122022010 Shrayank Mistry
IDS Assignment:

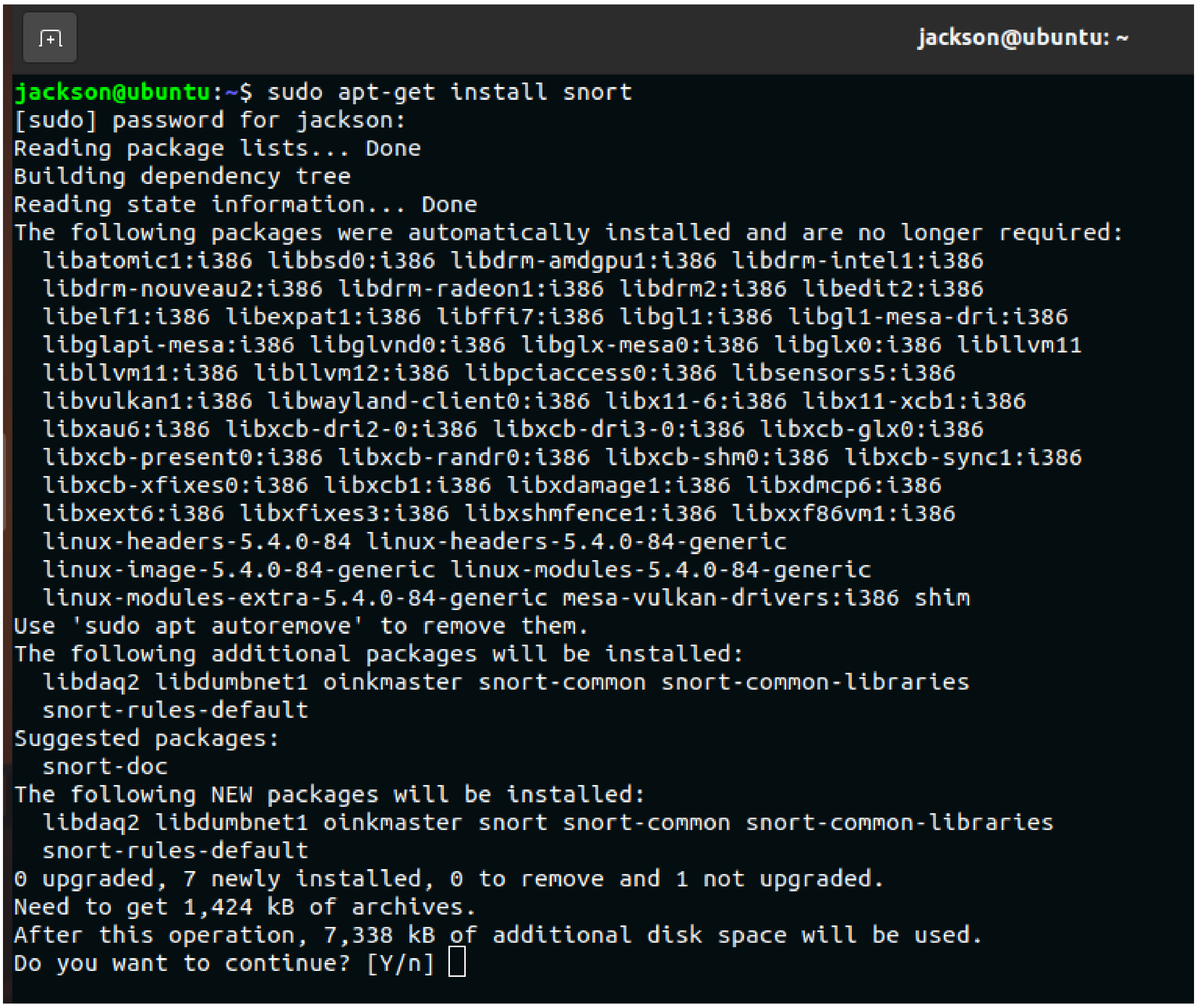
Install, Configure and study any Intrusion Detection System (IDS). Prepare a brief report on it and submit the same in .doc/.pdf format.

