Snort Installation Manual

Snort, MySQL, ACID, & IIS

Windows NT4 Server, 2000, & XP
(All Versions)

Prepared & Written by Michael E. Steele
Technical Support Engineer for Silicon Defense
michaels@silicondefense.com
http://www.silicondefense.com

Document Version 1.1
Revised Date: Feb, 20, 2003
Silicon Defense
info@silicondefense.com
Phone: 707 445 4355
Fax: 707 445 4222

Table of Contents

Introduction

This documentation will not only help understand how to install a stand alone Master sensor using Snort, but guide you through the entire process, step by step.

When I set out to write this documentation, there was very little documentation for installing Snort for Windows. I have tried to make installing a full blown Intrusion Detection System using Snort in a Windows environment as painless as possible for the novice Windows user, and hopefully that is what I have done.

This guide includes all the necessary information and file linking's for installing an Intrusion Detection System, using Snort on a Windows box. It is **imperative** that the files in the links below are used in this installation, or the procedure may fail.

Copyright Notice

Disclaimer

Use the information in this document at your own risk. Silicon Defense disavows any potential liability of this document. Use of the concepts, examples, and/or other content of this document are entirely at your own risk.

This guide is written in the hope that it will be useful, but without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose.

All copyrights are owned by their owners, unless specifically noted otherwise. Third party trademarks or brand names are the property of their owners. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark. Naming of particular products or brands should not be seen as endorsements.

Latest documentation & downloads

Latest up to date docs and files: http://www.silicondefense.com/support/windows

Comments & Corrections

If any errors that may be found or you would just like to make a comment please send them to: michaels@silicondefense.com

Conceptual Topology

There are four primary software packages that produce this topology. The IIS web server, MySQL database server, ACID and Snort. Below is a brief description of each of the packages and there purpose in the topology.

IIS Web Server: This is the web server of choice by certified Microsoft professionals. The sole purpose of IIS is for hosting the ACID web-based console.

MySQL Server: MySQL is a SQL based database server for a variety of platforms and is the most supported platform for storing Snort alerts. All of the IDS alerts that are triggered from our sensors are stored in the MySQL database.

Analysis Console for Intrusion Databases (ACID): ACID is a web-based application for viewing firewall logs and/or IDS alerts. This is where all the sensor information is consolidated for viewing.

Snort: Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. This is the software package that is used to gather information form the network.

Required Software

Some of the files included with this installation are UNIX specific, but will work with Windows, if all the installation procedures are followed as prescribed.

Download Snort 1.9.0 (Build 229) (StdDB w/Service)
Download WinPcap 3.0 alpha4; Download
Download MySQL Shareware 4.0.10 gamma
Download PHP 4.3.1
Download ADODB 3.10
Download PHPLot 4.4.6
Download JPGraph-1.10.1
Download ACID 0.9.6b23

Note: We will be using WinRAR to uncompress any compressed files.

How to use this guide

This installation is based on a single sensor, with a single interface, a Console that will be accessed through localhost (127.0.0.1), and using Apache as the webserver.

For this installation we started with a fresh install of XP with a single drive partitioned into 2 primary partitions (C & D). All programs and their subsystems will be installed on Drive ‘D’.

This installation is based on the installer being logged on as 'Administrator' for the entire installation. Only the files downloaded from our website will be used. This installation may NOT work with either newer versions or lesser versions of the same program.

Suggested prerequisites

- Fresh install of Windows
- Hard Drive Partition C - Min 2 Gigabytes
- Hard Drive Partition D - Min 10+ Gigabytes
- All Service Packs and Patches applied

I would strongly suggest a clean install to start this installation, but it's certainly is not required. If this is being installed on a dirty disk then make SURE that, all Service Packs and Patches have been applied, ANY of these programs that are going to be installed, that have been previously installed, are COMPLETELY removed before starting this installation, especially WinPcap.

Installing and configuring Snort

● Navigate into the 'D:' drive, and create a folder called 'Applications'.

● Uncompress 'Snort_1.9.0b6-228_Win32_StdDB_Service_Release.zip' into the 'D:\Applications' folder.

● Navigate into the 'D:\Applications' folder and rename the 'snort-1.9.0' folder to 'snort'.

