “Gathering SNMP Data”
- Chapter 3, “Generating Graphs”
This chapter describes the tasks and commands used to gather SNMP data so that Cacti can successfully generate graphs for a particular object identifier within the MIB. It is expected that the reader has some knowledge of MIB files.

Installing the MIB File

FortiGate MIB files are available from the Fortinet Technical Support web site at http://support.fortinet.com found under firmware images.

The MIB file used in this documentation is within the MR6 firmware branch.

Download the MIB file and place it in the /usr/share/snmp/mibs directory. This is the default directory where all MIB files are stored.

Look inside the MIB file and keep the file name the same as the ::= BEGIN line. The line is usually located within the first few lines of the MIB file. Matching the file name and the module name is not a must but it is a good idea to avoid confusion later. Add .txt to the end of the file name to maintain commonality with the rest of the MIBs in the same directory.

Some people rename the MIB files to something completely different and run SNMP commands against the file name instead of the ::= BEGIN module name. This will cause errors.

For example, my MIB file name is FORTINET-300-MIB-20080414.txt however looking inside the MIB the name loaded is FORTINET-300-MIB.

To see the actual name of the MIB module that is loaded into the system, look inside the .index file located under /usr/share/snmp/mibs. It will show the module name corresponding to the file name.
Obtaining OIDs

There are two commands commonly used in SNMP: snmptranslate and snmpwalk.

Looking inside the MIB there are different objects that can be queried in the FortiGate to produce an understandable value. For example fnSysVersion displays the firmware version information.

```
fnSysVersion OBJECT-TYPE
SYNTAX DisplayString ( SIZE ( 0 .. 128 ) )
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Firmware version of the device"
::= { fnSystem 3 }
```

The snmptranslate command can be run against the MIB file to produce an Object Identifier number that can then be used to query the FortiGate.

```
root@monitor:/usr/share/snmp/mibs# snmptranslate -m FORTINET-300-MIB -IR -On fnSysVersion .1.3.6.1.4.1.12356.1.3
```

The “-m” attribute specifies the MIB module name to use for the translation to get the OID.

Now that the OID is found, it can be used against a FortiGate to produce an understandable value. To do so use the snmpwalk command.

```
root@monitor:/usr/share/snmp/mibs# snmpwalk -v 2c -c public 10.69.69.1 .1.3.6.1.4.1.12356.1.3
```

The “-v” attribute specifics the SNMP version and “-c” attribute specifies the community name to be used.

Querying the FortiGate interface resulted in a model name and firmware version number. The snmptranslate command can be used against other objects to obtain their OIDs.
Using a MIB Browser

A MIB browser generally contains the same information as using the commands snmptranslate and snmpwalk. However, a MIB browser organizes the data into an easy to understand GUI structure. Opening the FortiGate MIB file and selecting fnSysVersion immediately displays the OID. Search for OIDs is made easier through the use of a MIB browser.

![MIB Browser Screenshot](image-url)
This chapter describes the tasks and commands used to navigate Cacti in order to generate SNMP graphs.
Graphing Interface Traffic

As a note, by default Cacti natively contains the ability to poll FortiGate interface statistics. No additional work has to be done except to place the ‘SNMP – Interface Statistics’ Data Query into a Host Template. This process will be shown in the following sections.

Creating Data Templates

Data templates are used to query the FortiGate to retrieve information relating to a particular OID. Be sure to have the OID information for objects ready during data template creation.

The following example illustrates how to create two data templates. One to show how many POP3 messages are being processed and another to show how many of the processed messages were flagged as SPAM. This will give an idea of the percentage of junk mail being downloaded.

To create Data Templates for each OID, log into cacti click on ‘Data Templates’ located in the template section and click ‘Add’. Fill in the values as shown below and ‘create’.
Once the ‘create’ button is pressed, the ‘Custom Data’ section will appear. Input the OID for the number of POP3 messages processed. Looking at the MIB browser, the OID can be found under the ‘fnApplications/fnAppProxyPOP3/fnApPOP3StatsEntry’. The OIDs we are looking for are the ones for ‘fnApPOP3ReqProcessed’ and ‘fnApPOP3SpamDetected’.

To verify the OID references the correct data, perform a snmpwalk on FortiGate to retrieve the value.

```
snmpwalk -v 2c -c public 10.69.69.1 .1.3.6.1.4.1.12356.17.102.3.1.2
SNMPv2-SMI::enterprises.12356.17.102.3.1.2.1 = Counter32: 1229
```

Notice that the snmpwalk came back with an OID of 12356.17.102.3.1.2.1. The extra trailing ‘1’ would be the OID that should be put into the Data Template Custom Data section.
‘Save’ and click on ‘Add’ again to create a POP3 SPAM data template. Follow the preceding procedures to retrieve the OID. Repeat the data template creation process for other types of queries such as CPU and sessions.
Creating Graph Templates

Graph Templates generate historical data relating to a particular OID. The following example illustrates how to create a graph that charts two Data Templates into one graph.

Click on ‘Graph Templates’ located in the template section then click ‘Add’. Fill in the values as shown below and click ‘create’.

