

# Snort 2.8.5 and Snort Report 1.3.1 on Ubuntu 8.04 LTS Installation Guide

Author: David Gullett

Published: February 22, 2010

Version: 1.0

Copyright 2010, Symmetrix Technologies

<http://www.symmetrixtech.com>

---

## Table of Contents

### A. Introduction

1. Equipment Assumptions
2. Knowledge Assumptions
3. Use of the Backslash
4. End Result

*Figure 1 - Snort Network Topology*

### B. Procedure

1. Operating System
  - Acquire Ubuntu LTS
  - Installation of Operating System
  - Ubuntu Updates
2. Snort Report
  - Download and Install JpGraph
  - Download and Set up Snort Report
3. Snort
  - Download and Install Snort
  - Download the Latest Snort Rules
  - Download and Install Barnyard
  - Setting up the Network Cards
  - Configuring and Running Snort
  - Testing Snort
4. Monitoring Your System
  - Watching Snort with Snort Report

### C. Future Tasks

1. Oinkmaster
2. BASE and Other Tools
3. Just a Beginning

## A. Introduction

The purpose of this document is to provide the user with a simple installation guide to get Symmetrix Technologies' Snort Report up and running with Sourcefire's Snort intrusion prevention and detection system on Ubuntu Linux. Please note that package numbers change often but were current as of this writing.

### 1. Equipment Assumptions

A dedicated PC for the Snort IDS/IPS (the faster the better) with two network cards  
An additional PC for IDS/IPS administration  
A broadband Internet connection  
A method to burn ISO files to a blank CD

### 2. Knowledge Assumptions

A working knowledge of Linux including SSH and editing configuration files with vi  
A basic knowledge of TCP/IP and network topologies

### 3. Use of the Backslash

There are many instances in this document where a command will not fit on one line so the commonly accepted backslash is used to split it into multiple lines. For example, this is one command, not two:

```
/usr/local/snort/bin/snort -D -u snort -g snort \  
-c /usr/local/snort/etc/snort.conf -i eth1
```

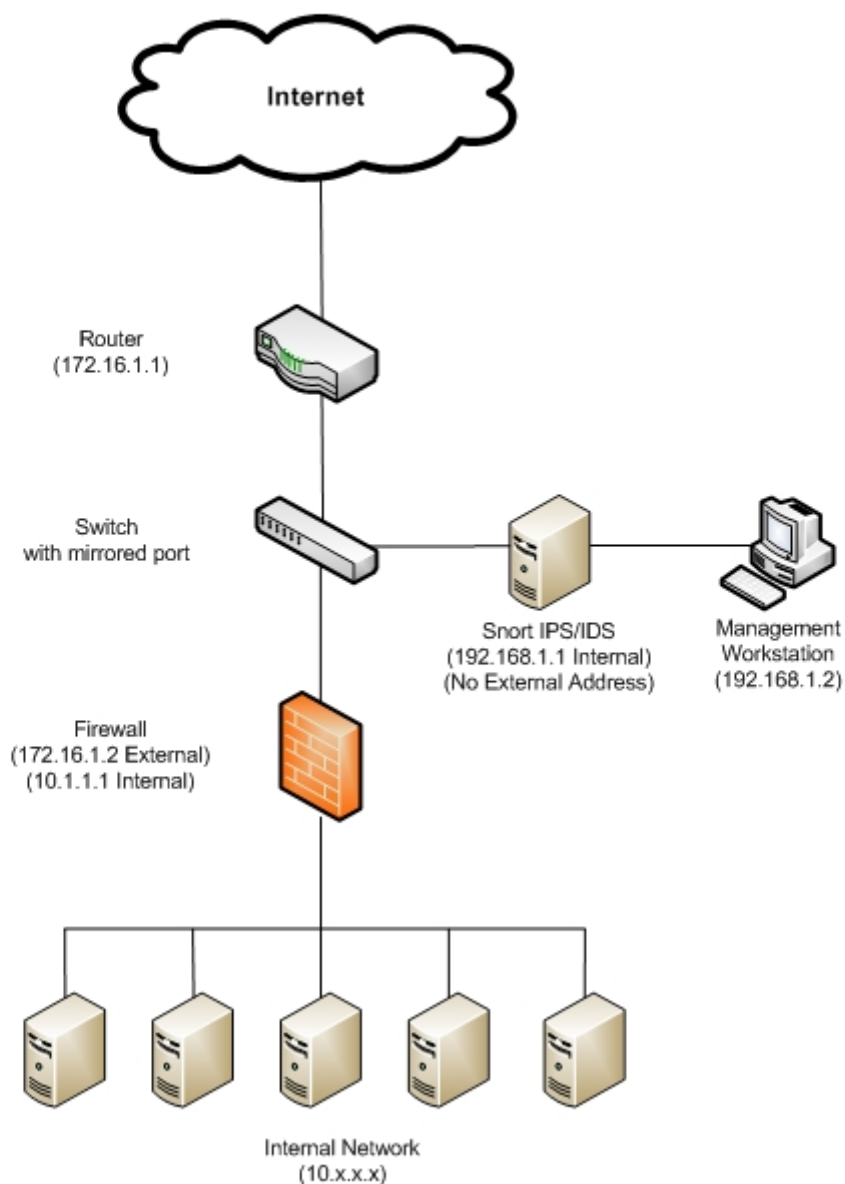
If you are copying and pasting you can leave the backslashes in place and Linux will understand it.

