UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

DATAMONITOR SYSTEMS LLC,

Plaintiff

v.

SOPHOS LTD.

Defendant

Case No. 6:24-cv-00185

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Datamonitor Systems LLC ("Plaintiff" or "Datamonitor") hereby files this Original Complaint for Patent Infringement against Defendant Sophos Ltd. ("Defendant" or "Sophos"), and alleges, on information and belief, as follows:

THE PARTIES

1. Datamonitor Systems LLC is a limited liability company organized and existing under the laws of the State of Delaware.

2. On information and belief, Sophos Ltd is a foreign corporation with its global headquarters at The Pentagon, Abingdon, OX14 3YP, United Kingdom.

JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, 35 U.S.C. § 1, *et seq*. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in the State of Texas and in this district, including operating systems, using

software, providing services and/or engaging in activities in Texas and in this district that infringe one or more claims of the Asserted Patents.

5. Defendant Sophos has further, either directly or through its extensive network of reseller and OEM partnerships, purposefully and voluntarily placed its infringing products and/or services into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District.

6. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) because, upon information and belief, Defendant Sophos is a foreign entity. Sophos has also committed acts of infringement within this District.

7. On information and belief, Sophos is a foreign corporation with significant contacts with this District. As an example, Sophos has entered into license agreements with end-users in Texas covering the Accused Products and their operation in this District. The Sophos Security Suite End User License Agreements all reference Sophos Limited as the rights-holder under the contract. (See, e.g., https://www.sophos.com/en-us/legal/sophos-end-user-license agreement.aspx.) Thus, Sophos has entered into license agreements with end-users covering the Accused Products and their operation in Texas and in this District.

ASSERTED PATENT

8. On September 22, 2009, United States Patent No. 7,594,009 ("the '009 Patent") was duly and legally issued for "Monitoring Network Activity." A copy may be obtained at: https://patents.google.com/patent/US7594009B2/en.

ACCUSED PRODUCT

9. On information and belief, Defendant makes, uses, imports, sells, and/or offers for sale the Unified Threat Management system (UTM). https://docs.sophos.com/nsg/sophos-utm/utm/9.703/pdf/en-us/manual-en.pdf

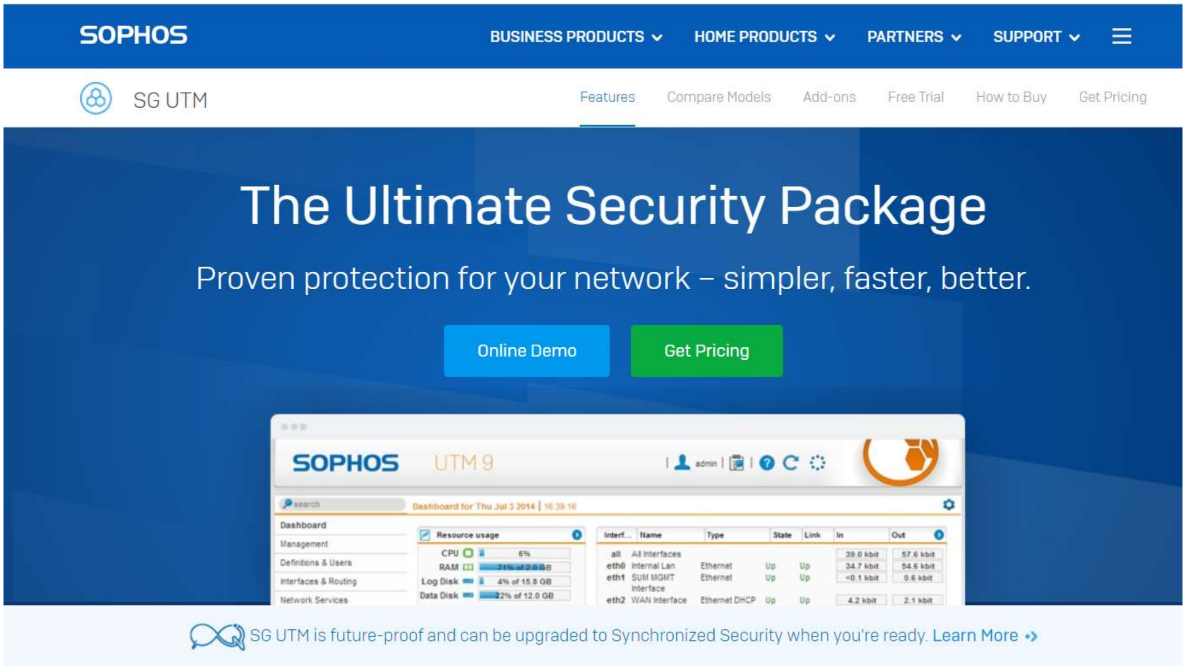
10. On information and belief, at all times Defendant owns and controls the operation of the Accused Instrumentalities in accordance with an end user license agreement.