<table>
<thead>
<tr>
<th>Template [edit: Fortigate - POP3]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Graph Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
</tr>
<tr>
<td>Image Format</td>
</tr>
<tr>
<td>Height</td>
</tr>
<tr>
<td>Width</td>
</tr>
<tr>
<td>Auto Scale</td>
</tr>
<tr>
<td>Auto Scale Options</td>
</tr>
<tr>
<td>Logarithmic Auto Scaling (--logarithmic)</td>
</tr>
<tr>
<td>Rigid Boundaries Mode (--rigid)</td>
</tr>
<tr>
<td>Auto Padding</td>
</tr>
<tr>
<td>Allow Graph Export</td>
</tr>
<tr>
<td>Upper Limit</td>
</tr>
<tr>
<td>Lower Limit</td>
</tr>
<tr>
<td>Basic Value</td>
</tr>
<tr>
<td>Unit Grid Value</td>
</tr>
<tr>
<td>Unit Exponent Value</td>
</tr>
<tr>
<td>Vertical Label</td>
</tr>
</tbody>
</table>
The ‘Graph Template Items’ and ‘Graph Item Inputs’ section will appear. Click ‘Add’ in the Graph Template Items section. Select the previously created Data Template that queries the number of POP3 messages processed and fill in the data as shown below. This section sets the type of graph and labels. For more information refer to the Cacti documentation.
Add a second Graph Template item to complete the graph settings of POP3 messages processed.

Add a third and fourth Graph Template item to complete the graph settings for the number of SPAM messages.
### Generating Graphs

#### Graph Template Items [edit graph: Fortigate - POP3]

<table>
<thead>
<tr>
<th>Data Source [Field Not Templated]</th>
<th>Fortigate - POP3SpamCount - (POP3SpamCount)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>FF0000</td>
</tr>
<tr>
<td>Graph Item Type</td>
<td>AREA</td>
</tr>
<tr>
<td>Consolidation Function</td>
<td>AVERAGE</td>
</tr>
<tr>
<td>CDEF Function</td>
<td>None</td>
</tr>
<tr>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>GPRINT Type</td>
<td>Normal</td>
</tr>
<tr>
<td>Text Format</td>
<td>SPAM</td>
</tr>
<tr>
<td>Insert Hard Return</td>
<td>☑ Insert Hard Return</td>
</tr>
<tr>
<td>Sequence</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Graph Template Items [edit graph: Fortigate - POP3]

<table>
<thead>
<tr>
<th>Data Source [Field Not Templated]</th>
<th>Fortigate - POP3SpamCount - (POP3SpamCount)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>None</td>
</tr>
<tr>
<td>Graph Item Type</td>
<td>GPRINT</td>
</tr>
<tr>
<td>Consolidation Function</td>
<td>LAST</td>
</tr>
<tr>
<td>CDEF Function</td>
<td>None</td>
</tr>
<tr>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>GPRINT Type</td>
<td>Normal</td>
</tr>
<tr>
<td>Text Format</td>
<td></td>
</tr>
<tr>
<td>Insert Hard Return</td>
<td>☑ Insert Hard Return</td>
</tr>
<tr>
<td>Sequence</td>
<td></td>
</tr>
</tbody>
</table>
Creating Host Templates

Graph templates contain data templates and hosts templates contain graph templates. Once created, hosts templates can be applied to similar types of devices. This makes the process of adding multiple devices easy.

Click on ‘Host Templates’ located in the template section and click ‘Add’. The following illustration shows that there are a number of Graph Templates already created. One of the graph templates shown is ‘FortiGate – POP3’. Associate all of the FortiGate graph templates to this host template. Previously, I spoke about Cacti having a native ability to graph interface statistics without creating a data template. This is done by adding ‘SNMP – Interface Statistics’ to the ‘Associated Data Queries’ section. Click ‘save’ to complete the host template.
Applying Host Templates to Devices

Host templates are applied devices by selecting the proper host template and inputting the SNMP Community string. To add a device, click on ‘Devices’ in the ‘Management’ section and click ‘Add’.

### Devices [new]

- **Description**: FG60B-Minh
- **Hostname**: 10.69.69.1
- **Host Template**: FortiGate MR6
- **SNMP Community**: public
- **SNMP Version**: Version 2c
- **SNMP Port**: 161
- **SNMP Timeout**: 500 ms

[Create button]
Once the create button is pressed, Cacti will query the FortiGate. A successful query will display the System name and Uptime, a bad query will display SNMP error. Should an error occur, verify that the IP address and SNMP Community is correct. Make sure that SNMP is enabled on the FortiGate and that the IP address of the Cacti server has access to the FortiGate.
Notice that each one of the Associated Graph Templates Status is shown as not being graphed. Click on ‘Create Graphs for this Host’ and select the graphs to be created. Once the graphs are created click on the ‘graphs’ tab to see the data being charted. Note that you must wait for two polling cycles before the graphs are generated and charted. This will take 10 minutes as polling takes place every 5 minutes.
Here are more graph examples.
Generating Graphs
Graphing Quick and Easy

Of course there's a quick way to create all those nice graphs since I've done all the work for you. Look for the Cacti-Fortinet-MR6-Template.xml on the FortiTech server, install Cacti and import the template then apply it to a device.