finjan®
Vital Security™
securing your web

Bandwidth Monitoring

December 2008

Copyright

For additional information, please visit www.finjan.com or contact one of our regional offices:

USA: San Jose 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com	**Europe: UK** 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
Israel/Asia Pacific Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com	**Europe: Germany** Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
For more information: Email: support@finjan.com Internet: www.finjan.com	**Europe: Netherlands** Printerweg 56 3821 AD Amersfoort, Netherlands Tel: +31 334 543 555 Fax: +31 334 543 550 salesne@finjan.com

Catalog name: Bandwidth Monitoring 1.0

1. Monitoring Bandwidth: Open Source Solutions

One of the most important aspects of designing a network correctly is by performing analysis of future network usage prior to the installation of the hardware. This process, known as sizing, indicates the amount of bandwidth potentially consumed by network clients. The derived numbers are especially significant when determining the bandwidth of the internet connection. Another aspect of network design is the possible bottlenecks caused on the users end by hardware positioned in the path between the client and the internet gateway. This is especially true for appliances that perform heavy operations on internet traffic such as; traffic shapers, Antivirus boxes, and various traffic analyzers. The Vital Security appliance performs such operations and is therefore no exception.

But how may one cope with a sudden growth in the number of users or the ever increasing demand for more HTTP bandwidth? In order to predict future changes, the load on the various network components should be constantly monitored. This allows the network administrator to view the performance of his network as a whole and easily locate the weakest links. This practice is quite common on enterprise networks, but small and medium sized businesses often neglect this methodology primarily because it requires expensive proprietary software and trained personnel and does not justify the price for the SMB.

Recent maturing of various free and open source solutions proposes an interesting opportunity for the SMB. Deploying an open source monitoring infrastructure, via a combination of open source tools can be an inexpensive but still powerful solution. A free monitoring environment can be set up in minutes without any prior knowledge of Linux. No dedicated products need to be purchased and no additional personnel must be trained.

This document Refers to two tools in particular, **VMware Player** and **Cacti**. Please visit the VMware Player and Cacti websites to familiarize yourself with the products:

- **VMware Player** – A freely available tool for Microsoft Windows which allows running *Virtual Machines* or, in essence, complete operating systems in a window on your desktop. The advantage of the VMware Player is its ability to run images of operating systems preconfigured to perform certain tasks. These are called virtual appliances. http://www.vmware.com/products/player/
- **Cacti** – A Linux based network graphing solution with an HTTP web interface. http://www.cacti.net/