### 4. End Result

There are many ways to set up Snort – we're going with a pretty simple deployment. The end result will be a dedicated IDS machine that actually does the sniffing and a workstation where you perform administration and view the attacks detected by Snort.

The following diagram illustrates the topology.

## Simple Snort Network Topology



Copyright 2010, Symmetrix Technologies

Figure 1 – Snort Network Topology

In the figure above, the network card facing the traffic you want to monitor will have no IP address. This will make it far more difficult for the IDS PC to be compromised from an external source. The network card facing your administrative workstation will have an internal non-routable IP address and access to any open ports will be limited to your administrative workstation.

It's important to note that in modern switched network environments that each port on a switch only sees a subset of the entire network's traffic. Ideally you need to set one port on the switch to be "mirrored" or "spanned" and connect the external IDS network card to it. With this method you can see all traffic going through the switch. As networks scale with multiple switches and segments this becomes much more complex and requires

multiple Snort IDS machines which is beyond the scope of this document. Consult <http://www.snort.org> for more information.

## B. Procedure

### 1. Operating System

#### Acquire Ubuntu Linux

The first order of business is to download Ubuntu Linux. We're going to use Ubuntu 8.04 LTS (named LTS for Long Term Support because Ubuntu will supply security updates for the OS for three years – in this case, until April 2011).

Please note that Ubuntu's download procedure changes occasionally so a direct walkthrough is not practical. Open <http://www.ubuntu.com> in your browser and go to the download section. You're looking for the following ISO: ubuntu-8.04.3-server-i386.iso. You can get this over HTTP, FTP or BitTorrent.

Once you've downloaded and burned the image to a blank CD we're ready to install the OS.

#### Installation of Operating System

For security's sake we will need to install the latest Ubuntu updates on the PC during installation. Temporarily connect one of the network cards to your internal network so it will have Internet access. You can leave the other one disconnected.

Boot up the IDS machine with the Ubuntu CD, select your language and then select Install Ubuntu Server. Select your language again, your country and then your keyboard type.

Once the network hardware detection is complete, the installer will ask you which network card is primary (usually either eth0 or eth1). It should preselect the card to which you have the cable connected. If the connection doesn't work later in the installation you can switch the network cable to the other card. It's highly advisable to label the cards on the back of the machine once you determine their identities.