COUNT I
(Infringement of U.S. Patent No. 7,594,009)

11. Datamonitor incorporates the above paragraphs by reference.

12. Defendant has been and is now infringing one or more claims of the ’009 patent under 35 U.S.C. § 271 by making and/or using the Accused Product in the United States without authority.

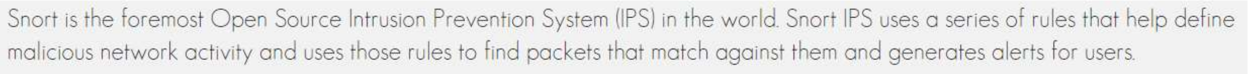
13. More particularly, the Accused Product is a system for analyzing network traffic.



The Ultimate Security Package

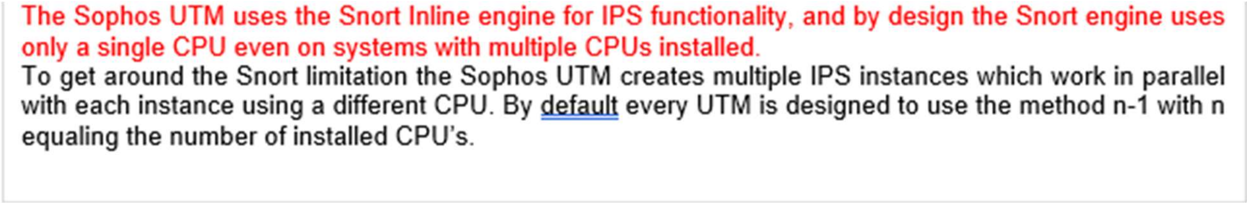
Proven protection for your network – simpler, faster, better.

SG UTM is future-proof and can be upgraded to Synchronized Security when you're ready. Learn More



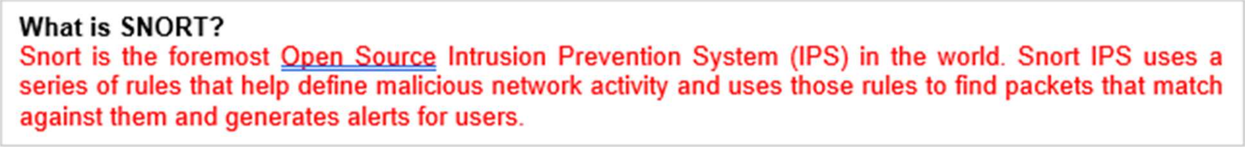
Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