● Navigate into the folder 'D:\Applications\snort', and create a folder called 'log'

● Load the file 'D:\Applications\snort\etc\snort.conf' into WordPad. Several variables located in that file will need to be changed. Use the search routine to find and edit them.

Original: var HOME_NET any

Note: The IP and Subnet variables in the examples below are purely fictitious.

To monitor a single host, with an IP of 10.0.0.3
Change: var HOME_NET 10.0.0.3/32

To monitor a class C Network with an IP of 10.0.0.x, and a subnet of 255.255.255.x
Change: var HOME_NET 10.0.0.0/24

To monitor a class B network with an IP of 10.0.x.x, and a subnet of 255.255.x.x
Change: var HOME_NET 10.0.0.0/16

To monitor a class A Network with an IP of 10.x.x.x, and a subnet of 255.x.x.x
Change: var HOME_NET 10.0.0.0/8

Note: By default Snort will monitor the complete network using 'var HOME_NET any'

Note: There are several other settings that will need to be changed, and these MUST be copied EXACTLY as they are described here. Do a search and replace the like same lines.

Original: var RULE_PATH ../rules
Change: var RULE_PATH d:/applications/snort/rules

Original: # output database: log, mysql, user=root password=test dbname=db host=localhost
Change: output database: log, mysql, user=snort password=123 dbname=snort host=127.0.0.1 port=3306 sensor_name=SENSOR_NAME

Original: # output database: alert, postgresql, user=snort dbname=snort
Cange: output database: alert, mysql, user=snort password=123 dbname=snort host=127.0.0.1 port=3306 sensor_name=SENSOR_NAME

Note: In the two output database lines above, there is a sensor_name=SENSOR_NAME. This SENSOR_NAME is usually the hostname of the sensor. This name is displayed in the Acid console when alerts are being viewed.

Original: # output alert_syslog: LOG_AUTH LOG_ALERT
Change: output alert_syslog: LOG_AUTH LOG_ALERT

Note: This will allow Snort to send alerts to the Application log located in the Event Viewer. If logging to the Application Log is not important, then leave the hash mark (#) in.

Original: include classification.config
Change: include d:/applications/snort/etc/classification.config

Original: include reference.config
Change: include d:/applications/snort/etc/reference.config

● Save the file and exit!

Installing WinPcap

● Double click on the 'WinPcap_3_0_a4.exe' file, and install using all defaults.

Testing the Snort installation

Navigate to 'D:\Application\snort'

● At the command prompt '>' type: snort –W

Note: If WinPcap is operating properly, and snort has been installed correctly, there will be a list of possible sniffing interfaces shown by a number. The correct interface MUST be selected.

Note: The interface number that was derived using the 'Snort -W' switch, will be used throughout the next several exercises. The switch for designating a particular interface, is '-ix', and 'x' will always be the interface number that was derived by using the 'Snort -W' switch.

● At the command prompt '>' type: snort -v –ix

Note: This will run Snort in verbose mode (-v) on a specific interface (-ix). The 'x' in '-ix' is the number of the Network Interface Card that Snort will sniff on.

Note: All errors must be resolve before continuing, see debugging installation errors!

Configuring Snort to run as a service

Note: If a Snort service was previously installed using the 'INSTSRV.exe' program, then that service MUST me removed, otherwise the built-in service installer for Snort will fail.

● To remove the service that was installed using "INSTSRV.EXE" and "SRVANY.EXE"

● From a command prompt type (make sure INSTSRV is in the path):

"instsrv srvany remove"
"instsrv snort remove"

● Start "REGEDIT.EXE" from the run box and Locate and delete the following sub key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Snort

Now reboot the sensor…

Explanation of the service options and commands

● There are three command switches that Snort uses for the Service activation.

Note: It is IMPERATIVE these commands ALWAYS be executed in the same folder as Snort.

/SERVICE /INSTALL
/SERVICE /UNINSTALL
/SERVICE /SHOW

This will install Snort as a service with the specified parameters:
snort /SERVICE /INSTALL -de -c c:/snort/snort.conf -l c:/snort/logs –ix

Note: -ix (x is the number of the NIC for Snort to sniff on)

Note: After every 'snort /SERVICE /INSTALL', be SURE to run the service applet, and set the 'snort' entry to 'Automatic', or the service will fail to start at a reboot.