The installer will now try to automatically configure the network card with DHCP. If you don't have this running on your internal network you will have to hard code the IP address information. Continuing on, you can name the host whatever you like (I chose "snort") then select your time zone.

The disk partitioner will then start. Ideally you would have multiple disks with the mount points spread among them (for high speed logging, etc) but for now just select "Guided – use entire disk." Accept the next few prompts and then the base system will begin installing.

You will then be prompted to set up a user account. This can be anything you want – just pick one and set the password.

Now we are going to pick the packages to install. Keeping with best practices we're going to install the minimum amount of software that we need. For now, just select "OpenSSH server" then pick Continue. We'll add a few more later.

The installation should finish shortly. Select Continue, remove the CD and the machine will boot into a all-text version of Ubuntu. You will then need to log in with the user account you created earlier. By default you cannot log in as root – everything that requires those privileges is done with the sudo command.

Once you've logged in, use the "ifconfig" command to determine the temporary IP address of the machine if you used DHCP. You can then SSH to it from a workstation using the account you set up earlier which makes the rest of the process a bit easier (copy and paste, etc). However, the remainder of the instructions will also work

directly from the console.

Let's add a few more packages that you need. Enter these commands at the prompt (you'll have to enter your password after the first sudo command to provide authorization):

```
sudo apt-get install nmap
sudo apt-get install nbtscan
sudo apt-get install apache2
sudo apt-get install php5
sudo apt-get install php5-mysql
sudo apt-get install php5-gd
sudo apt-get install libssl-dev
sudo apt-get install libpcap0.8-dev
sudo apt-get install libpcre3-dev
sudo apt-get install make
sudo apt-get install gcc
sudo apt-get install g++
```

(You'll be prompted to choose a secure password for the MySQL root user when you install the next package. Don't forget it.)

```
sudo apt-get install mysql-server
sudo apt-get install libmysqlclient15-dev
```

## Ubuntu Updates

To ensure the operating system has the latest security patches installed execute the following commands:

```
sudo apt-get update
sudo apt-get upgrade
```

You might have to reboot if the Linux kernel or core libraries are updated. At this point you should have a working and updated installation of Ubuntu and we're ready to install Snort and Snort Report.

## 2. Snort Report

### Download and Install JpGraph (Optional)

This step is not required – it's only to provide the graphics library for the pie chart on the main page of Snort Report. As of this writing, the current “old” version of JpGraph is 1.27.1. Even though the documentation says this version will not work on PHP5 it does have enough functionality for our purposes. You can download it at this location: <http://hem.bredband.net/jpgraph/jpgraph-1.27.1.tar.gz>

Download that file to a directory on your Snort machine and unpack it with the following commands:

```
sudo mkdir /var/www/jpgraph
sudo tar zxvf jpgraph-1.27.1.tar.gz
sudo cp -r jpgraph-1.27.1/src /var/www/jpgraph/
```

### Download and Set up Snort Report

The next step is to download and configure Snort Report. It's available at <http://www.symmetrixtech.com> under the downloads section. As of this writing the current version is 1.3.1. Download snortreport-1.3.1.tar.gz to a directory on your IDS machine.

Open a command prompt in the directory to which you downloaded Snort Report and issue the following commands:

```
sudo tar zxvf snortreport-1.3.1.tar.gz -C /var/www/
```

Now we need to modify the Snort Report configuration file to reflect your MySQL login info and location of the jgraph libraries. Change the file by editing srconf.php with this command:

```
sudo vi /var/www/snortreport-1.3.1/srconf.php
```

Change the following line from:

```
$pass = "YOURPASS";
```

To this value (use the password you chose in the MySQL setup step earlier rather than YOURPASSWORD):

```
$pass = "YOURPASSWORD";
```

To enable nmap and nbtscan from the web interface, change the following lines from this:

```
define("NMAP_PATH", "/usr/local/bin/nmap -v");  
define("NBTSCAN_PATH", "/usr/local/bin/nbtscan");
```

To this:

```
define("NMAP_PATH", "/usr/bin/nmap -v");  
define("NBTSCAN_PATH", "/usr/bin/nbtscan");
```

If you chose to install the JpGraph library, change the following line from:

```
define("JPGRAPH_PATH", "../..jpgraph/");
```

To this value:

```
define("JPGRAPH_PATH", "../jpgraph/src/");
```

Save the file and exit.