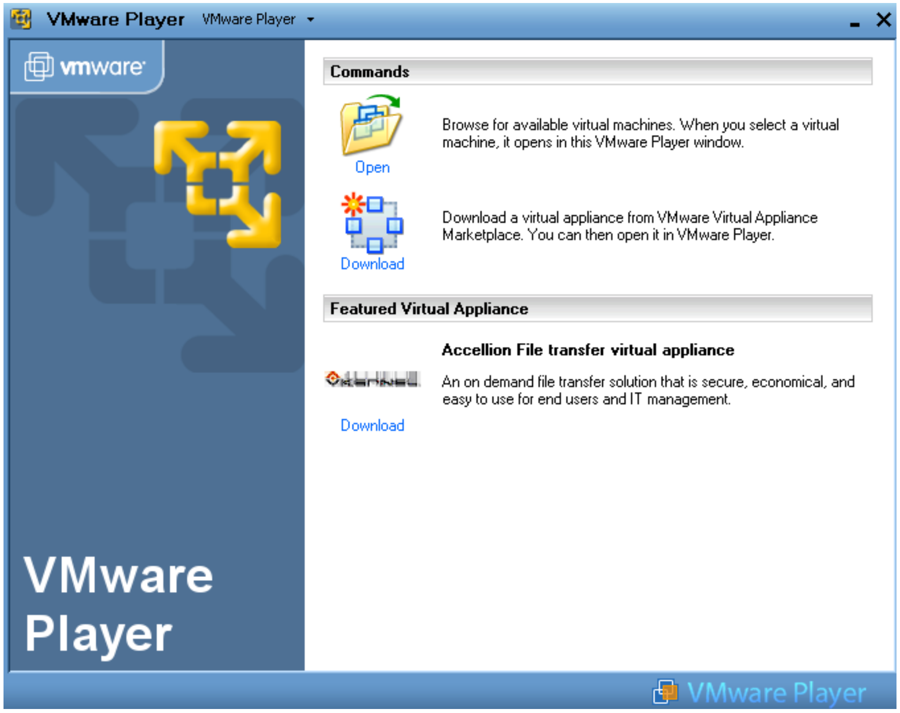
1.1 Installing the VMware Player

⇨ **To install the VMware Player on a company server:**

1. Download the latest release from: http://www.vmware.com/download/player/
2. Run setup.exe and follow the installation instructions.

   The virtual appliance employed for this demonstration is not CPU intensive, and therefore, any internal server with a network connection and a reasonable average load is usable.

   Note: 128MB of RAM is dedicated solely to the virtual appliance.
3. Open the VMware Player window.



Browse for available virtual machines. When you select a virtual machine, it opens in this VMware Player window.

Download a virtual appliance from VMware Virtual Appliance Marketplace. You can then open it in VMware Player.

Accellion File transfer virtual appliance

An on demand file transfer solution that is secure, economical, and easy to use for end users and IT management.

VMware player after installation

1.2 Installing Cacti Appliance

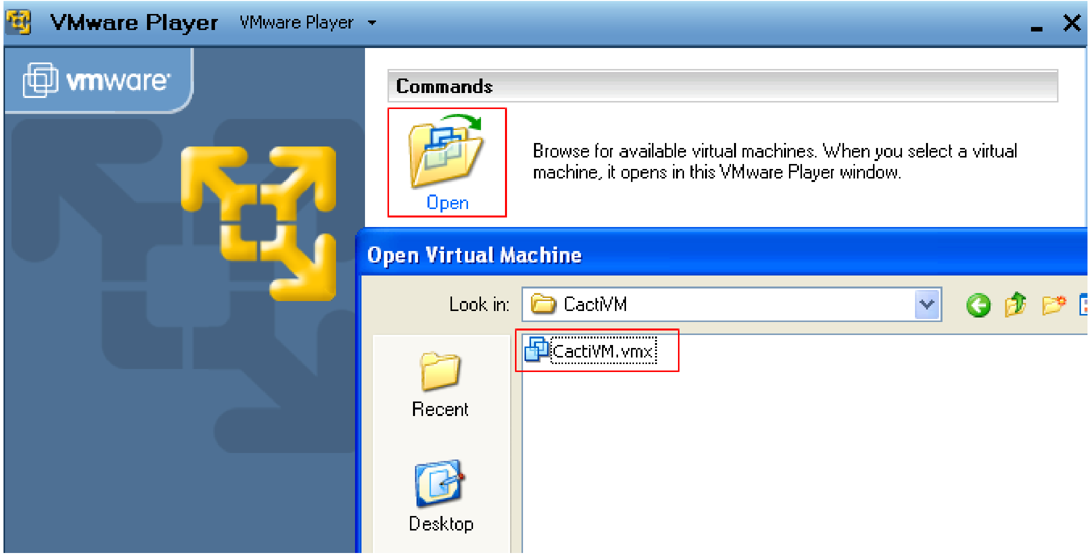
⇨ Download a Cacti virtual appliance:

There are many appliances from which to choose, and all easily downloadable. (Be aware of which are free and which are not)

For the purpose of this document, the following appliance has been chosen: http://www.cacti.net/downloads/packages/VMware/contrib/

This community based appliance relies on Debian Linux 3.1, Cacti 0.8.6g, and mySQL. Its biggest benefit is that it includes all the plug-ins from http://www.cactiusers.org and therefore supports many types of network equipment out of the box.