This will remove snort as a service:
snort /SERVICE /UNINSTALL

This will display the parameters:
snort /SERVICES /SHOW

Starting and stopping Snort from a command prompt:

net stop snort or net start snort

Note: Snort can be stopped, started, and restarted from the Service applet.

Configuring the service

● From a command prompt, navigate to the 'D:\Application\snort folder and type:
snort /SERVICE /INSTALL -c d:/applications/snort/etc/snort.conf -l d:/applications/snort/log –ix

Note: -ix (x is the number of the NIC for Snort to sniff on)

Note: You should receive a confirmation that the service has successfully installed.

● Start the Services applet, either in the Windows 2000 or Windows XP Control Panel, or in the Administrative Tools folder located in the Control Panel.

● From the Services applet, scroll down, right click on the entry 'snort', select 'Properties', in the 'Startup Type' select 'Automatic', click the 'OK' button, and exit the Services applet.

Installing and configuring the MySQL databases

Note: If running Terminal Services, then MySQL must be installed from the Add/Remove panel, or by selecting the RUN dialog box in the start menu and typing: 'change user /install' and after MySQL has installed then type: 'change user /execute' to revert back to user execution mode.

● From WordPad place the lines between the '>----- CUT -----<' in a new file, and save it as ‘my.ini’ in the Root Folder, which could be 'C:\WINDOWS\' or ‘C:\WINNT\’.

```
>----- CUT -----<
[mysqld]
basedir=D:/Applications/mysql
bind-address=127.0.0.1
datadir=D:/Applications/mysql/data
port=3306
set-variable=key_buffer=64M

[WinMySQLadmin]
server=D:/Applications/mysql/bin/mysqld-nt.exe
#user=root
#password=0100
>----- CUT -----<
```

● Save the file and exit!

● Uncompress 'mysql-4.0.10-gamma-win.zip' into a temp folder, and navigate to that folder.

● Install MySQL by double clicking on the setup.exe file, click 'Next', click 'Next', click 'Browse' type d:\applications\mysql into the dialog box, click 'OK', click 'Next', tick 'Typical', click 'Next', let the install complete, and select finish.

● The temp storage folder for MySQL can be deleted.

● Navigate into, and execute the 'D:\Application\mysql\bin\winmysqladmin.exe'.

Note: If MySQL has installed properly, an icon that resembles a traffic light will be in the system tray. This is a status indicator for MySQL, green indicates running, and red indicates stopped.

● Right Click the MySQL icon in the system tray and click on 'Show Me'.

● Select the 'Start Check' tab and the first line should be 'There is a my.ini file' and to the right of that it should say 'yes'.

Note: If there are any errors then reboot and check them again prior to proceeding.

● Select the 'my.ini Setup' tab and make sure the Base Dir is set to 'D:\Applications\mysql', and also the 'mysqld file' has a tick next to the 'mysqld-nt'.

● Click the 'Save Modifications' button, click the 'Yes' button, click the 'OK' button, click 'Create Shortcut on Start Menu' button, and click 'OK'.

Note: By clicking the 'Create Shortcut on Start Menu' this will place a shortcut into the Startup folder for the 'winmysqladmin.exe' file, which will allow it to auto run the administration panel, and status indicator when the sensor is restarted.

● Right click anywhere in the MySQL Administration panel and select 'Hide Me'.

Removing default users and databases

From a command prompt Navigate to the 'D:\Applications\mysql\bin' folder.

● At the command prompt '>' type: mysql -u root
Note: It is IMPERATIVE that a semicolon is added as shown in the commands below.

● At the 'mysql>' prompt type: use mysql;

● At the 'mysql>' prompt type: delete from user where host = "%";

● At the 'mysql>' prompt type: delete from user where user = "";

● At the 'mysql>' prompt type: select * from user;

Note: There should only be a user 'root' listed.

● At the 'mysql>' prompt type: drop database test;

● At the 'mysql>' prompt type: show databases;

Note: There should only be a 'mysql' database listed.

Creating databases

● At the 'mysql>' prompt type: create database snort;

● At the 'mysql>' prompt type: create database archive;

● At the 'mysql>' prompt type: show databases;

Note: There should be three databases listed, 'archive', 'mysql', and 'snort'.