Snort is the foremost Open Source Intrusion prevention system (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has 3 primary uses:

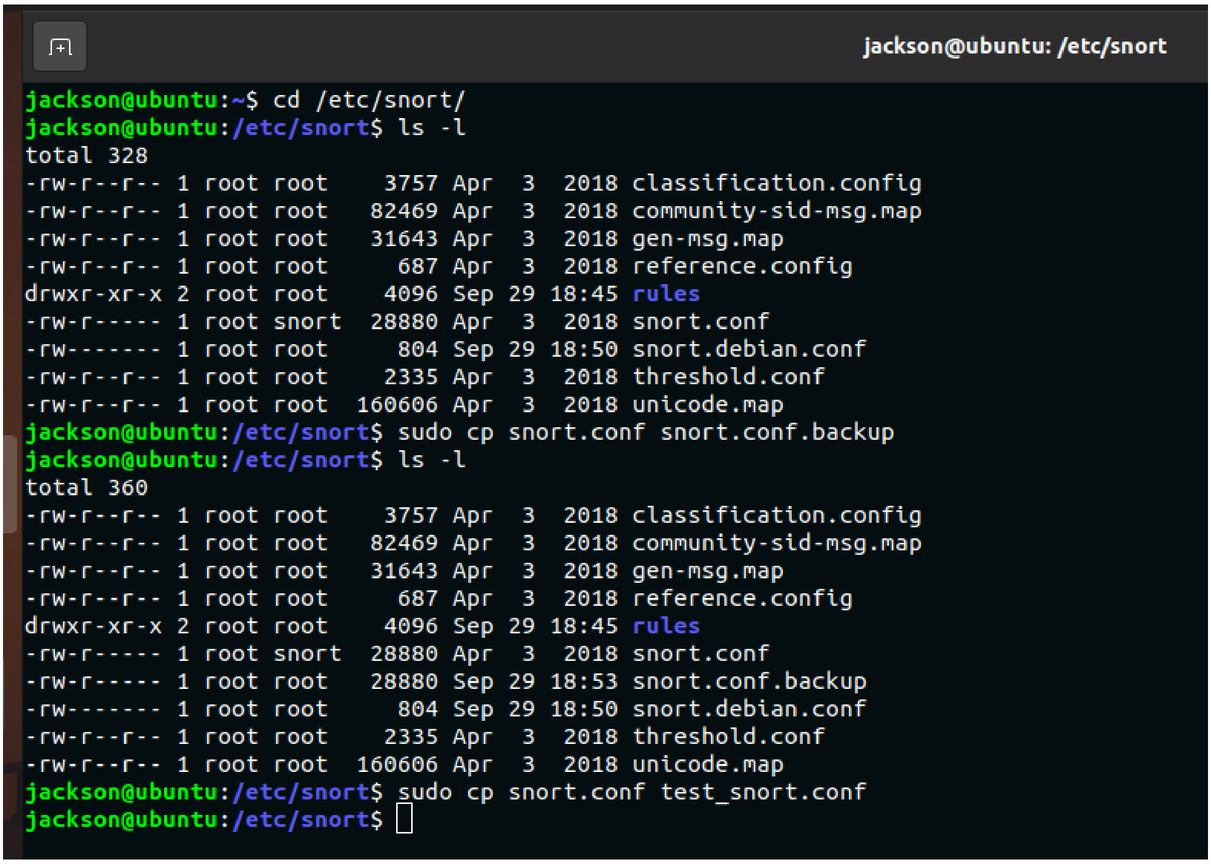
1. As a packet sniffer like tcpdump.
2. As a packet logger - which is useful for network traffic debugging
3. Can also be used as a full blown network intrusion prevention system.