4. Extract the contents of the archive to **c:\cactivm\** in **VMware player** click open and locate **c:\cactivm\CactiVM.vmx**



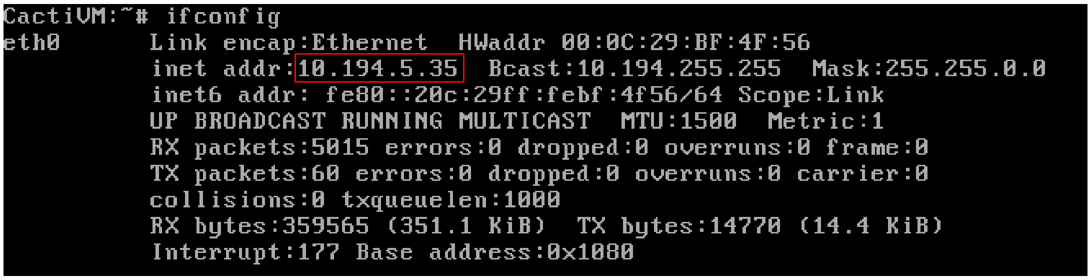
Browse for available virtual machines. When you select a virtual machine, it opens in this VMware Player window.

5. Wait for the virtual machine to boot and log-in with the following credentials:

   User*: root*

   Password*: cacti*

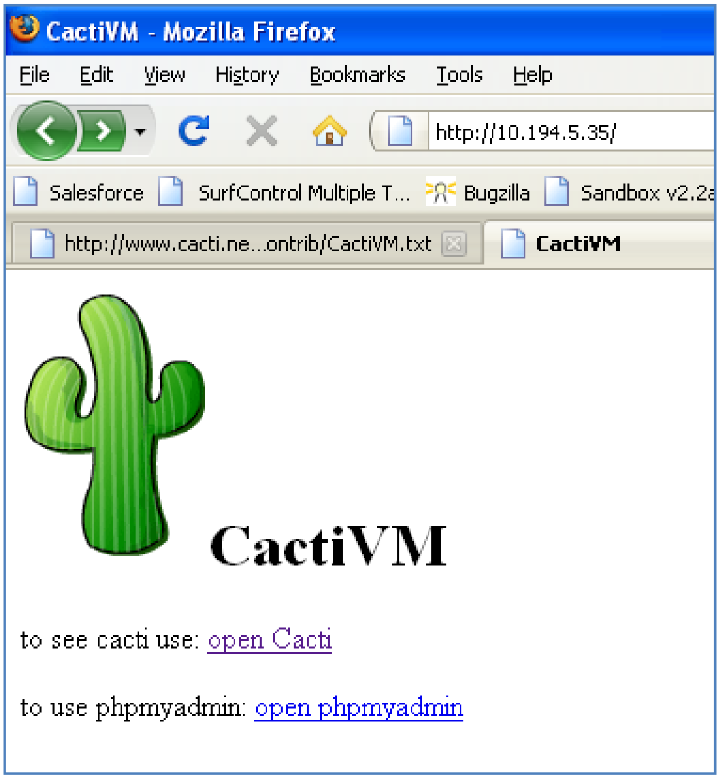
6. In the command prompt enter the command: *ifconfig*



```
CactiVM:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:BF:4F:56
          inet addr:10.194.5.35  Bcast:10.194.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20c:29ff:febf:4f56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5015 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:359565 (351.1 KiB)  TX bytes:14770 (14.4 KiB)
          Interrupt:177 Base address:0x1080
```

The output will show the IP address acquired from the DHCP. This is the address given to the virtual appliance.

7. Open this address in a web browser. The following will be presented:


CactiVM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://10.194.5.35/
Salesforce SurfControl Multiple T... Bugzilla Sandbox v2.2a
http://www.cacti.ne...ontrib/CactiVM.txt
CactiVM
CactiVM
to see cacti use: open Cacti
to use phpmyadmin: open phpmyadmin