### 3. Snort

#### Download and Install Snort

While we could install the Snort packages from the Ubuntu 8.04 repositories, that wouldn't result in the latest and greatest version of Snort being set up so we're going to compile and install the source code. Open <http://www.snort.org/downloads> with your browser and download the newest stable version. As of this writing, it's located here: <http://dl.snort.org/snort-current/snort-2.8.5.3.tar.gz>. Copy this to a directory on your IDS machine.

The following steps will install Snort into /usr/local/snort but you can change this to a directory of your liking by modifying the paths below.

Open a command prompt and issue the following commands from the directory where you downloaded the Snort source code:

```
sudo tar zxvf snort-2.8.5.3.tar.gz
cd snort-2.8.5.3
sudo ./configure --prefix=/usr/local/snort
sudo make
sudo make install
sudo mkdir /var/log/snort
sudo groupadd snort
sudo useradd -g snort snort
sudo chown snort:snort /var/log/snort
```

You'll have to enter the MySQL password that you chose earlier in the next two steps in order to create the Snort database:

```
echo "create database snort;" | mysql -u root -p
mysql -u root -p -D snort < ./schemas/create_mysql
```

Next we need to create an additional MySQL user for Snort to use as it's not a good idea to run the daemon as root. Remember the password that you enter below. Also note the single quotes around the password in addition to the double quotes around the entire echo statement:

```
echo "grant create, insert, select, delete, update on snort.* to snort@localhost
      identified by 'YOURPASSWORD'" | mysql -u root -p
```

## Download the Latest Snort Rules

The next step is to download the latest public Snort ruleset. It's currently located here: <http://dl.snort.org/reg-rules/snortrules-snapshot-CURRENT.tar.gz> but you will need to register on the Sourcefire website in order to download this file. Create an account if you don't already have one then download the tarball to a directory on your machine.

Open a command prompt in the directory where you downloaded the Snort ruleset file and issue the following commands:

```
sudo tar zxvf snortrules-snapshot-CURRENT.tar.gz -C /usr/local/snort

sudo cp /usr/local/snort/so_rules/precompiled/Debian-Lenny/i386/2.8.5.1/* \
      /usr/local/snort/lib/snort_dynamicrules
```

## Download and Install Barnyard2

Barnyard2 improves the efficiency of Snort by reducing the load on the main detection engine. It reads Snort's unified logging output files and enters them into a database. If the database is unavailable Barnyard will input all data when the database comes back online so no alerts will be lost.

The current version of Barnyard2 is 1.7 as of this writing – which you can download here: <http://www.securixlive.com/download/barnyard2/barnyard2-1.7.tar.gz>

Unpack and install Barnyard2 with the following commands:

```
sudo tar zxvf barnyard2-1.7.tar.gz
cd barnyard2-1.7
sudo ./configure --with-mysql
sudo make
sudo make install
sudo cp etc/barnyard2.conf /usr/local/snort/etc
sudo mkdir /var/log/barnyard2
```

Modify the Barnyard2 configuration file with the following command:

```
sudo vi /usr/local/snort/etc/barnyard2.conf
```

Change the following lines from this:

```
config reference_file: /etc/snort/reference.config
config classification_file: /etc/snort/classification.config
config gen_file: /etc/snort/gen-msg.map
config sid_file: /etc/snort/sid-msg.map
#config hostname: thor
#config interface: eth0
#output database: log, mysql, user=root password=test dbname=db host=localhost
```

