Suricata IDS Configuration and Tuning

Flowmon IDS Probe Version 3.2.3 rev. 12/22

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.

For more information about Suricata IDS visit its official documentation.

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.

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 allows to reduce the load of the Suricata IDS system and to use the system in networks with high amounts of traffic.

Configuration in the Flowmon user interface

This section contains a 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>
```

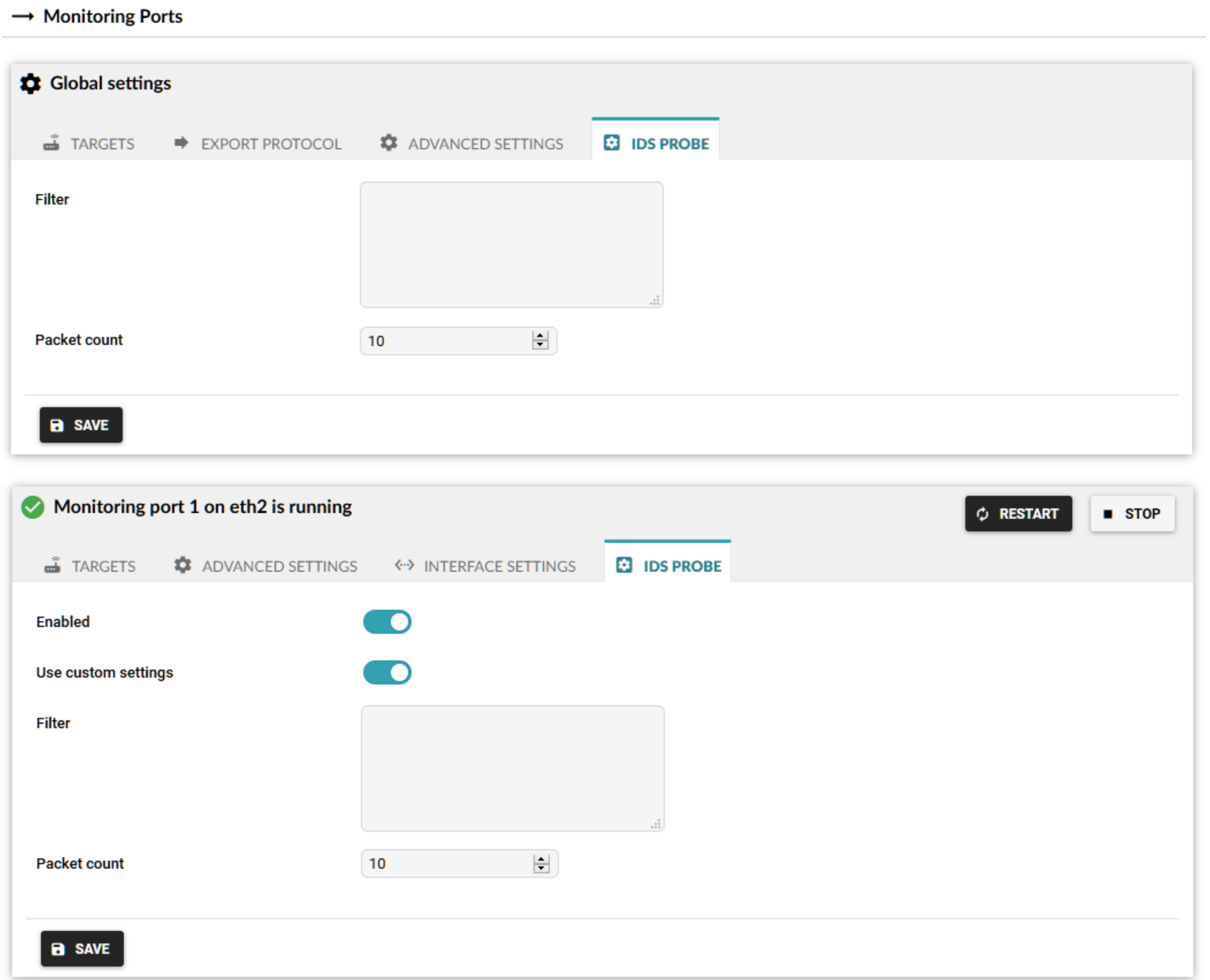
The first type *`ip`* can be used to specify the IP address that should be present in the packet header (it is applied to both - source or destination IP address). It supports both IPv4 and IPv6 addresses. It is also possible to specify the entire address range with the **second filter type** `net`.

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

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.

As mentioned in the [Introduction](#) chapter, only the first N packets from each session (per bi-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 (i.e., 5 packets from both directions). 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.**



Global settings

Filter

Packet count 10

Monitoring port 1 on eth2 is running

Enabled

Use custom settings

Filter

Packet count 10

Detected IDS events are sent via syslog:

- To all servers defined in Syslog event logging settings (Flowmon Configuration Center - System - System settings). Selecting or deselecting any of "Configure Syslog Message" groups does not affect IDS Probe.
- Directly to IDS Collector in the Flowmon ADS module if installed on the same machine.

Detected events are stored in /data/idsp/outputs/eve.json file. The json file is processed by syslog-ng according to the configuration file /etc/syslog-ng/conf.d/idsp.conf. In the idsp.conf, you can configure sending of events via syslog manually.

IDS Probe can be stop/start via **Flowmon Configuration Center** (Version - Flowmon IDS Probe - stop/start).

Configuration in the command line

This section contains a description of advanced settings of the Suricata IDS system. These settings can be configured only using the command-line interface.

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/user-config/threshold.config**.

Syntax of suppress rule is the following:

```
suppress gen_id <gid>, sig_id <sid>
```

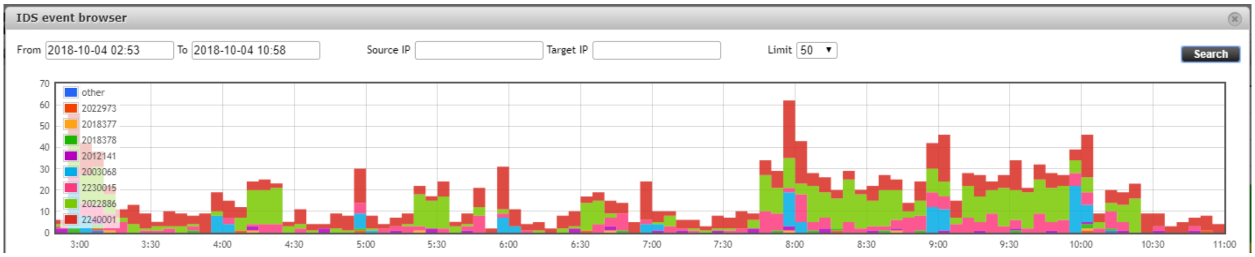
If we want to suppress one or more IP addresses in specific signature, we can do it with suppress rule:

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

Example for signature with ID 2022886:

1. Log in as user flowmon to IDS probe.
2. vim **/data/idsp/user-config/threshold.config**
3. Write **suppress gen_id 1, sig_id 2022886**
4. Restart IDS Probe
5. Check the result in IDS event browser:



IDS event browser

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

