

The Barracuda Spam & Virus Firewall provides an intuitive Web interface with which the administrator can monitor system performance. Additionally, using the Barracuda Spam & Virus Firewall SNMP agent, administrators can use their SNMP monitor to query the system for status on CPU health, queue size, latency and other important statistics. The administrator can also use SNMP monitoring to receive traps reporting system load and other vitals of the Barracuda Spam & Virus Firewall. This document covers the basics of using the Barracuda SNMP agent with the Barracuda Spam & Virus Firewall, firmware version 4.0 and higher.

Configure the Barracuda Spam & Virus Firewall

To use your SNMP monitor with the Barracuda Spam & Virus Firewall, you will first need to log into the Web interface of the Barracuda Spam & Virus Firewall as the administrator and set the **Allowed SNMP and API IP/Range** from the **BASIC > Administration** page. The IP addresses/networks you enter will be allowed SNMP access to the Barracuda Spam & Virus Firewall and will also have the ability to change configuration information through the Barracuda API.

MIBs

You will need to obtain and import two MIB files to your SNMP monitor:

1. The Barracuda Reference MIB (standard across all Barracuda Networks products)
2. The Barracuda Spam & Virus Firewall MIB

You can use reference objects included in these MIBs for monitoring either from custom scripts or from your SNMP monitor. The MIB files are located on the appliance and can be obtained by replacing **YOURBARRACUDA** in the following links with the IP address of your Barracuda Spam & Virus Firewall:

<http://YOURBARRACUDA:8000/Barracuda-SPAM-MIB.txt>
<http://YOURBARRACUDA:8000/Barracuda-REF-MIB.txt>

Syntax

If you are using an SNMP monitor tool, all you need to do is import the MIBs as mentioned above into the SNMP monitor. You can refer to the MIBs for the Object IDs (OIDs) that correspond to the type of status you want to monitor. Please refer to the objects and traps listed in the next section.

If you are querying the Barracuda Spam & Virus Firewall from code, use the following syntax (where **System IP or hostname or localhost** is the IP address of the Barracuda Spam & Virus Firewall). Note that, if using the `snmpwalk` command, if you don't include an OID you will get a listing of all of the OIDs in the MIB.

This example checks the Inbound Queue size on the Barracuda Spam & Virus Firewall, where the OID for Inbound Queue is 1.3.6.1.4.1.20632.2.2 (see Objects and Traps below). Note that Barracuda Networks currently supports SNMP version 2c for the Barracuda Spam & Virus Firewall.

```
snmpget -v 2c -c public [System IP or hostname or localhost] .1.3.6.1.4.1.20632.2.2
```

Example: Getting Accurate SNMP values for CPU Load

The standard SNMP MIB reports the CPU load values averaged since the time the Barracuda Spam & Virus Firewall was last booted. To obtain a periodic CPU load value, measurements for active CPU and idle CPU must be taken at two different times.

The calculations are as follows:

```
active_cpu = ssCpuRawSystem.0 + ssCpuRawNice.0 + ssCpuRawUser.0
```

```
idle_cpu = ssCpuRawIdle.0
```

Commands for the raw values are:

```
ssCpuRawSystem.0:      snmpwalk -Os -v1 -c public 127.0.0.1 1.3.6.1.4.1.2021.11.52
ssCpuRawNice.0:       snmpwalk -Os -v1 -c public 127.0.0.1 1.3.6.1.4.1.2021.11.51
ssCpuRawUser.0:      snmpwalk -Os -v1 -c public 127.0.0.1 1.3.6.1.4.1.2021.11.50
ssCpuRawIdle.0:      snmpwalk -Os -v1 -c public 127.0.0.1 1.3.6.1.4.1.2021.11.53
```

Let `active_cpu[0]` and `active_cpu[1]` be two values taken after an interval of time has passed, and let `idle_cpu[0]` and `idle_cpu[1]` be values taken, respectively, at the same time. The total CPU usage as a percentage is:

$$((\text{active_cpu}[1] - \text{active_cpu}[0]) * 100) / ((\text{active_cpu}[1] - \text{active_cpu}[0]) + (\text{idle_cpu}[1] - \text{idle_cpu}[0]))$$

Objects and Traps

As you will see in the Barracuda Spam & Virus Firewall MIB, the system provides the following objects:

OID	Object	Description
1.3.6.1.4.1.20632.2.2	inQueueSize	Number of messages waiting to be processed by the Barracuda Spam & Virus Firewall.
1.3.6.1.4.1.20632.2.3	outQueueSize	Number of messages waiting to be sent to the mail server. Note that alerts and notifications are queued separately from outbound email.
1.3.6.1.4.1.20632.2.4	deferredQueueSize	Number of messages deferred because they could not be processed, and will be requeued for processing.
1.3.6.1.4.1.20632.2.5	avgEmailLatency	Difference between the time a message was received by the Barracuda Spam & Virus Firewall and the time it is sent to the mail server.
1.3.6.1.4.1.20632.2.7	clusterQueueSize	Number of configuration changes made on one Barracuda Spam & Virus Firewall to be synchronized across the cluster

The system provides the following traps:

OID	Object
1.3.6.1.4.1.20632.2.1.2	cpuFanDead
1.3.6.1.4.1.20632.2.1.3	sysFanDead
1.3.6.1.4.1.20632.2.1.4	cpuTempHigh
1.3.6.1.4.1.20632.2.1.5	firmwareStorageHigh
1.3.6.1.4.1.20632.2.1.6	mailStorageHigh
1.3.6.1.4.1.20632.2.1.7	raidDegradation
1.3.6.1.4.1.20632.2.1.8	inQueueHigh – "Severity: Alert. In-queue size is high"
1.3.6.1.4.1.20632.2.1.9	outQueueHigh – "Severity: Alert. Out-queue size is high"
1.3.6.1.4.1.20632.2.1.10	notifyQueueHigh
1.3.6.1.4.1.20632.2.1.11	latencyHigh
1.3.6.1.4.1.20632.2.1.12	noMailForTooLong

Note that the Barracuda Spam & Virus Firewall communicates SNMP information using a community string of `public` by default. To change the string, please contact Barracuda Networks Technical Support.