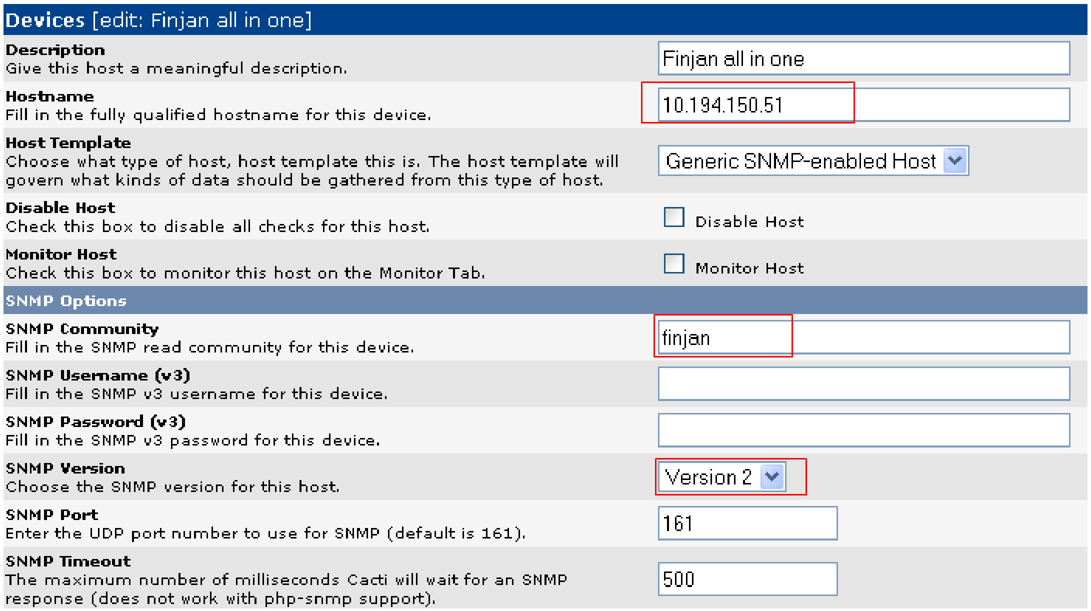
8. Click **Open Cacti** and log-in with the following credentials:

   Username: *admin*

   Password: *cacti*

9. Navigate to **Management** → **Devices** → **Add**.

10. Define the Finjan device as follows:



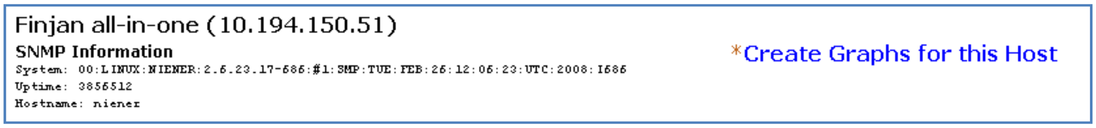
Devices [edit: Finjan all in one]

Description Give this host a meaningful description.	Finjan all in one
Hostname Fill in the fully qualified hostname for this device.	10.194.150.51
Host Template Choose what type of host, host template this is. The host template will govern what kinds of data should be gathered from this type of host.	Generic SNMP-enabled Host
Disable Host Check this box to disable all checks for this host.	□ Disable Host
Monitor Host Check this box to monitor this host on the Monitor Tab.	□ Monitor Host
SNMP Options	
SNMP Community Fill in the SNMP read community for this device.	finjan
SNMP Username (v3) Fill in the SNMP v3 username for this device.	
SNMP Password (v3) Fill in the SNMP v3 password for this device.	
SNMP Version Choose the SNMP version for this host.	Version 2
SNMP Port Enter the UDP port number to use for SNMP (default is 161).	161
SNMP Timeout The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support).	500

Defining the Device

11. Click **Create**.

If the **SNMP information status** is shown as below, the transaction was successful. If not, ensure that no firewall is blocking the SNMP traffic.



