Suricata IDS Configuration and Tuning

Flowmon IDS Probe Version 2.0.0

Flowmon IDS Probe package integrates 3rd party open-source project Suricata IDS to the Flowmon platform with community rules. This package is provided free of charge and the Flowmon IDS Probe is not covered by Flowmon support service.

This document contains basic instructions for adjusting Suricata IDS settings when it is integrated to the Flowmon platform. It includes the description of basic settings that can be performed directly from the Flowmon user interface or advanced settings that need to be performed from the command-line of the Flowmon appliance.

For more information about Suricata IDS visit its official documentation.

Table of Contents

Introduction

Suricata is an Intrusion detection system (IDS) that detects potential threats in the network traffic. For the detection of these threats, it uses so-called signatures. A signature represents a structured list of rules that describes a threat based on the content of packets. An IDS system then inspects network traffic and applies these rules to each packet that comes through the IDS system. If rules stated in the signature are satisfied for the inspected packet, the IDS system generates an alert to notify the user.

Intrusion detection systems perform *full packet capture* which means that all the packets coming through an IDS system are inspected for a potential intrusion. This process may be very computationally and resource intensive. In addition, for the detection of potential intrusion, these systems usually do not need to inspect all the packets. For this reason, we propose a solution that inspects only first N[1] packets from each network flow. This enables to reduce the load of the Suricata IDS system and to use the system in networks with high amount of traffic.

Configuration in the Flowmon user interface

This section contains description of basic settings that can be configured directly in the Flowmon user interface. For more advanced tuning of the Suricata IDS system (e.g. false positive tuning, suricata rules management), please continue to the next section.

The settings can be found in the **Flowmon Configuration Center**, under the section **Monitoring Ports** (left menu). At this page, it is possible to set the global settings for all interfaces or configure individual interfaces by clicking on tab **IDS probe** in the respective section. The global settings are always applied to all interfaces that have no individual configuration set.

By default, the Suricata IDS monitoring is disabled for all monitoring interfaces, so it is necessary to explicitly enable it for interfaces where the monitoring should be performed. This is possible using the slider with label **Enabled**, that can be found under the tab **IDS probe** for each monitoring interface.

As mentioned above, it is possible to set the individual configuration for each interface when the global setting is not convenient for some reason. It can be enabled by the slider named **Use custom settings.** If this slider is activated, two more options are displayed - **Filter** and **Packet count.**

The first option called **Filter** can be used to enable packet filtering and specify which packets should be processed by the Suricata IDS. The filter can contain more than one filtering rule - in this case, it is necessary to enter **one rule per each line**. In case more rules are provided, the logical conjunction **or** is inserted between rules (at least one rule has to be satisfied to pass the packet for processing). For filtering packets, two types of filtering rules can be used and their syntax is the following:

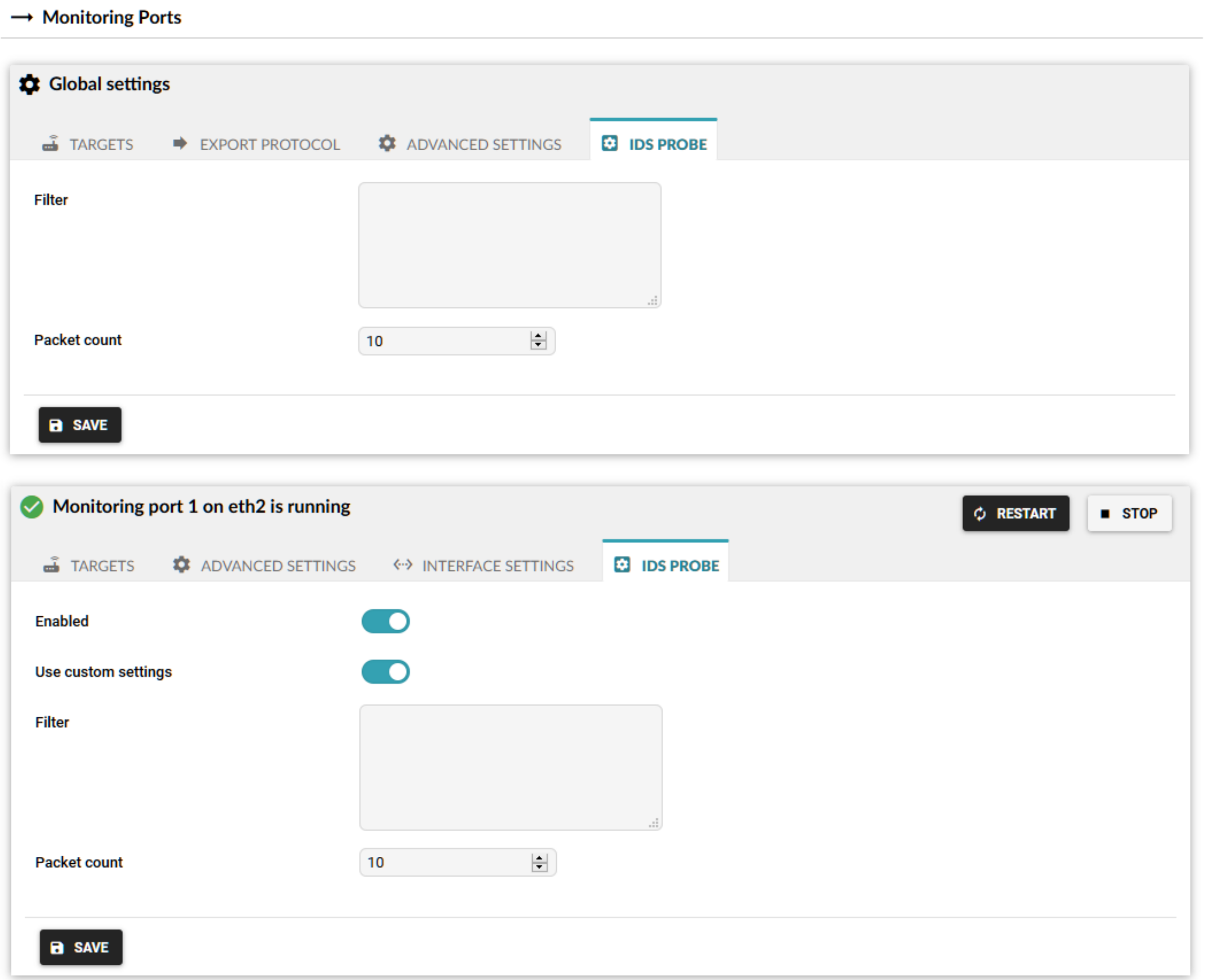
```
ip <ipv4_address>|<ipv6_address>
net <ipv4_address>|<ipv6_address>/<subnet>
```

The first type *ip* can be used to specify the IP address that should be present in the packet header (it is applied to both - source or destination IP address). It supports both IPv4 and IPv6 addresses. It is also possible to specify the entire address range with the **second filter type** `net`. Value of this filter should be valid IPv4 or IPv6 address range in the CIDR notation. As in the previous case, the IP range is applied to both - source or destination IP address.

[1] N is a value that can be specified by a user, the default value is 10 packets.

As mentioned in the Introduction chapter, only the first N packets from each flow are passed to the Suricata IDS system for inspection. To adjust this value, the option **Packet count** can be used. By default, this value is set to 10 packets. The value can be in the range from 3-100 packets.

In the following screenshot, it is possible to see the configuration of the IDS probe in the **Flowmon Configuration Center.**



→ Monitoring Ports

Global settings

Filter

Packet count: 10

Monitoring port 1 on eth2 is running

Enabled: ●

Use custom settings: ●

Filter

Packet count: 10

Configuration in the command line

This section contains description of advanced settings of the Suricata IDS system. These settings can be configured only using the command-line interface. Please note that after every change, it is necessary to restart the plugin (see Suricata IDS Probe restart section for more information). **Please note that every restart of the IDS probe leads to the restart of the Flowmon exporter, so the possible loss of flow data may be encountered.**

False positive tuning with “suppress"

When there are too many uninteresting events detected, we can suppress any of them in the threshold configuration file saved as **`/data/idsp/threshold.config`**.