Creating database users

● At the 'mysql>' prompt type: grant INSERT,SELECT on snort.* to snort@localhost identified by "123";

● At the 'mysql>' prompt type: show grants for snort@localhost;

Note: This should show the privileges for user 'snort', and they should match what was added.

● At the 'mysql>' prompt type: grant USAGE on *.* to acid@localhost identified by "12345";

● At the 'mysql>' prompt type: grant SELECT,INSERT,UPDATE,DELETE,CREATE,ALTER on snort.* to acid@localhost;

● At the 'mysql>' prompt type: grant SELECT,INSERT,UPDATE,DELETE,CREATE on archive.* to acid@localhost;

● At the 'mysql>' prompt type: show grants for acid@localhost;

Note: This should show the privileges for user 'acid', and they should match what was added.

● At the 'mysql>' prompt type: select * from user;

Note: There should be three users listed, 'root', 'acid', and 'snort'.

● At the 'mysql>' prompt type: quit;

This completes setting up the databases, and users.

Creating ACID tables in the MySQL database

● At the command prompt '>' type: mysql -u root snort < :\Applications\snort\contrib\create_mysql

● At the command prompt '>' type: mysql -u root archive < :\Applications\snort\contrib\create_mysql

● At the command prompt '>' type: mysql -u root

● At the 'mysql>' prompt '>' type: use snort;

● At the 'mysql>' prompt '>' type: show tables;

Note: If the snort database has been populated, there will be table listings.

● At the 'mysql>' prompt '>' type: use archive;

● At the 'mysql>' prompt '>' type: show tables;

Note: If the archive database has been populated, there will be table listings.

Locking MySQL down

● At the 'mysql>' prompt '>' type: set password for root@localhost = password("0100");

● At the 'mysql>' prompt '>' type: quit;

Note: In order do any manual maintenance; user 'root will need to be used along with its ssigned password to gain access to the MySQL database.

● Right click on the MySQL Admin module in the system tray and select 'Show Me'

● Select the 'my.ini Setup' tab

● Just below the 'server=' entry edit these two lines:

Original: #user=root
Change: user=root

Original: #password=0100
Change: password=0100

● Click the 'Save Modification' button, click 'Yes', and click 'OK'.

● Right click anywhere in the MySQL Admin applet, and select 'Hide Me'.
Note: At this point Snort is configured to run as a service, and MySQL is completely configured.

Now restart the sensor...

Confirming MySQL and Snort are operational

● Open 'Task Manager' and 'snort.exe'. 'mysqld-nt.exe', and 'winmysqladmin.exe' should be listed under 'Processes'.

● In the System Tray in the bottom right, by the clock, there should be a MySQL status indicator resembling a traffic light. Green indicates MySQL is on, Red indicates MySQL is off.

Installing Internet Information Services (IIS) Webserver

Note: For NT Server 4 the Internet Information Services 4 is included with the Option Pack, together with other tools and services. The Option Pack setup wizard makes it easy to setup and install the Web services and the various components that are part of the Windows NT 4 Option Pack. Simply check the items that you want to install, answer a few questions, and the installation wizard installs the desired configuration on the target machine. If IIS4 is being installed then skip this next section, but only after you have installed IIS4.

Note: If you have installed a 2000 or XP server product and chose the default installation, then IIS will have been installed by default and you can skip this section.

Note: The Windows 2000 or XP Professional CD will be required to add IIS5.

● Place your 2000 or XP Professional CD into your CD player.
● In your Control Panel go to your Add/Remove Programs.

● Select Add/Remove Windows Components

● When the Windows Components Wizard appears double click the 'Internet Information Services (IIS)'

● Select 'World Wide Web Service'.

Note: Several options will be auto selected, leave them selected.

● Select 'OK', Select 'next' and this will install Internet Information Services (IIS).

● Select 'Finish' and you're done installing IIS.

Now restart the sensor...

Configuring IIS for the Acid Console

Note: If you are installing this IDS on an XP box then 'Use simple file sharing' must be off.