Finjan all-in-one (10.194.150.51)

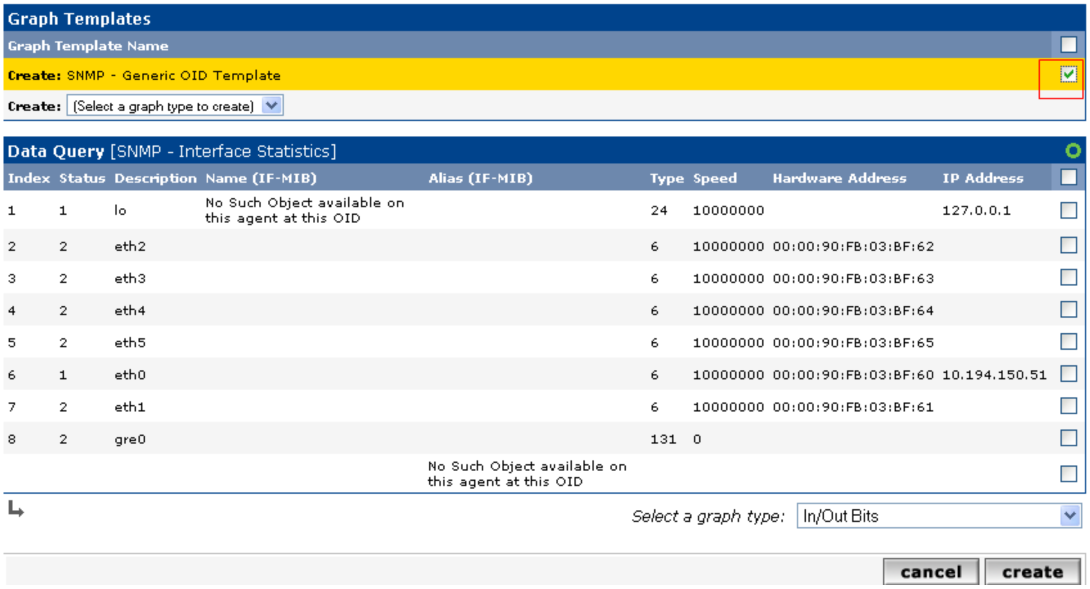
SNMP Information

```
System:  00:LINUX:NIENER:2.6.23.17-686:#1:SMP:TUE:FEB:26:12:06:23:UTC:2008:I686
Uptime:  3856512
Hostname: niener
```

SNMP Information

12. Click **Create Graphs for this Host**,

13. Select **SNMP – Generic OID** and click **Create**.



Graph Templates

Graph Template Name	□
Create: SNMP - Generic OID Template	☑
Create: (Select a graph type to create)	

Data Query [SNMP - Interface Statistics]

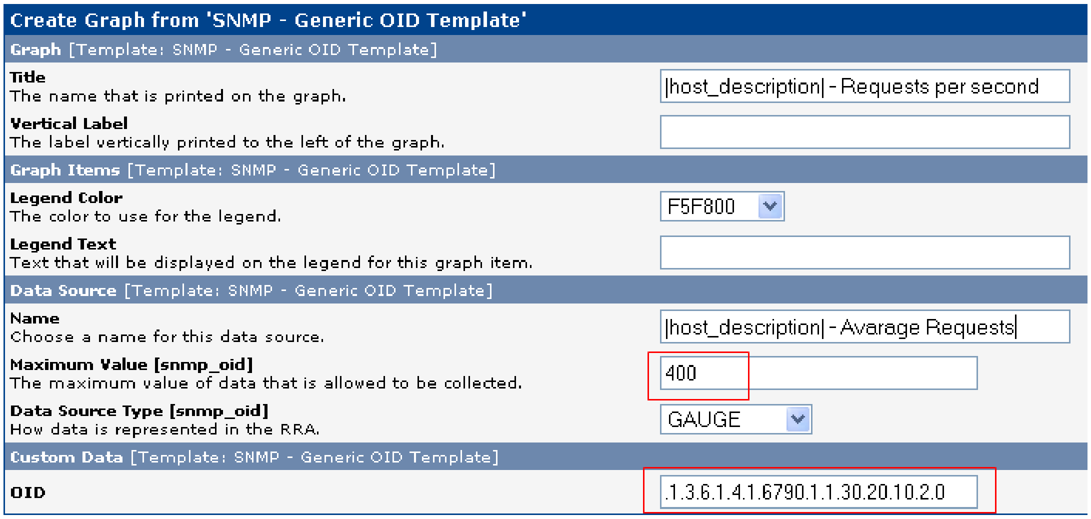
Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	Hardware Address	IP Address	□
1	1	lo	No Such Object available on this agent at this OID		24	10000000		127.0.0.1	□
2	2	eth2			6	10000000	00:00:90:FB:03:BF:62		□
3	2	eth3			6	10000000	00:00:90:FB:03:BF:63		□
4	2	eth4			6	10000000	00:00:90:FB:03:BF:64		□
5	2	eth5			6	10000000	00:00:90:FB:03:BF:65		□
6	1	eth0			6	10000000	00:00:90:FB:03:BF:60	10.194.150.51	□
7	2	eth1			6	10000000	00:00:90:FB:03:BF:61		□
8	2	gre0			131	0			□
				No Such Object available on this agent at this OID					□

