How to install Suricata IDS on the Vigor 3912S routers?

suricata IDS 3912S installation

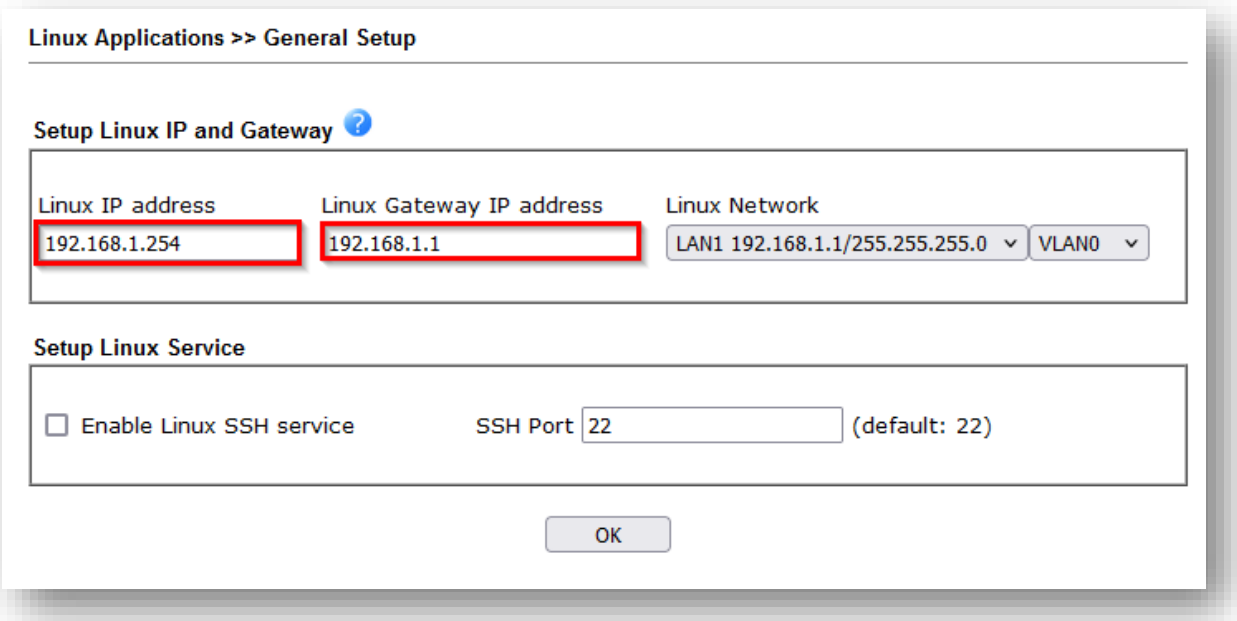
The Vigor 3912S routers can run multiple applications on its built-in SSD drive. There is some software already preinstalled to make this process even quicker. By default, Suricata, VigorConnect, and other applications are available on the router.

Thanks to Docker and router's WUI integration, enabling Suricata is a matter of a few mouse clicks.

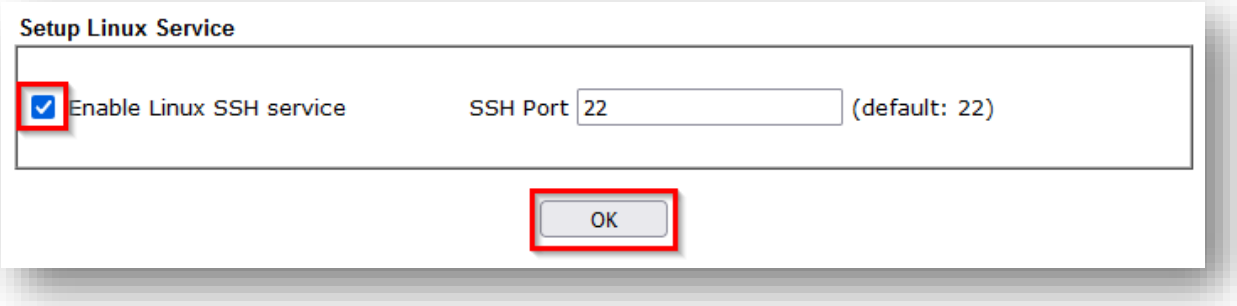
This article depicts activation process of Suricata IDS on the Vigor 3912S routers.