Step 1: Install Snort using command line terminal



```
jackson@ubuntu:~$ sudo apt-get install snort
[sudo] password for jackson:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libatomic1:i386 libbsd0:i386 libdrm-amdgpu1:i386 libdrm-intel1:i386
  libdrm-nouveau2:i386 libdrm-radeon1:i386 libdrm2:i386 libedit2:i386
  libelf1:i386 libexpat1:i386 libffi7:i386 libgl1:i386 libgl1-mesa-dri:i386
  libglapi-mesa:i386 libglvnd0:i386 libglx-mesa0:i386 libglx0:i386 libllvm11
  libllvm11:i386 libllvm12:i386 libpciaccess0:i386 libsensors5:i386
  libvulkan1:i386 libwayland-client0:i386 libx11-6:i386 libx11-xcb1:i386
  libxau6:i386 libxcb-dri2-0:i386 libxcb-dri3-0:i386 libxcb-glx0:i386
  libxcb-present0:i386 libxcb-randr0:i386 libxcb-shm0:i386 libxcb-sync1:i386
  libxcb-xfixes0:i386 libxcb1:i386 libxdamage1:i386 libxdmcp6:i386
  libxext6:i386 libxfixes3:i386 libxshmfence1:i386 libxxf86vm1:i386
  linux-headers-5.4.0-84 linux-headers-5.4.0-84-generic
  linux-image-5.4.0-84-generic linux-modules-5.4.0-84-generic
  linux-modules-extra-5.4.0-84-generic mesa-vulkan-drivers:i386 shim
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries
  snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 7 newly installed, 0 to remove and 1 not upgraded.
Need to get 1,424 kB of archives.
After this operation, 7,338 kB of additional disk space will be used.
Do you want to continue? [Y/n] 
```

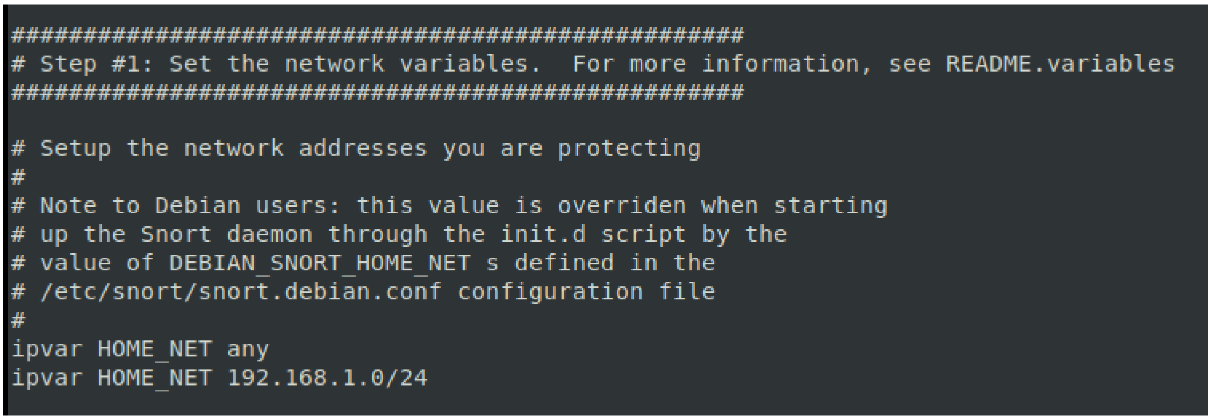
Step 2: Creating a copy of Snort Config File As Backup



```
jackson@ubuntu:~$ cd /etc/snort/
jackson@ubuntu:/etc/snort$ ls -l
total 328
-rw-r--r-- 1 root root    3757 Apr  3  2018 classification.config
-rw-r--r-- 1 root root   82469 Apr  3  2018 community-sid-msg.map
-rw-r--r-- 1 root root   31643 Apr  3  2018 gen-msg.map
-rw-r--r-- 1 root root     687 Apr  3  2018 reference.config
drwxr-xr-x 2 root root    4096 Sep 29 18:45 rules
-rw-r----- 1 root snort  28880 Apr  3  2018 snort.conf
-rw------- 1 root root     804 Sep 29 18:50 snort.debian.conf
-rw-r--r-- 1 root root    2335 Apr  3  2018 threshold.conf
-rw-r--r-- 1 root root  160606 Apr  3  2018 unicode.map
jackson@ubuntu:/etc/snort$ sudo cp snort.conf snort.conf.backup
jackson@ubuntu:/etc/snort$ ls -l
total 360
-rw-r--r-- 1 root root    3757 Apr  3  2018 classification.config
-rw-r--r-- 1 root root   82469 Apr  3  2018 community-sid-msg.map
-rw-r--r-- 1 root root   31643 Apr  3  2018 gen-msg.map
-rw-r--r-- 1 root root     687 Apr  3  2018 reference.config
drwxr-xr-x 2 root root    4096 Sep 29 18:45 rules
-rw-r----- 1 root snort  28880 Apr  3  2018 snort.conf
-rw-r----- 1 root root   28880 Sep 29 18:53 snort.conf.backup
-rw------- 1 root root     804 Sep 29 18:50 snort.debian.conf
-rw-r--r-- 1 root root    2335 Apr  3  2018 threshold.conf
-rw-r--r-- 1 root root  160606 Apr  3  2018 unicode.map
jackson@ubuntu:/etc/snort$ sudo cp snort.conf test_snort.conf
jackson@ubuntu:/etc/snort$ 
```