Select a graph type: In/Out Bits

Sample OIDs for monitoring (relevant for VSOS version 9):

OID	Description
.1.3.6.1.4.1.6790.1.1.30.20.10.2.0	Average rate of requests scanned per second
.1.3.6.1.4.1.6790.1.1.30.21.10.2.0	Average rate of HTTP requests scanned per second
.1.3.6.1.4.1.6790.1.1.30.22.10.2.0	Average rate of HTTPS requests scanned per second
.1.3.6.1.4.1.6790.1.1.30.23.10.2.0	Average rate of FTP requests scanned per second
.1.3.6.1.4.1.6790.1.1.30.24.10.2.0	Average rate of ICAP requests scanned per second

To monitor total average requests:



Create Graph from 'SNMP - Generic OID Template'

Graph [Template: SNMP - Generic OID Template]

Title The name that is printed on the graph.	|host_description| - Requests per second
Vertical Label The label vertically printed to the left of the graph.	

Graph Items [Template: SNMP - Generic OID Template]

Legend Color The color to use for the legend.	F5F800
Legend Text Text that will be displayed on the legend for this graph item.	

Data Source [Template: SNMP - Generic OID Template]

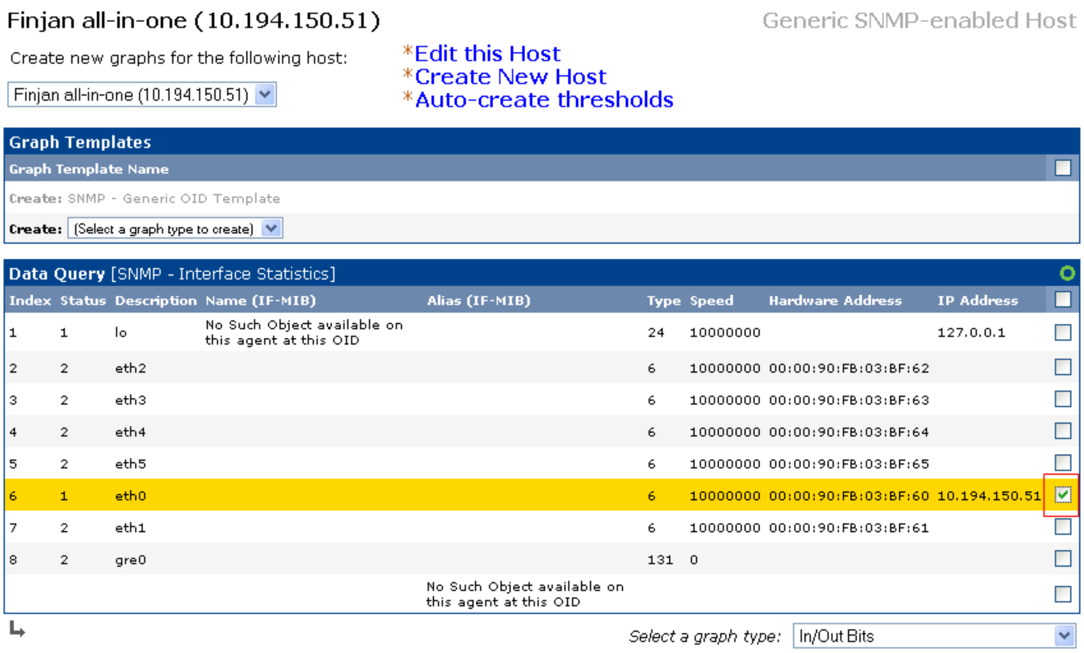
Name Choose a name for this data source.	|host_description| - Avarage Requests
Maximum Value [snmp_oid] The maximum value of data that is allowed to be collected.	400
Data Source Type [snmp_oid] How data is represented in the RRA.	GAUGE