https://www.sophos.com/en-us/products/unified-threat-management.aspx



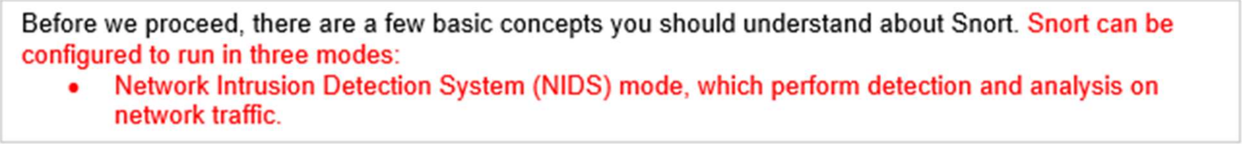
The Sophos UTM uses the Snort Inline engine for IPS functionality, and by design the Snort engine uses only a single CPU even on systems with multiple CPUs installed.
To get around the Snort limitation the Sophos UTM creates multiple IPS instances which work in parallel with each instance using a different CPU. By default every UTM is designed to use the method n-1 with n equaling the number of installed CPU's.

Source: https://support.sophos.com/support/s/article/KB-000034850?language=en_US



What is SNORT?
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.

Source: https://www.snort.org/

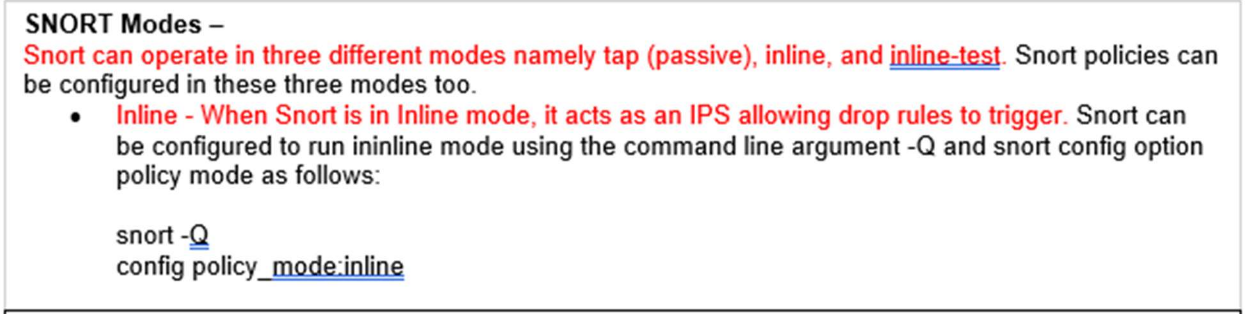


Before we proceed, there are a few basic concepts you should understand about Snort. Snort can be configured to run in three modes:

- Network Intrusion Detection System (NIDS) mode, which perform detection and analysis on network traffic.

Source:https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page 9 of 269

14. In operation, the Accused Product uses a detecting means including a tap which receives and selects packets of data from network traffic.



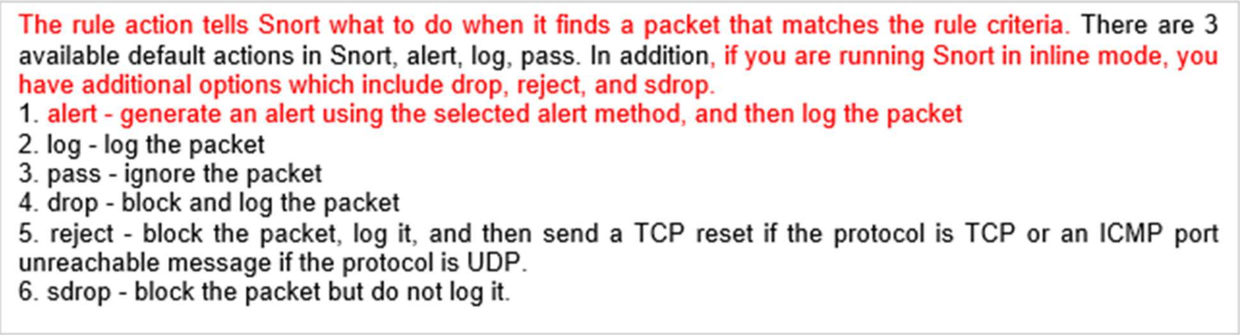
SNORT Modes –

Snort can operate in three different modes namely tap (passive), inline, and inline-test. Snort policies can be configured in these three modes too.