Syntax of suppress rule is the following: `suppress gen_id <gid>, sig_id <sid>`

If we want to suppress one or more IP addresses in specific signature, we can do it with suppress rule:

```
suppress gen_id <gid>, sig_id <sid>, track
<by_src|by_dst|by_either>, ip <ip|subnet|addressvar>
```

To select all signatures or all groups, select **`sig_id 0`** or **`gen_id 0`**.

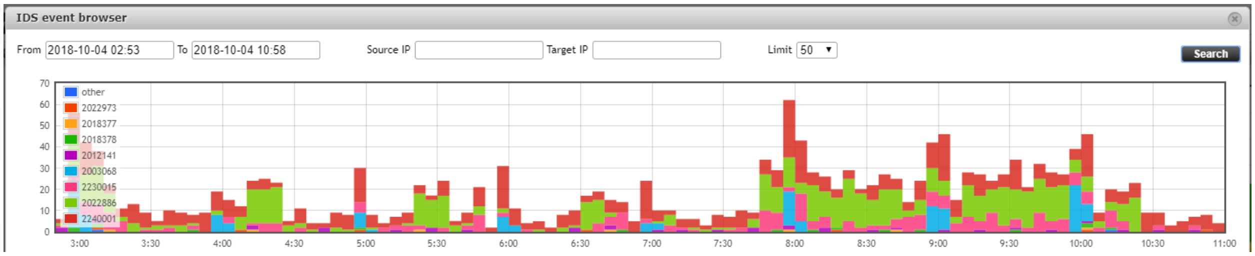
Log in as user flowmon to IDS probe.

```
vim /data/idsp/threshold.config
```

Write **`suppress gen_id 1, sig_id 2022886`**

Restart IDS Probe (in FCC/Versions Stop and Start IDS Probe package).

See the result in the dashboard:



IDS event browser

From 2018-10-04 02:53 To 2018-10-04 10:58 Source IP Target IP Limit 50

For example, in our environment, signature 2022886 was generating too many events, so we suppressed it with **`suppress gen_id 1, sig_id 2022886`** in **`/data/idsp/threshold.config`** file.

Signature 2022886 is displayed in green and as we can see after 10:25 when we processed the suppress, this event is no longer displayed.

For more information, see [the official](#) documentation of the Suricata IDS.

Setup of network variables in Suricata config file

It helps to describe networks as variables which can be used for suppression or rule setup.

IP addresses can be defined as variables, set at the beginning of **`/data/idsp/suricata.yaml`** file.

Log in as user flowmon to IDS probe.

`vim /data/idsp/suricata.yaml`
Set some variables, you can also use negation: **`EXTERNAL_NET : “!$HOME_NET”`**
Now you can use these variables in rules or suppress commands.

Example:
`suppress gen_id 1, sig_id 0, track by_src, ip $EXTERNAL_NET`
This rule suppresses events, where source IP addresses are from the external network.