Note: please make sure that the router is connected to the Internet so that the latest version of software is used.

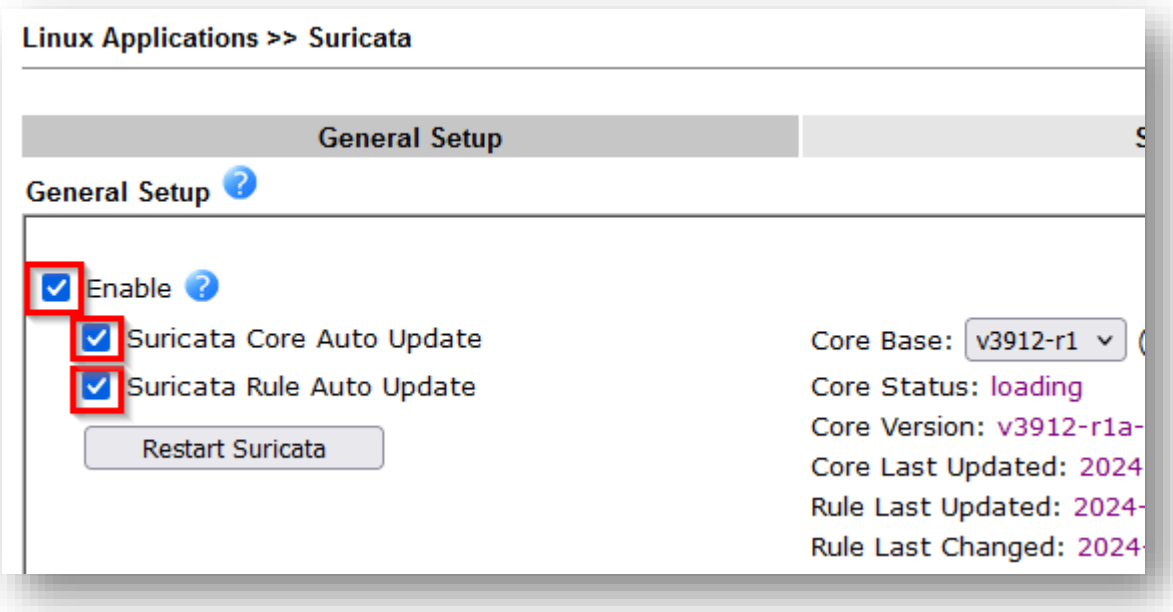
1. Configuration of the Linux Application layer on the router
   The **[Linux Application] > [General Setup]** page should be configured so that pre-installed or new Docker-compatible applications can be run on the router.
   The **Linux IP address** and **Linux Gateway IP address** fields must be populated with the IP address and network range of your choice.



Activation of the **Linux SSH service**, although optional, is highly recommended.



2. Navigate to **[Linux Applications] > [Suricata]**, select **Enable**, and the **Suricata Core Auto Update** and **Suricata Rule Auto Update** options which check daily for the latest version that is then automatically installed.