- Inline - When Snort is in Inline mode, it acts as an IPS allowing drop rules to trigger. Snort can be configured to run ininline mode using the command line argument -Q and snort config option policy mode as follows:

```
snort -Q
config policy_mode:inline
```

Source:https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page 25 of 269

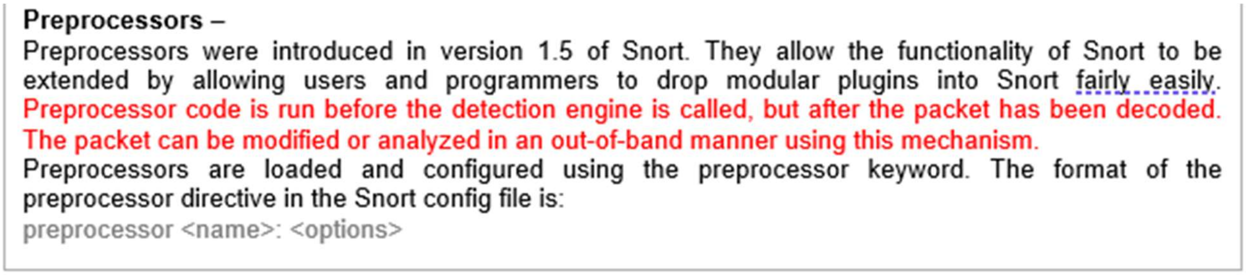


The rule action tells Snort what to do when it finds a packet that matches the rule criteria. There are 3 available default actions in Snort, alert, log, pass. In addition, if you are running Snort in inline mode, you have additional options which include drop, reject, and sdrop.

1. alert - generate an alert using the selected alert method, and then log the packet
2. log - log the packet
3. pass - ignore the packet
4. drop - block and log the packet
5. reject - block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
6. sdrop - block the packet but do not log it.

Source:https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page 183 of 269

15. In operation, the Accused Product uses a packet creating means which, for each packet selected by the tap, creates a modified selected packet for analysis which consists of the selected packet and a unique identifier for the selected packet which distinguishes that selected packet from all other selected packets.



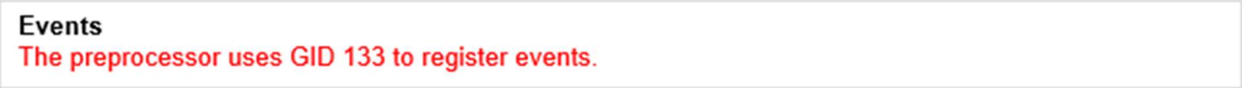
Preprocessors –

Preprocessors were introduced in version 1.5 of Snort. They allow the functionality of Snort to be extended by allowing users and programmers to drop modular plugins into Snort fairly easily. Preprocessor code is run before the detection engine is called, but after the packet has been decoded. The packet can be modified or analyzed in an out-of-band manner using this mechanism.

Preprocessors are loaded and configured using the preprocessor keyword. The format of the preprocessor directive in the Snort config file is:

preprocessor <name>: <options>

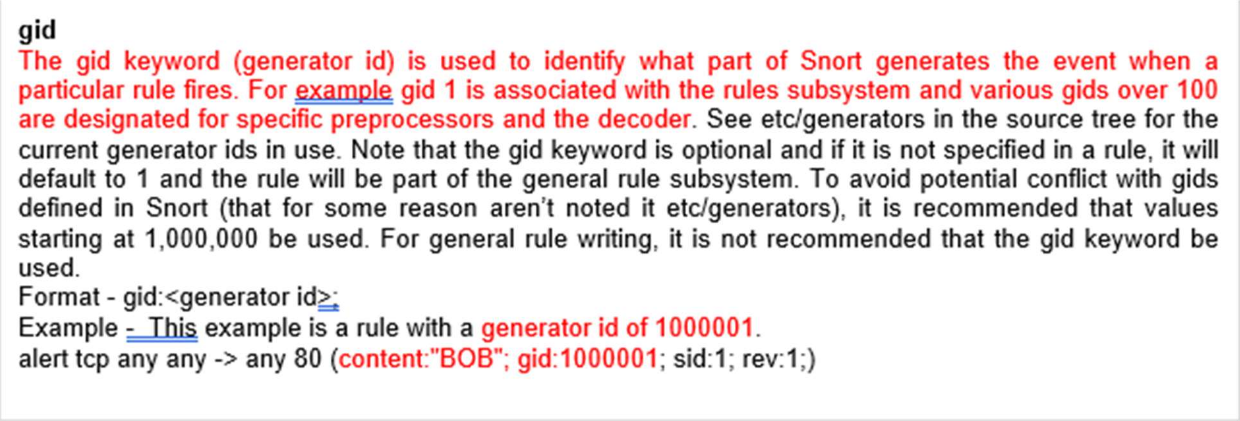
Source : https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page - 40 of 269



Events

The preprocessor uses GID 133 to register events.

Source: https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page - 105 of 269



gid

The gid keyword (generator id) is used to identify what part of Snort generates the event when a particular rule fires. For example gid 1 is associated with the rules subsystem and various gids over 100 are designated for specific preprocessors and the decoder. See etc/generators in the source tree for the current generator ids in use. Note that the gid keyword is optional and if it is not specified in a rule, it will default to 1 and the rule will be part of the general rule subsystem. To avoid potential conflict with gids defined in Snort (that for some reason aren't noted it etc/generators), it is recommended that values starting at 1,000,000 be used. For general rule writing, it is not recommended that the gid keyword be used.

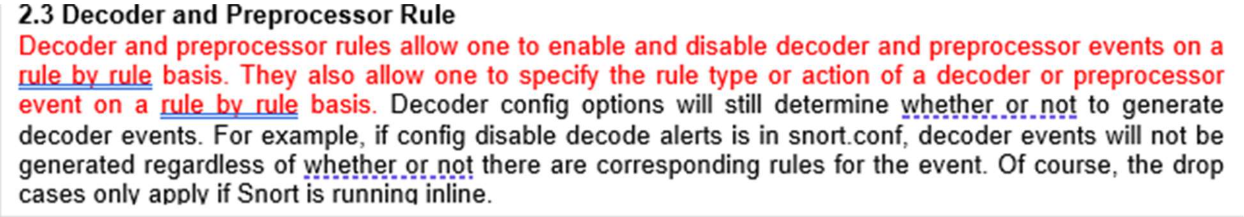
Format - gid:<generator id>;

Example - This example is a rule with a generator id of 1000001.

alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

Source: https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page - 186 of 269

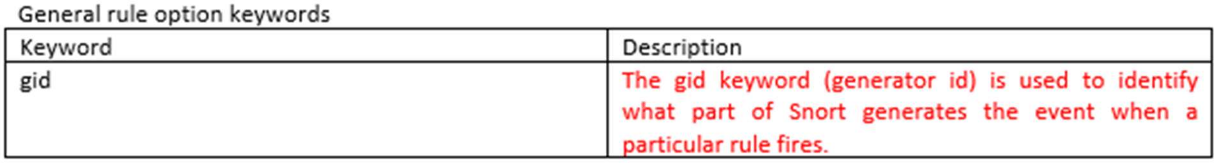
16. In operation, the detecting means analyzes the modified selected packets to detect suspect modified data packets which meet criteria defined by one or more functions in the detecting means, the criteria being indicative of potentially damaging traffic on the network.