Custom Data [Template: SNMP - Generic OID Template]

OID	.1.3.6.1.4.1.6790.1.1.30.20.10.2.0

⇨ To monitor the inbound and the outbound bandwidth:

1. Click **Management** → **Devices** → **Finjan all-in-one** → **Create graphs for this host**.



Finjan all-in-one (10.194.150.51) Generic SNMP-enabled Host

Create new graphs for the following host: Finjan all-in-one (10.194.150.51)

*Edit this Host
*Create New Host
*Auto-create thresholds

Graph Templates

Graph Template Name	□
Create: SNMP - Generic OID Template	
Create: (Select a graph type to create)	

Data Query [SNMP - Interface Statistics]

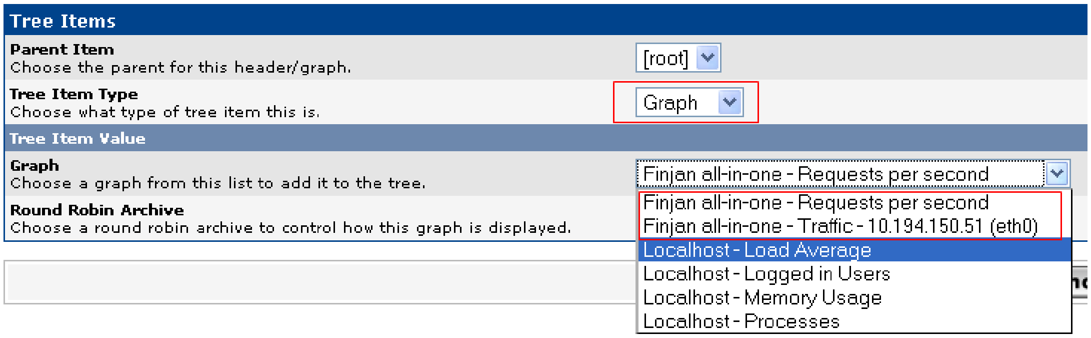
Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	Hardware Address	IP Address	□
1	1	lo	No Such Object available on this agent at this OID		24	10000000		127.0.0.1	□
2	2	eth2			6	10000000	00:00:90:FB:03:BF:62		□
3	2	eth3			6	10000000	00:00:90:FB:03:BF:63		□
4	2	eth4			6	10000000	00:00:90:FB:03:BF:64		□
5	2	eth5			6	10000000	00:00:90:FB:03:BF:65		□
6	1	eth0			6	10000000	00:00:90:FB:03:BF:60	10.194.150.51	☑
7	2	eth1			6	10000000	00:00:90:FB:03:BF:61		□
8	2	gre0			131	0			□
				No Such Object available on this agent at this OID					□

Select a graph type: In/Out Bits

2. Select the interfaces which have assigned IP addresses and click **Create**.

3. Add the defined charts to the graphs tree.

4. Click **Management** → **Graph trees** → **Default tree** → **Add** and add the graphs as follows:



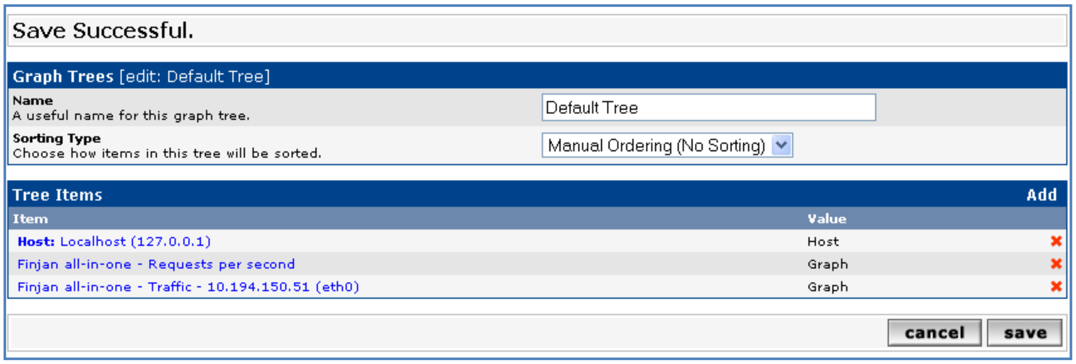
Tree Items

Parent Item Choose the parent for this header/graph.	[root]
Tree Item Type Choose what type of tree item this is.	Graph