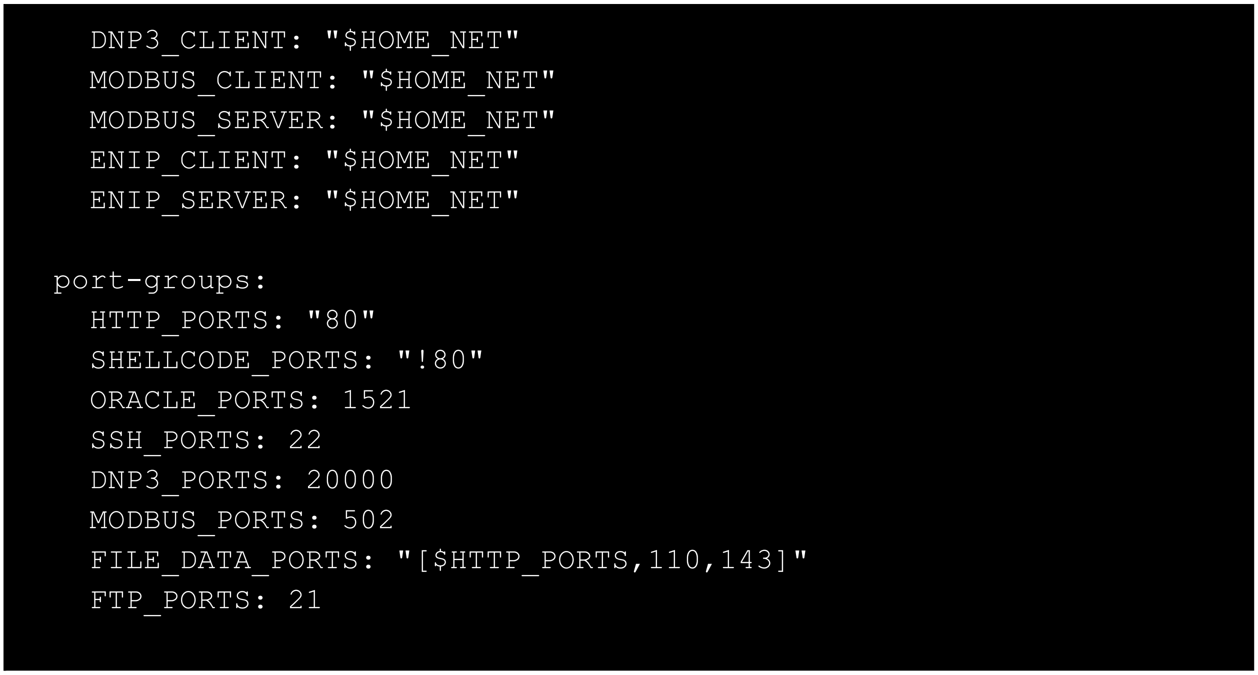
Restart IDS Probe (in FCC/Versions Stop and Start IDS Probe package).

For more information, see the official documentation of the Suricata IDS.

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DNP3_SERVER: "$HOME_NET"
```



```
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

  port-groups:
    HTTP_PORTS: "80"
    SHELLCODE_PORTS: "!80"
    ORACLE_PORTS: 1521
    SSH_PORTS: 22
    DNP3_PORTS: 20000
    MODBUS_PORTS: 502
    FILE_DATA_PORTS: "[$HTTP_PORTS,110,143]"
    FTP_PORTS: 21
```

Figure: list of variables in suricata.yaml file

Suricata rules management

The path to rule files for Suricata must be added to suricata.yaml file, so it knows where it can find the .rules files and which of them it can use.

List of rules with signatures

Rules can be found here: **`/data/idsp/rules`**

Enable or disable rule

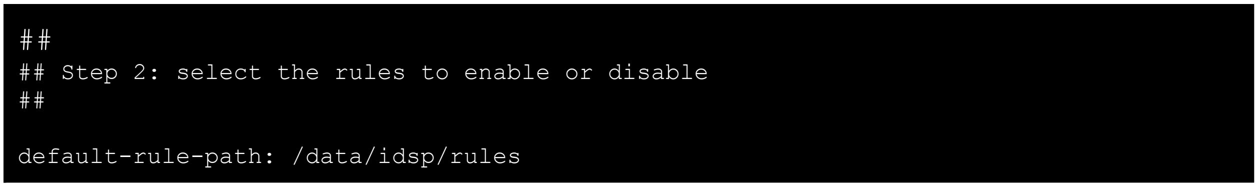
Log in as user flowmon to IDS probe.

`vim /data/idsp/suricata.yaml`

The default path is set, you can set other paths to specific rules (then the default path will be ignored to this one rule).

Example with new rule in different path:

- **`/example/rules/mynewrules.rules`**