2.3 Decoder and Preprocessor Rule

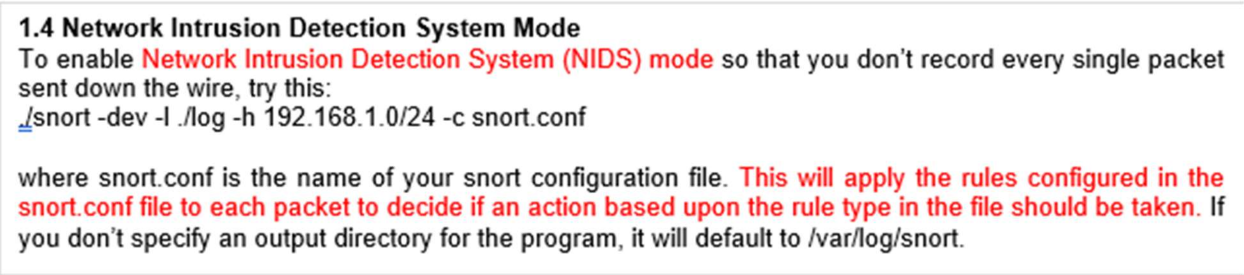
Decoder and preprocessor rules allow one to enable and disable decoder and preprocessor events on a rule by rule basis. They also allow one to specify the rule type or action of a decoder or preprocessor event on a rule by rule basis. Decoder config options will still determine whether or not to generate decoder events. For example, if config disable decode alerts is in snort.conf, decoder events will not be generated regardless of whether or not there are corresponding rules for the event. Of course, the drop cases only apply if Snort is running inline.

Source:https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page 145 of 269



General rule option keywords

Keyword	Description
gid	The gid keyword (generator id) is used to identify what part of Snort generates the event when a particular rule fires.



1.4 Network Intrusion Detection System Mode

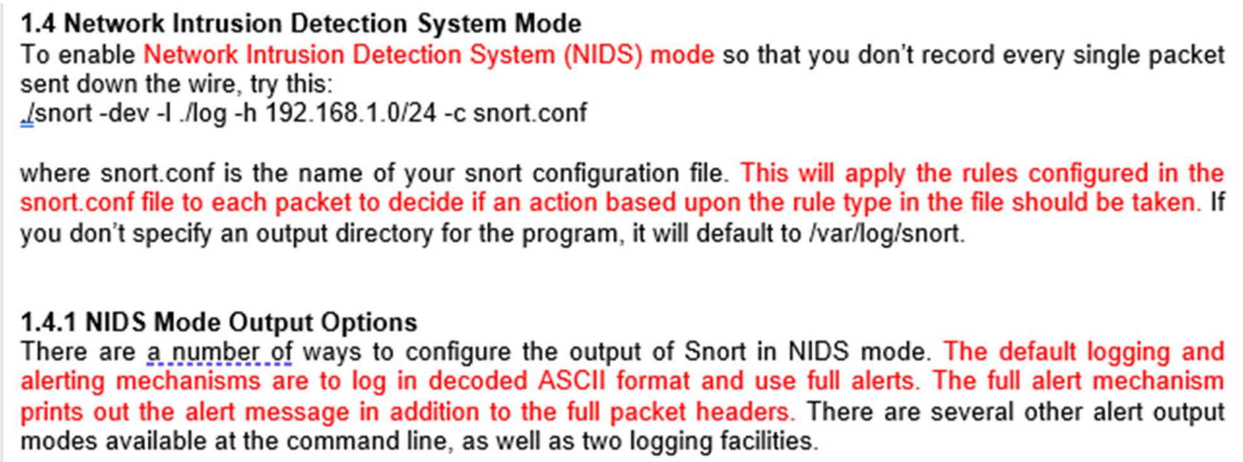
To enable Network Intrusion Detection System (NIDS) mode so that you don't record every single packet sent down the wire, try this:

```
./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf
```

where snort.conf is the name of your snort configuration file. This will apply the rules configured in the snort.conf file to each packet to decide if an action based upon the rule type in the file should be taken. If you don't specify an output directory for the program, it will default to /var/log/snort.