Tree Item Value

Graph Choose a graph from this list to add it to the tree.	Finjan all-in-one - Requests per second
Round Robin Archive Choose a round robin archive to control how this graph is displayed.	

Finjan all-in-one - Requests per second
Finjan all-in-one - Traffic - 10.194.150.51 (eth0)
Localhost - Load Average
Localhost - Logged in Users
Localhost - Memory Usage
Localhost - Processes



Save Successful.

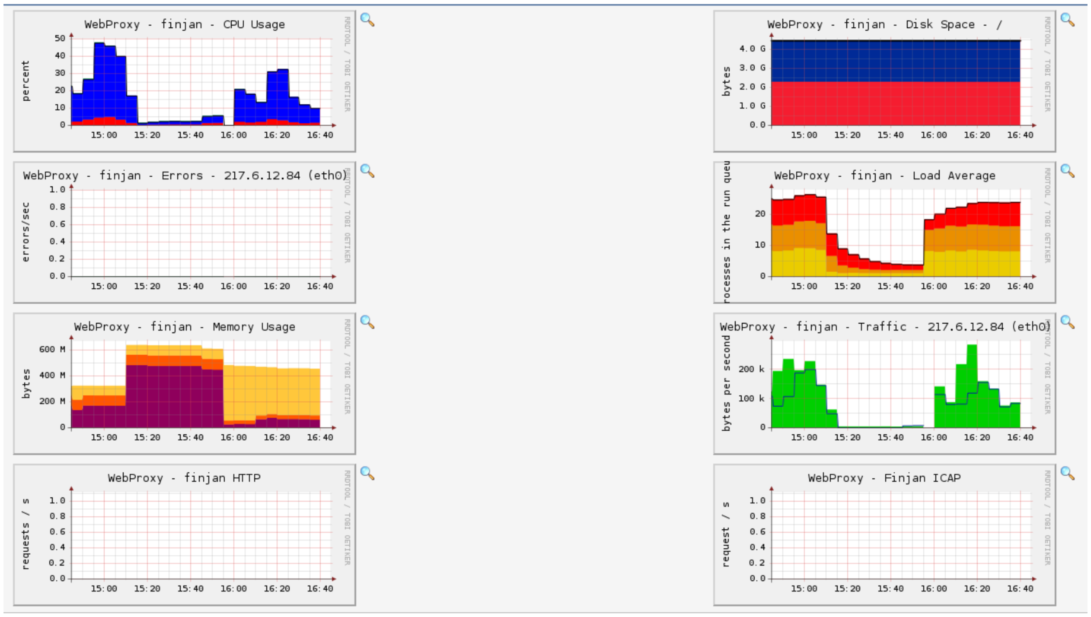
Graph Trees [edit: Default Tree]

Name A useful name for this graph tree.	Default Tree
Sorting Type Choose how items in this tree will be sorted.	Manual Ordering (No Sorting)

Tree Items **Add**

Item	Value	
Host: Localhost (127.0.0.1)	Host	✖
Finjan all-in-one - Requests per second	Graph	✖
Finjan all-in-one - Traffic - 10.194.150.51 (eth0)	Graph	✖

5. Click **Save**.
6. Click the **Graphs** tab → **Default tree** to view all relevant charts.



Informational Graphs

The same monitoring process should be done for all other equipment. To get an accurate account of network resource usage, monitoring should encompass all network components; from the switch connected to the client through to the gateway router.

A properly monitored environment should supply the administrator with the relevant and useful data needed to design and extend an efficient network.