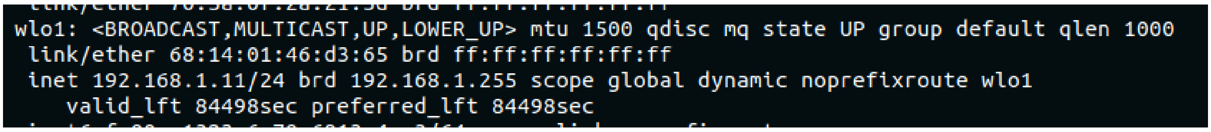
Step 3: Configuring the file to add rules

1. **Setting up the network variable ipvar for home address**



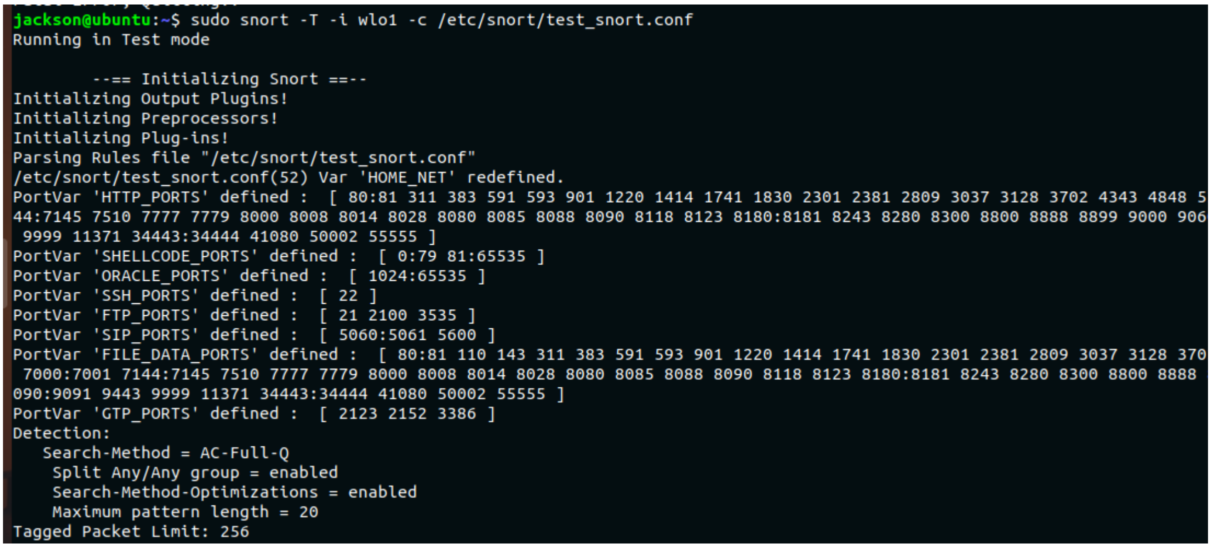
```
###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET any
ipvar HOME_NET 192.168.1.0/24
```