Source:https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page 191 and 12 of 269

17. In operation, the Accused Product forwards details of each detected suspect modified data packet to data processing means.



1.4 Network Intrusion Detection System Mode

To enable Network Intrusion Detection System (NIDS) mode so that you don't record every single packet sent down the wire, try this:

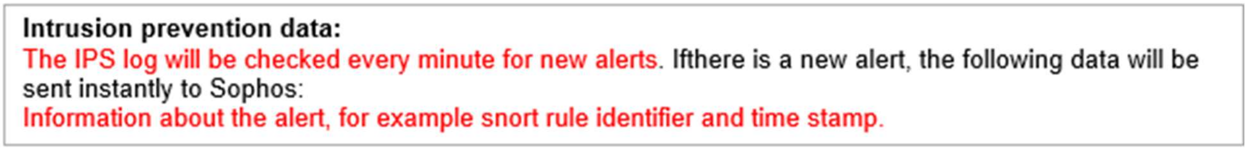
```
./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf
```

where snort.conf is the name of your snort configuration file. This will apply the rules configured in the snort.conf file to each packet to decide if an action based upon the rule type in the file should be taken. If you don't specify an output directory for the program, it will default to /var/log/snort.

1.4.1 NIDS Mode Output Options

There are a number of ways to configure the output of Snort in NIDS mode. The default logging and alerting mechanisms are to log in decoded ASCII format and use full alerts. The full alert mechanism prints out the alert message in addition to the full packet headers. There are several other alert output modes available at the command line, as well as two logging facilities.

Source:https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page 53 and 261 of 269



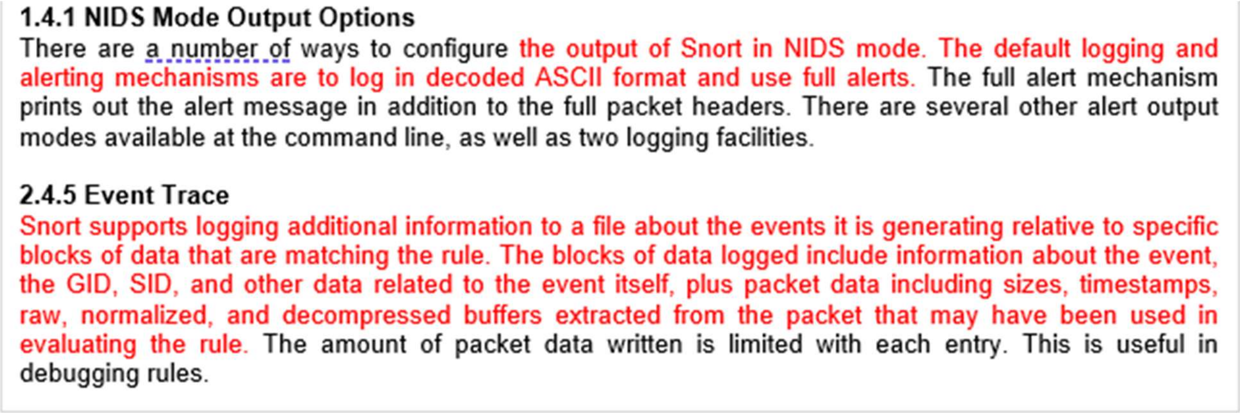
Intrusion prevention data:

The IPS log will be checked every minute for new alerts. Ifthere is a new alert, the following data will be sent instantly to Sophos:

Information about the alert, for example snort rule identifier and time stamp.

Source : https://docs.sophos.com/nsg/sophos-utm/utm/9.703/pdf/en-us/manual-en.pdf Page 60 of 568

18. In operation, the Accused Product stores details of each detected suspect modified data packet so as to be accessible for use in analysis by the data processing means in conjunction with the details of other detected modified suspect packets.