```
##
## Step 2: select the rules to enable or disable
##

default-rule-path: /data/idsp/rules
```

```
rule-files:
 - botcc.rules
 # - botcc.portgrouped.rules
 - ciarmy.rules
 - compromised.rules
 - drop.rules
 - dshield.rules
# - emerging-activex.rules
 - emerging-attack_response.rules
 - emerging-chat.rules
 - emerging-current_events.rules
 - emerging-dns.rules
 - emerging-dos.rules
 - emerging-exploit.rules
 - emerging-ftp.rules
# - emerging-games.rules
# - emerging-icmp_info.rules
# - emerging-icmp.rules
 - emerging-imap.rules
# - emerging-inappropriate.rules
# - emerging-info.rules
 - emerging-malware.rules
 - emerging-misc.rules
 - emerging-mobile_malware.rules
 - emerging-netbios.rules
 - emerging-p2p.rules
 - emerging-policy.rules
 - emerging-pop3.rules
 - emerging-rpc.rules
# - emerging-scada.rules
# - emerging-scada_special.rules
 - emerging-scan.rules
# - emerging-shellcode.rules
 - emerging-smtp.rules
 - emerging-snmp.rules
 - emerging-sql.rules
 - emerging-telnet.rules
 - emerging-tftp.rules
 - emerging-trojan.rules
 - emerging-user_agents.rules
 - emerging-voip.rules
 - emerging-web_client.rules
 - emerging-web_server.rules
# - emerging-web_specific_apps.rules
 - emerging-worm.rules
 - tor.rules
# - decoder-events.rules # available in suricata sources under rules dir
# - stream-events.rules  # available in suricata sources under rules dir
 - http-events.rules    # available in suricata sources under rules dir
 - smtp-events.rules    # available in suricata sources under rules dir
 - dns-events.rules     # available in suricata sources under rules dir
 - tls-events.rules     # available in suricata sources under rules dir
# - modbus-events.rules  # available in suricata sources under rules dir
# - app-layer-events.rules  # available in suricata sources under rules dir
# - dnp3-events.rules       # available in suricata sources under rules dir
# - ntp-events.rules       # available in suricata sources under rules dir
# - local.rules
```

Add a new online source with signatures (rules)

When we want to use rules from external sources, we need to add URL to these files to **`oinkmaster.config`** file.

```
vim /data/idsp/oinkmaster.conf
```

```
# URL examples follows. Replace <oinkcode> with the code you get on the
# Snort site in your registered user profile.

url = https://services.flowmon.com/rules/public/emerging.rules.tar.gz

# Example for Snort 2.4
# url =
http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-2.4.tar.gz
```

For more information, see the official documentation of the Suricata IDS.

GID - Group/Generator ID

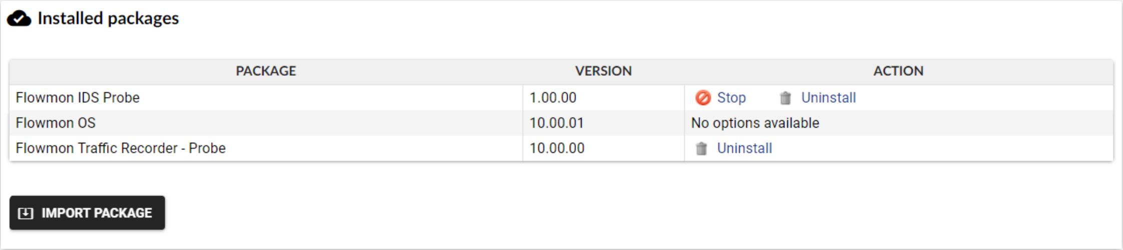
We can set gid when creating for example new rule or prepare copy of some rule for test purpose. Default gid is 1 for all rules, the new one must be greater than 1 000 000.

Then you can use the gid to suppress rules.

```
alert tls any any -> any any (msg:"SURICATA TLS invalid record version"; flow:established;
app-layer-event:tls.invalid_record_version; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; gid:1000001; sid:2230015; rev:1;)
```

Suricata IDS Probe restart

After each configuration change, the IDS Probe should be restarted to update the changed settings. This can be done in the **Flowmon Configuration Center (FCC)**, section **Versions** (left menu). Then click on the **stop** button in the row with Flowmon IDS Probe package, and after that **start** button again. **Please note that every restart of the IDS probe leads to the restart of the Flowmon exporter, so the possible loss of flow data may be encountered.**



PACKAGE	VERSION	ACTION
Flowmon IDS Probe	1.00.00	Stop Uninstall
Flowmon OS	10.00.01	No options available
Flowmon Traffic Recorder - Probe	10.00.00	Uninstall