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.

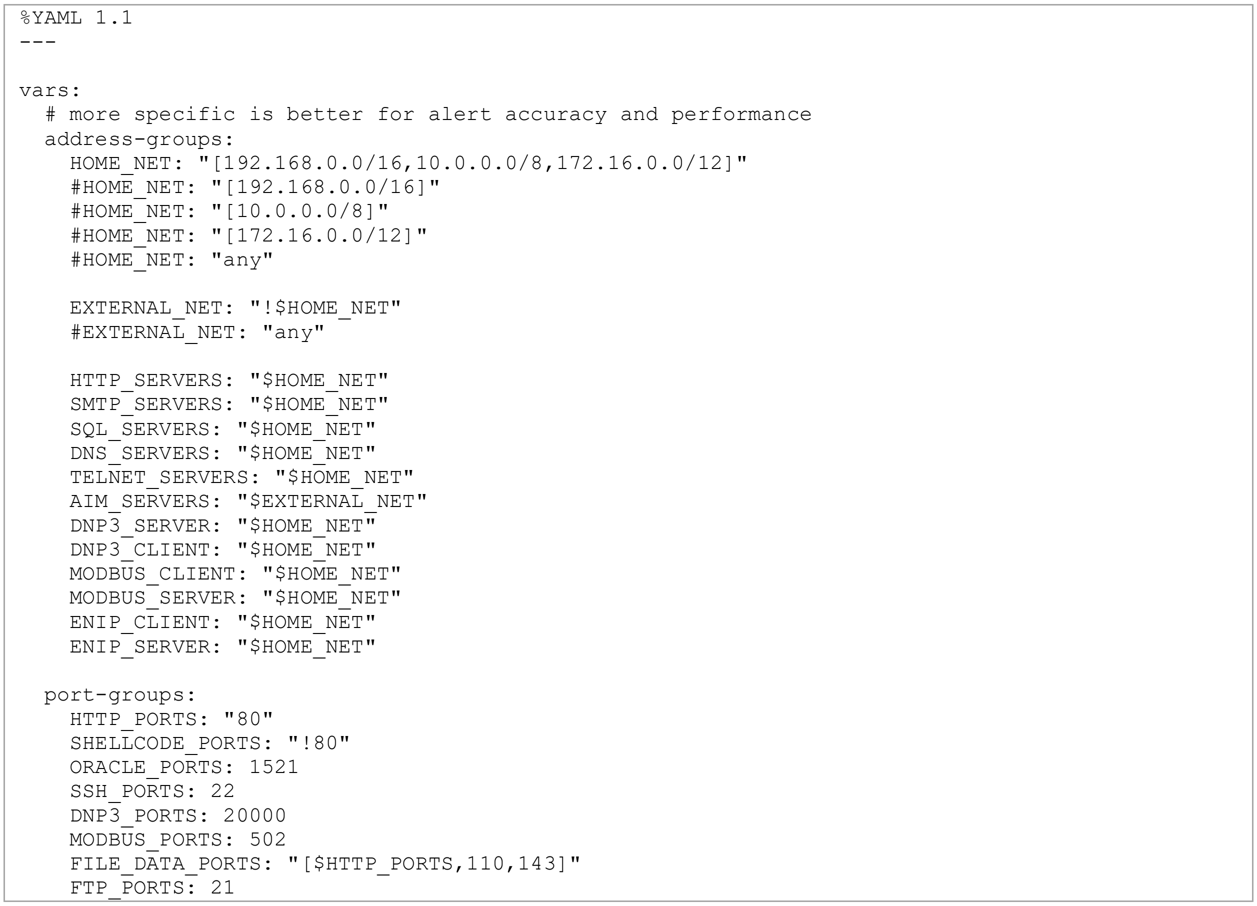
Setup of network variables in Suricata config file

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

IP addresses can be defined as variables in the **/data/idsp/user-config/suricata.yaml** file.

1. Log in as user flowmon to the Flowmon IDS Probe.
2. vim **/data/idsp/user-config/suricata.yaml**
3. 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.
4. Restart IDS Probe

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