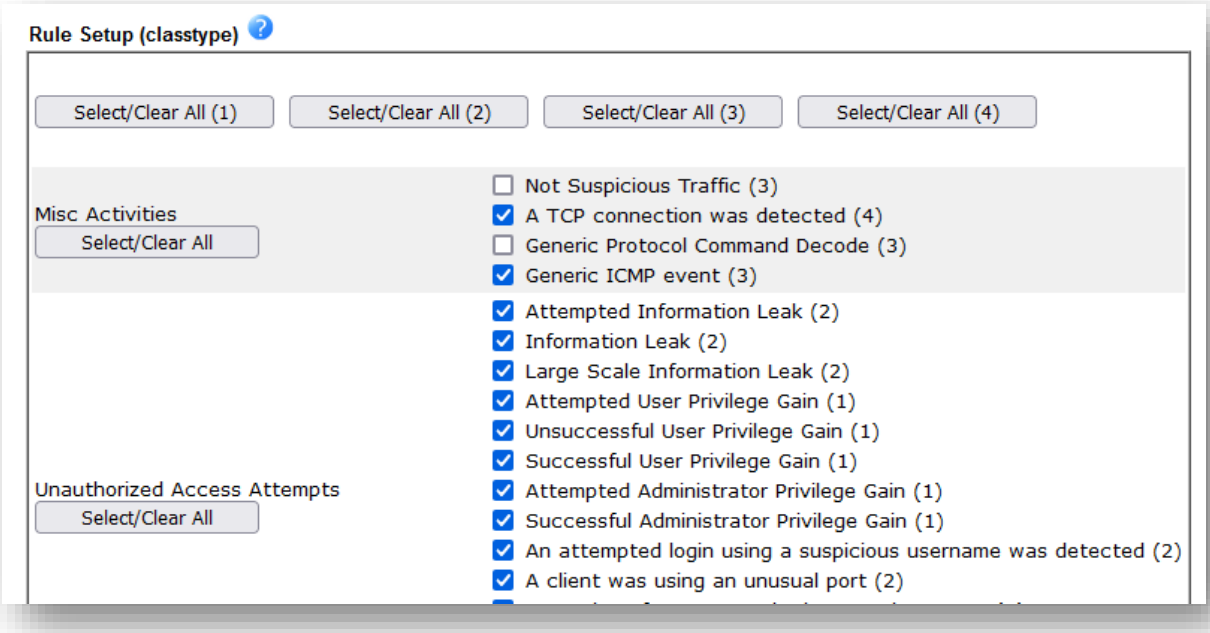
Notes:
Core Base – two core base options are available. V3912-r1 uses Suricata version 6.0.x; v3912-r2 uses Suricate version 7.0.x; The current Suricata version will be shown next to the Core Base drop-down menu.

Suricata Core Auto Update is run every 24 hours to check for the latest core image. Once downloaded, the new image will be used after the next router reboot.

Suricata Core Auto Update – this process should run at around 6:30 am local time (each day).

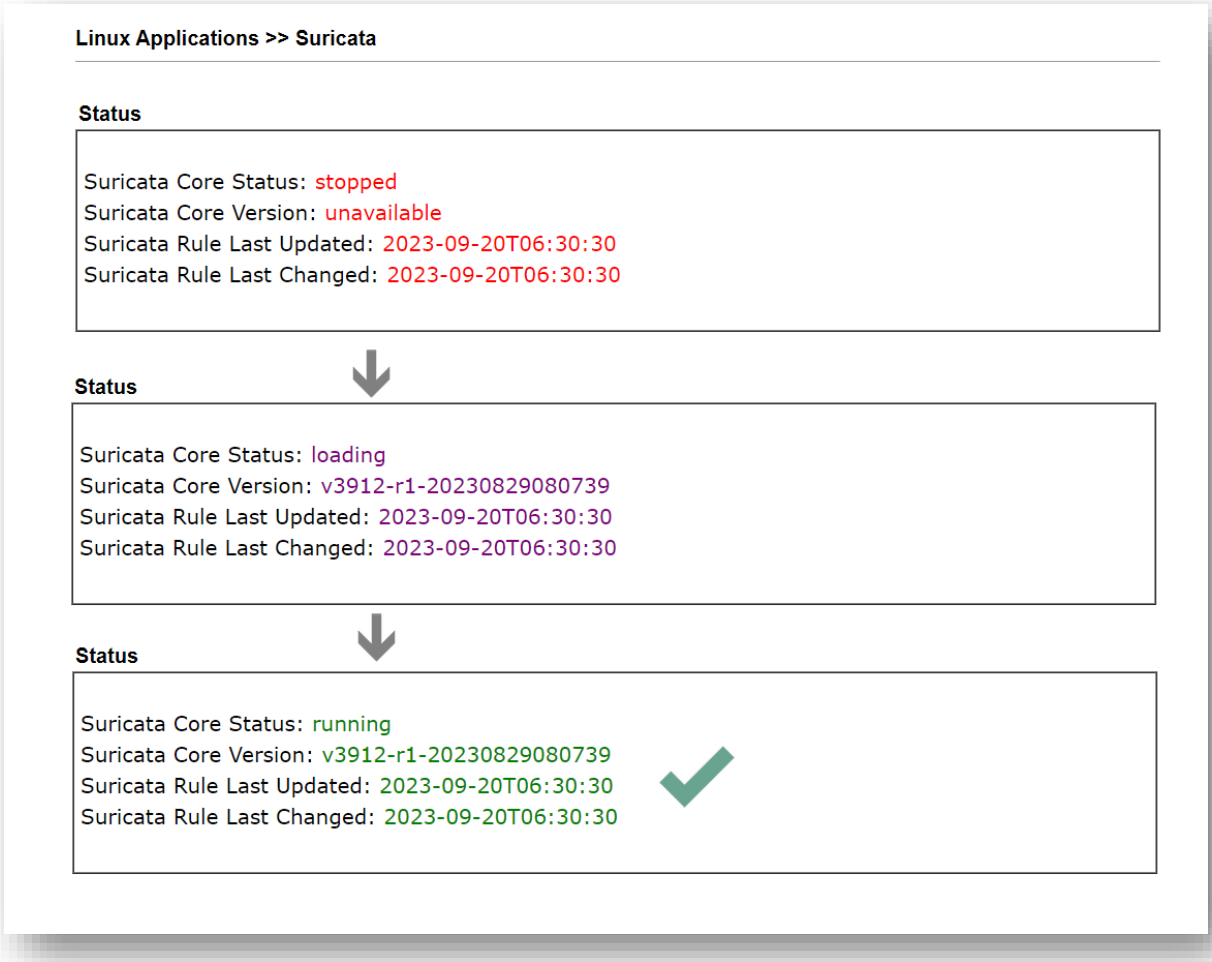
If the core image isn't update, some Suricata rules may have received an update thanks to the core image SOP process that detects and updates the rules.