To this (use your MySQL password instead of YOURPASSWORD on the last line below):

```
config reference_file: /usr/local/snort/etc/reference.config
config classification_file: /usr/local/snort/etc/classification.config
config gen_file: /usr/local/snort/etc/gen-msg.map
config sid_file: /usr/local/snort/etc/sid-msg.map
config hostname: localhost

config interface: eth1

output database: log, mysql, user=snort password=YOURPASSWORD dbname=snort \
    host=localhost
```

## Setting up the network cards

Now that we have all the necessary software installed and ready to go, we can configure the network cables, IP addresses, Snort and Snort Report. The examples below will reflect the information in Figure 1 at the top of this document so you will likely have to tune the IP addresses, subnet masks etc in order to reflect your network.

To set the IP address on the first card modify the network configuration file with this command:

```
sudo vi /etc/network/interfaces
```

Change the following lines from this:

```
auto eth0
iface eth0 inet dhcp
```

to these values:

```
auto eth0
iface eth0 inet static
address 192.168.1.1
```



```
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Now add the following lines at the end of the file to start the second card without an IP address:

```
auto eth1
iface eth1 inet manual
ifconfig eth1 up
```

Save and exit the file then either reboot or issue this command:

```
sudo /etc/init.d/networking restart
```

Now you can connect the network cables as illustrated in Figure 1. Eth0 is connected to the same subnet as your monitoring workstation and eth1 is connected to the segment that you want to monitor. You can verify this by using the “ifconfig” command. Your output should look something like this (abbreviated here):

```
eth0      Link encap:Ethernet  HWaddr 00:00:00:00:00:00
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth1      Link encap:Ethernet  HWaddr 11:11:11:11:11:11
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Notice how eth1 does not have an IP address but the interface has a status of “up.”

## Configuring and Running Snort

Let's configure Snort and start capturing data.

Edit the Snort configuration file with the following command:

```
sudo vi /usr/local/snort/etc/snort.conf
```

We need to change the following lines from this (these are in multiple sections in the file):

```
dynamicpreprocessor file \
    /usr/local/lib/snort_dynamicpreprocessor/libsf_dce2_preproc.so
dynamicpreprocessor file \
    /usr/local/lib/snort_dynamicpreprocessor/libsf_dns_preproc.so
dynamicpreprocessor file \
    /usr/local/lib/snort_dynamicpreprocessor/libsf_ftptelnet_preproc.so
dynamicpreprocessor file \
    /usr/local/lib/snort_dynamicpreprocessor/libsf_smtp_preproc.so
dynamicpreprocessor file \
    /usr/local/lib/snort_dynamicpreprocessor/libsf_ssh_preproc.so
dynamicpreprocessor file \
    /usr/local/lib/snort_dynamicpreprocessor/libsf_ssl_preproc.so

dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so

dynamicdetection file /usr/local/lib/snort_dynamicrules/bad-traffic.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/chat.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/dos.so
```

```
dynamicdetection file /usr/local/lib/snort_dynamicrules/exploit.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/imap.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/misc.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/multimedia.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/netbios.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/nntp.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/p2p.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/smtp.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/sql.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/web-client.so
dynamicdetection file /usr/local/lib/snort_dynamicrules/web-misc.so
```

To this:

```
dynamicpreprocessor file \
    /usr/local/snort/lib/snort_dynamicpreprocessor/libsf_dce2_preproc.so
dynamicpreprocessor file \
    /usr/local/snort/lib/snort_dynamicpreprocessor/libsf_dns_preproc.so
dynamicpreprocessor file \
    /usr/local/snort/lib/snort_dynamicpreprocessor/libsf_ftptelnet_preproc.so
dynamicpreprocessor file \
    /usr/local/snort/lib/snort_dynamicpreprocessor/libsf_smtp_preproc.so
dynamicpreprocessor file \
    /usr/local/snort/lib/snort_dynamicpreprocessor/libsf_ssh_preproc.so
dynamicpreprocessor file \
    /usr/local/snort/lib/snort_dynamicpreprocessor/libsf_ssl_preproc.so
```

```
dynamicengine /usr/local/snort/lib/snort_dynamicengine/libsf_engine.so
```

```
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/bad-traffic.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/chat.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/dos.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/exploit.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/imap.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/misc.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/multimedia.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/netbios.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/nntp.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/p2p.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/smtp.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/sql.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/web-client.so
dynamicdetection file /usr/local/snort/lib/snort_dynamicrules/web-misc.so
```