Local IP address on network

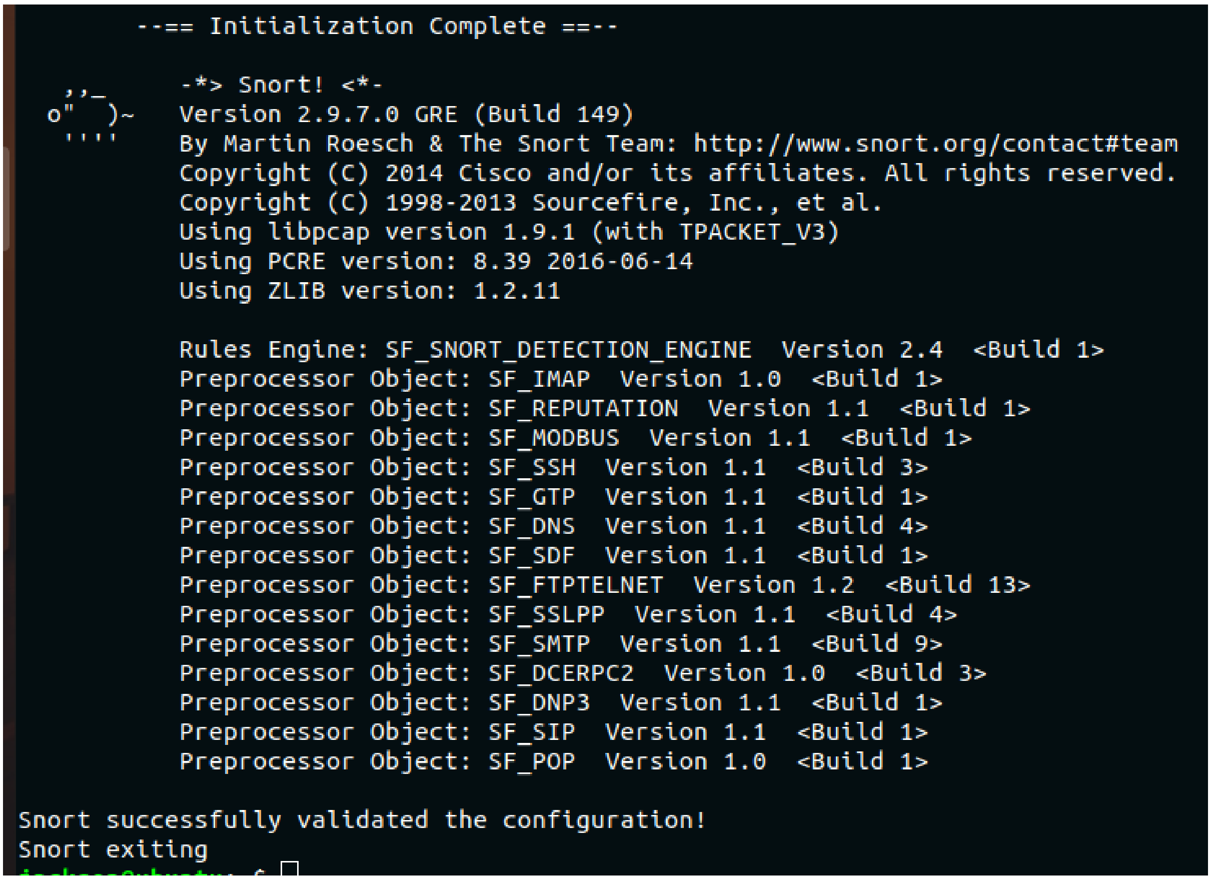


```
wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
 link/ether 68:14:01:46:d3:65 brd ff:ff:ff:ff:ff:ff
 inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic noprefixroute wlo1
    valid_lft 84498sec preferred_lft 84498sec
```

2. Testing Snort with modified config file



```
jackson@ubuntu:~$ sudo snort -T -i wlo1 -c /etc/snort/test_snort.conf
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/test_snort.conf"
/etc/snort/test_snort.conf(52) Var 'HOME_NET' redefined.
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5
44:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 906
 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 370
 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888
090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
```



```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>

Snort successfully validated the configuration!
Snort exiting
```

Conclusion:

Snort really isn't very hard to use, but there are a lot of command line options to play with, and it's not always obvious which ones go together well. But there are a few basic concepts you should understand about Snort. Snort can be configured to run in three modes:

- *Sniffer mode,* which simply reads the packets off of the network and displays them for you in a continuous stream on the console (screen).
- *Packet Logger mode,* which logs the packets to disk.
- *Network Intrusion Detection System (NIDS) mode,* which performs detection and analysis on network traffic. This is the most complex and configurable mode.