```
%YAML 1.1
---

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

For management of the rules, Flowmon IDS Probe uses preconfigured Suricata-Update tool. The tool gathers rules from multiple sources combining them into one **suricata.rules** file.

By default, the tool is configured to gather rules from two sources:

- **Flowmon Services** (Remote Rule Source)
    - Flowmon copy of Emerging Threats Open Rules.
    - If the services.flowmon.com is not reachable, offline backup is used.
- **/data/idsp/user-config/rules** (Local Rule Source)
    - All files ending in ***.rules*** inside this folder are loaded.
    - The directory is empty after a new installation. The folder is intended to be used for the user-defined rules.

The rules sources can be adjusted via configuration files:

- **/data/idsp/user-config/update.yaml**
    - ⊄ Attributes *sources* and *local* can be used to add additional remote or local sources. Default sources provided by the Flowmon IDS Probe are not visible in this configuration file.
    - ⊄ Examples for *sources* attribute:

```
# Remote rule sources. Simply a list of URLs.
sources:
  # Emerging Threats Open with the Suricata version dynamically replaced.
  # -
https://rules.emergingthreats.net/open/suricata-%(__version__)s/emerging.rules.t
ar.gz
  # The SSL blacklist, which is just a standalone rule file.
  # - https://sslbl.abuse.ch/blacklist/sslblacklist.rules
```

- **/data/idsp/user-config/flowmon-idsp-suricata-update.yaml**
    - ⊄ Attribute *enable_flowmon_rules_feed* allows you to disable the default rules from Flowmon Services feed. Deactivation is useful for completely replacing default rules with your own rules source.

Suricata-Update tool allows users to customize rulesets via separated configuration files. The order of application of configuration files and their meaning is following:

- /data/idsp/user-config/**disable.conf** (deactivate rules)
- /data/idsp/user-config/**enable.conf** (activate deactivated rules)
- /data/idsp/user-config/**drop.conf** (convert rules action to “drop”, not usable for IDSP)
- /data/idsp/user-config/**modify.conf** (rewrite rules definition)

Configuration files inside /data/idsp/user-config/ folder can be recreated (if they are missing or invalid) by copying their original version in the following way:

```
cp /data/components/flowmon-idsp-suricata-update/etc/suricata/* /data/idsp/user-config/
```

The configuration will be applied during the next execution of the Suricata-Update tool. The tool is scheduled to be executed every hour. If you want to speed up the process, you can manually restart the service by executing command:

```
sudo systemctl restart flowmon-idsp-suricata-update
```

For more information about suricata-update tool configuration files and rule matching please visit the official documentation.

Please note that Flowmon IDS Probe uses own service for executing suricata-update tool.
Do not run suricata-update command directly.

GID - Group/Generator ID

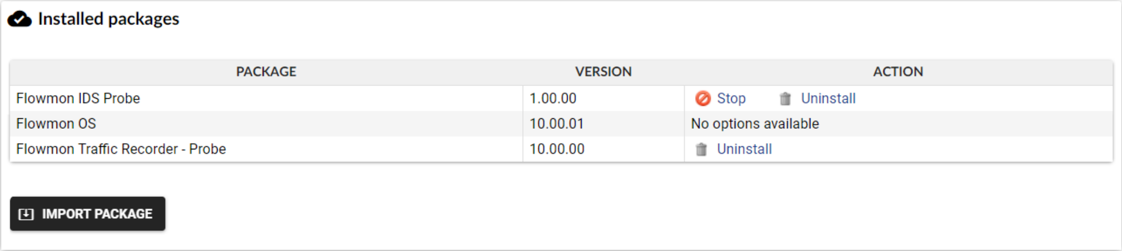
We can set gid when creating for example new rules or prepare a copy of some rule for test purposes. Default gid is 1 for all rules, the new one must be greater than 1 000 000.

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

The restart of the Flowmon IDS Probe 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.



Installed packages

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

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.

Please note that Flowmon IDSP Probe uses own service for executing suricata.
Do not run suricata command directly.

Appendix A: Encapsulation Support

The list of supported encapsulations on Flowmon Probe and IDS Probe.

Protocol	Flowmon Probe	IDS Probe
GRE	Y	Y
ERSPAN	Y	Y
VLAN	Y	Y
MPLS	Y	Y
VxLAN	Y	Y
PPPoE	Y	Y[1]
ESP	Y	N
4in6	Y	Y

[1] - PPPoE decapsulation must be enabled on exporter to pass it to the IDS Probe.