Now combine the following two lines in the config file into one line. Change them from this:

```
config detection: search-method ac-bnfa
config detection: max_queue_events 5
```

To this:

```
config detection: search-method ac-bnfa max_queue_events 5
#config detection: max_queue_events 5
```

Next change these lines from this:

```
max_encrypted_packets 20 \  
disable_srvoverflow \  
disable_protomismatch \  
disable_badmsgdir
```

To this (note that the trailing backslash on the first line has been deleted):

```
max_encrypted_packets 20  
#disable_srvoverflow \  
#disable_protomismatch \  
#disable_badmsgdir
```

Below this line (this is to output the unified2 logs for Barnyard):

```
#output log_unified: filename snort.log, limit 128
```

Add this line:

```
output unified2: filename snort.u2, limit 128
```

Save the file and exit back to the command prompt.

## Testing Snort

You can test to see if Snort will run by using this command:

```
sudo /usr/local/snort/bin/snort -u snort -g snort \  
-c /usr/local/snort/etc/snort.conf -i eth1
```

You should see a message saying "Initialization Complete." You can cancel out of it by hitting Control-C. If it fails to initialize please see the forums at [snort.org](http://snort.org) to determine the problem. It will usually be something in the configuration file.

To set Snort to start automatically on your machine edit the rc.local file with the following command:

```
sudo vi /etc/rc.local
```

Then paste the following content in the file (before the "exit 0" line):

```
/usr/local/snort/bin/snort -D -u snort -g snort \  
-c /usr/local/snort/etc/snort.conf -i eth1  
  
/usr/local/bin/barnyard2 -c /usr/local/snort/etc/barnyard2.conf \  
-G /usr/local/snort/etc/gen-msg.map \  
-S /usr/local/snort/etc/sid-msg.map \  
-d /var/log/snort \  
-f snort.u2 \  
-w /var/log/snort/barnyard2.waldo \  
-D
```

Save the file and exit. Then either reboot or use the following command to start Snort:

```
sudo /etc/init.d/rc.local start
```

## 4. Monitoring Your System

### Watching Snort with Snort Report

From your administrative workstation you should now be able to pull up the Snort Report main page by browsing to: <http://192.168.1.1/snortreport-1.3.1/alerts.php>. If you used different IP addresses for the Snort and admin workstation you'll need to change the '192.168.1.1' part of the URL to reflect your network.

Note: We have seen cases where you will need to clear your browser's cache in order to see PHP files properly rather than downloading them.

## C. Future Tasks

It's highly recommended for you to research the following topics as you become more familiar with Snort.

### 1. Oinkmaster

This is a free tool that you can use to automatically download the latest Snort rules. For more information, please visit <http://oinkmaster.sourceforge.net/>

### 2. BASE and Other Tools

There are other popular traffic analysis tools available for Snort such as BASE. These are documented exhaustively at <http://www.snort.org>.

### 3. Just a Beginning

As a reminder, this is a very basic document to get you up and going with Snort and Snort Report. It is extremely critical that you learn all the options in the Snort configuration files in order to set up an effective IDS/IPS. In particular, familiarize yourself with preprocessors and performance tuning along with the tools listed above.

-----

Comments, feedback and contributions are welcome and encouraged at [articles@symmetrixtech.com](mailto:articles@symmetrixtech.com).

Visit us on the web at <http://www.symmetrixtech.com> for the latest news on Snort Report and to download the latest version.

Revision History:

2010-02-22 – 1.0 - Initial release