1.4.1 NIDS Mode Output Options

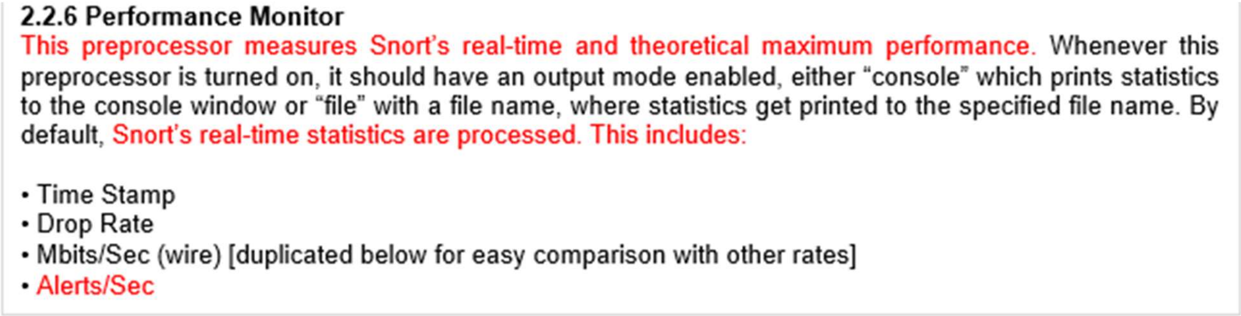
There are a number of ways to configure the output of Snort in NIDS mode. The default logging and alerting mechanisms are to log in decoded ASCII format and use full alerts. The full alert mechanism prints out the alert message in addition to the full packet headers. There are several other alert output modes available at the command line, as well as two logging facilities.

2.4.5 Event Trace

Snort supports logging additional information to a file about the events it is generating relative to specific blocks of data that are matching the rule. The blocks of data logged include information about the event, the GID, SID, and other data related to the event itself, plus packet data including sizes, timestamps, raw, normalized, and decompressed buffers extracted from the packet that may have been used in evaluating the rule. The amount of packet data written is limited with each entry. This is useful in debugging rules.

Source:https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page 12 and 154 of 269

19. using the data processing means to analyze the stored suspect modified data packets.



2.2.6 Performance Monitor

This preprocessor measures Snort's real-time and theoretical maximum performance. Whenever this preprocessor is turned on, it should have an output mode enabled, either "console" which prints statistics to the console window or "file" with a file name, where statistics get printed to the specified file name. By default, Snort's real-time statistics are processed. This includes:

- Time Stamp
- Drop Rate
- Mbits/Sec (wire) [duplicated below for easy comparison with other rates]
- Alerts/Sec

Source:https://snortorgsite.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf Page 21 and 22 of 269

20. Datamonitor has been damaged by Defendant's infringement of the '009 Patent.

PRAYER FOR RELIEF

WHEREFORE, Datamonitor respectfully requests the Court enter judgment against Defendant:

1. declaring that the Defendant have infringed the '009 Patent;

2. awarding Datamonitor its damages suffered as a result of Defendant's infringement of the Patents-in-Suit;

3. awarding Datamonitor its costs, attorneys' fees, expenses, and interest;

4. awarding Datamonitor ongoing post-trial royalties; and

5. granting Datamonitor such further relief as the Court finds appropriate.

JURY DEMAND

Datamonitor demands trial by jury, under Fed. R. Civ. P. 38.

Dated: April 11, 2024

Respectfully Submitted

/s/ Raymond W. Mort, III
Raymond W. Mort, III
Texas State Bar No. 00791308
raymort@austinlaw.com
THE MORT LAW FIRM, PLLC
111 Congress Ave, Suite 500
Austin, Texas 78701
Tel/Fax: (512) 865-7950

ATTORNEYS FOR PLAINTIFF