● To turn 'Simple file sharing off' on an XP box: Go to the control panel and select the 'Folder options' applet, Select the 'View' tab, Use the scroll bar and scroll to the bottom, Remove the tick from 'Use simple file sharing (recommended)', click 'Apply', and exit out of the control panel.

● Navigate to the 'D:\Applications' folder and create a folder called 'acid'.

● Right mouse click on the 'acid' folder and select 'Properties', select the 'Security' tab, click the 'Advanced' button (the 'Everyone' group should be selected), remove the tick from 'Inherit from parent the permission entries that apply to child objects.', select 'Remove' (The 'Everyone' group should disappear), select the 'Add' tab, select the 'Advanced' tab, select the 'Find Now' tab, Double click on 'Administrator, click the 'OK' tab, In the permissions window, tick the 'Allow' for 'Full Control' (all the permissions will be automatically ticked), select the 'OK' tab three times, and the 'acid dialog' properties panel goes away.

● Start the Microsoft Management Console (may appear as 'Internet Services Manager', either in the Windows 2000 or Windows XP Control Panel in Administrative Tools.

● Double click 'local computer', double click 'Web Sites', right mouse click on 'Default Web Site', select 'New', select 'Virtual Directory', click 'Next', in Alias: dialog box type: Console, click 'Next', in directory: dialog box type: d:\Applications\acid, click 'Next', click 'Next', click 'Finish'.

Note: Under 'Default Web Site' there should be an entry called: Console

Installing PHP the HTML embedded scripting language

● Uncompress 'php-4.3.1-Win32.zip' to 'D:\Applications\php'.

● Copy the file 'D:\Applications\php\php4ts.dll' to your "System32" folder.

Note: The 'System32' folder could be located in 'C:\WINDOWS\', or 'C:\WINNT'.

● Copy 'D:\Applications\php\php.ini-dist to the 'SYSTEM ROOT' Folder, and rename it to php.ini.

Note: The 'SYSTEM ROOT' folder is usually 'C:\WINDOWS\', or 'C:\WINNT'.
● In WordPad edit the 'php.ini' file and change these variables:

Original: max_execution_time = 30
Change: max_execution_time = 60

Original: session.save_path = /tmp
Change: session.save_path = C:\WINDOWS\Temp

Note: Make SURE the 'session.save_path =' variable is pointing to the correct and existing 'Temp' or 'Tmp' folder, and 'everyone' has permissions to use.

Original: ; cgi.force_redirect = 1
Change: cgi.force_redirect = 0

Original: ; extension=php_gd.dll
Change: extension=php_gd.dll

Original: doc_root =
Change: doc_root = d:\applications\apache\apache2\htdocs\acid

Original: extension_dir = ./
Change: extension_dir = d:\applications\php\extensions

● Save the file and exit!

Configure PHP extensions for IIS 4/5

● Start the Microsoft Management Console (may appear as 'Internet Services Manager', either in the Windows 2000 or Windows XP Control Panel in Administrative Tools).

● Double click 'local computer', double click 'Web Sites', double click on 'Default Web Site', right click on 'Console', select properties, select 'Virtual Directory' tab, click 'Configuration' button, and then click he Applications Mappings tab.

● Click Add, and in the Executable box, type: d:\applications\php\php.exe

● In the Extension box, type: .php

● Leave 'Method exclusions' blank if there is one.

● Check the Script engine checkbox.

Note: By placing a tick on the 'check that file exists' box - for a small performance penalty, IIS will check that the script file exists and sort out authentication before firing up php.

● Click 'OK', click 'Apply', and click 'OK'

Installing and configuring ADODB

● Uncompress 'adodb310.zip' into 'D:\Applications\adodb'.

● In WordPad edit the 'D:\Applications\adodb\adodb.inc.php' file and change these variables:

Original: $ADODB_database = '';
Change: $ADODB_database = 'd:\applications\adodb';

● Save the file and exit!

Installing and configuring PHPLot

● Uncompress 'phplot-4.4.6.zip' into 'D:\Applications'

● Navigate into the 'D:\Applications' folder and rename the 'phplot-4.4.6' folder to 'phplot'.

Installing and configuring JPGraph

● Uncompress 'jpgraph-1.10.1.zip' into 'D:\Applications'.

● Navigate into the 'D:\Applications\jpgraph-1.10.1\src' folder, and copy all the *.php files into 'D:\Applications\phplot', then the folder 'jpgraph-1.10.1' can be deleted.

Installing the ACID console

● Uncompress 'acid-0.9.6b23.zip' into the 'D:\Applications' folder.

● In WordPad edit the 'D:\Applications\acid\acid_conf.php' file and change these variables:

Original: $DBlib_path = "";
Change: $DBlib_path = "d:\applications\adodb";

Original:
$alert_dbname = "snort_log";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "root";
$alert_password = "mypassword";

Change:
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "3306";
$alert_user = "acid";
$alert_password = "12345";

Original:
$archive_dbname = "snort_archive";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "root";
$archive_password = "mypassword";

Change:
$archive_dbname = "archive";
$archive_host = "localhost";
$archive_port = "3306";
$archive_user = "acid";
$archive_password = "12345";

Original: $ChartLib_path = "";
Change: $ChartLib_path = "d:\applications\phplot";

Note: It is IMPERATIVE that QUOTES are used in the above modifications or Acid will fail.

● Save the file and exit!

Now reboot your new IDS sensor!

● Start a browser and type: http://localhost/Console/Index.html

Note: An error stating 'the underlying database snort@local appears to be invalid' will appear the first time ACID is run. Select the link 'Setup page' when this error appears. Then select 'Create ACID AG' button to complete the Acid Alert Group configuration. A message stating 'The underlying Alert DB is configured for usage with Acid' will appear, and the database is completely configured.

● Return to a browser and retype: http://localhost/Console/Index.html

Note: Acid MUST always be initiated using: http://localhost/Console/Index.html

Note: It may take a little while to start seeing alerts just let it go, and Acid will auto refresh.

Debugging Installation errors

As of Snort V 1.9.0 b229, Snort will now throw FATAL errors to the Event Viewer under the System log tab.

If there is no traffic moving, there are several possibilities.

- Wrong network card selected using the -i switch.
- Network card may need a driver update.
- A previously installed 'WinPcap' was not properly removed.
- No network connection.
- Snort does not operate on duel processors.
- Snort does not operate on a PPOE connection.
- If connected to a switch the ports must be mirrored.
- Ethernet card or cable not secure, or bad.

If there is a MySQL connection refused error, there are several possibilities.

- The Snort run line may be incorrect (make SURE -l is a lowercase L).

Websites of interest

Snort Home Page	http://www.snort.org/
Snort FAQ	http://www.snort.org/docs/faq.html
Snort Users Manual	http://www.snort.org/docs/writing_rules/
Usenet Groups	
Snort-announce	http://lists.sourceforge.net/mailman/listinfo/snort-announce
Snort-users	http://lists.sourceforge.net/mailman/listinfo/snort-users
Snort-sigs	http://lists.sourceforge.net/mailman/listinfo/snort-sigs
Snort-devel	http://lists.sourceforge.net/mailman/listinfo/snort-devel
Snort-cvsinfo	http://lists.sourceforge.net/mailman/listinfo/snort-cvsinfo
Snort CVS tree	http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/snort/snort/
ACID Home Page	http://acidlab.sourceforge.net/
MySQL Home Page	http://www.mysql.com/
PHP Home Page	http://www.php.net
WinPcap Home Page	http://winpcap.polito.it/

Security tools & information

XP Security Checklist	http://www.labmice.net/articles/winxpsecuritychecklist.htm
NSA Securing XP	http://nsa1.www.conxion.com/winxp/guides/wxp-1.pdf

Revisions & Updates

V1.0 Feb 4, 2003
- Initial 1.9.x document in HTML format

V1.1 Feb 20, 2003
- Initial 1.9.x document converted to PDF
- Update PHP (security Fixes)
- Update MySQL to 4.0.10 (minor)
- Update Snort to b229 (Fatal errors to Event Log)

Michael E. Steele | System Engineer / Support Technician
Email Me: mailto:michaels@silicondefense.com
Commercial Snort Support - 1.866.41.SNORT
Silicon Defense - **The Cyber-War Defense Company**
Silicon Defense - **Complete IDS solutions** - http://www.silicondefense.com
Snort: Open Source Network IDS - http://www.snort.org