3. With over 60k rules, including the 6k+ CVE definitions, it is worth selecting the right rules. There are 4 priority levels. Use the **Select/Clear All (x)** buttons to activate specific category. Number 1 is the highest priority (out of 4).

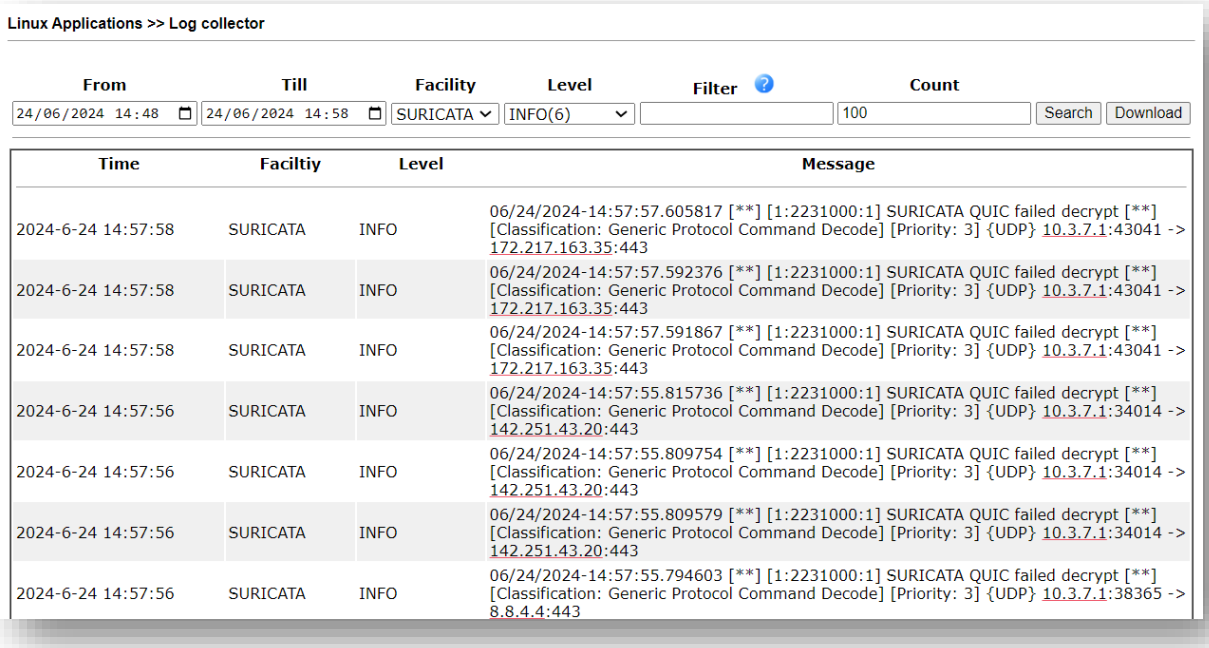


Note 2:

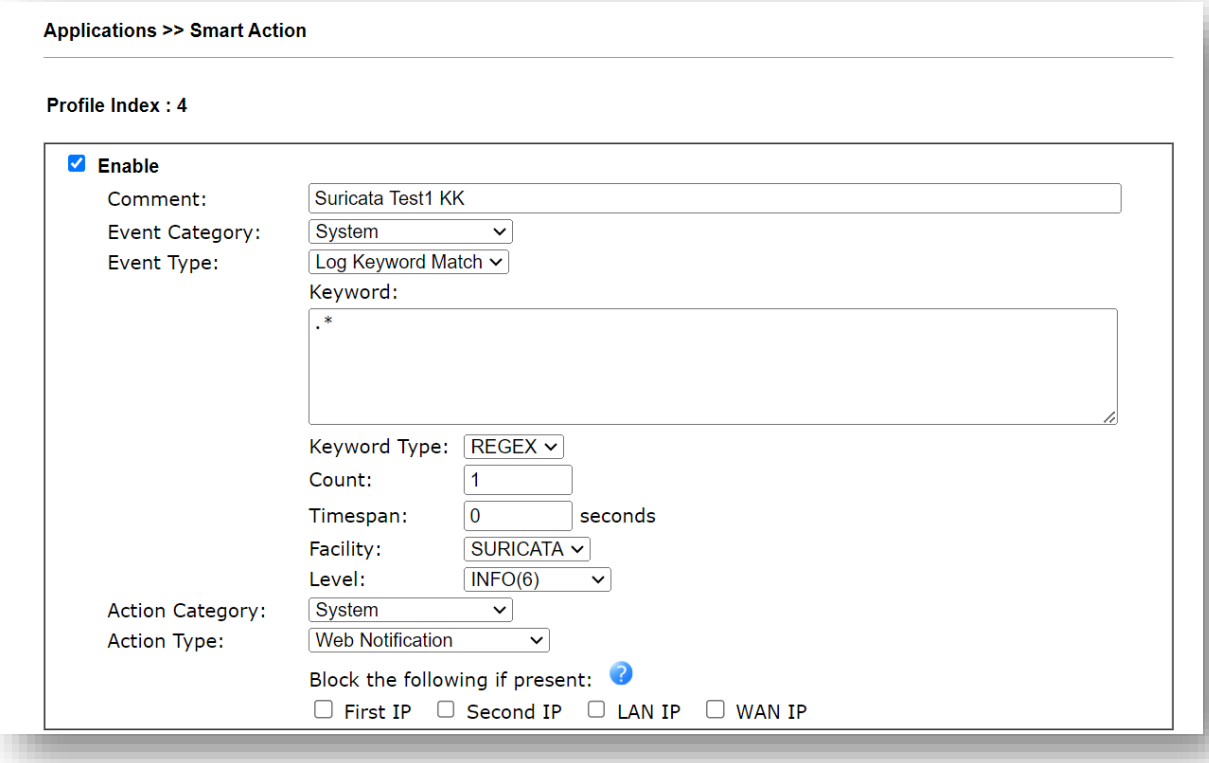
Once some rules have been selected, Suricata helps to detect the network activities. If the Suricata rule is changes, Vigor 3912S will reload the Suricata service.



4. Go to **[Linux Applications] > [Log Collector]**. Select the time range and SURICATA as the Facility to view the network events that SURICATA detected. The detected events may not all really the bad ones. We have to check which network event trigger the log and determine the further action. If the network event is the normal one, we can deselect the specific class rule from the Rule Setup.



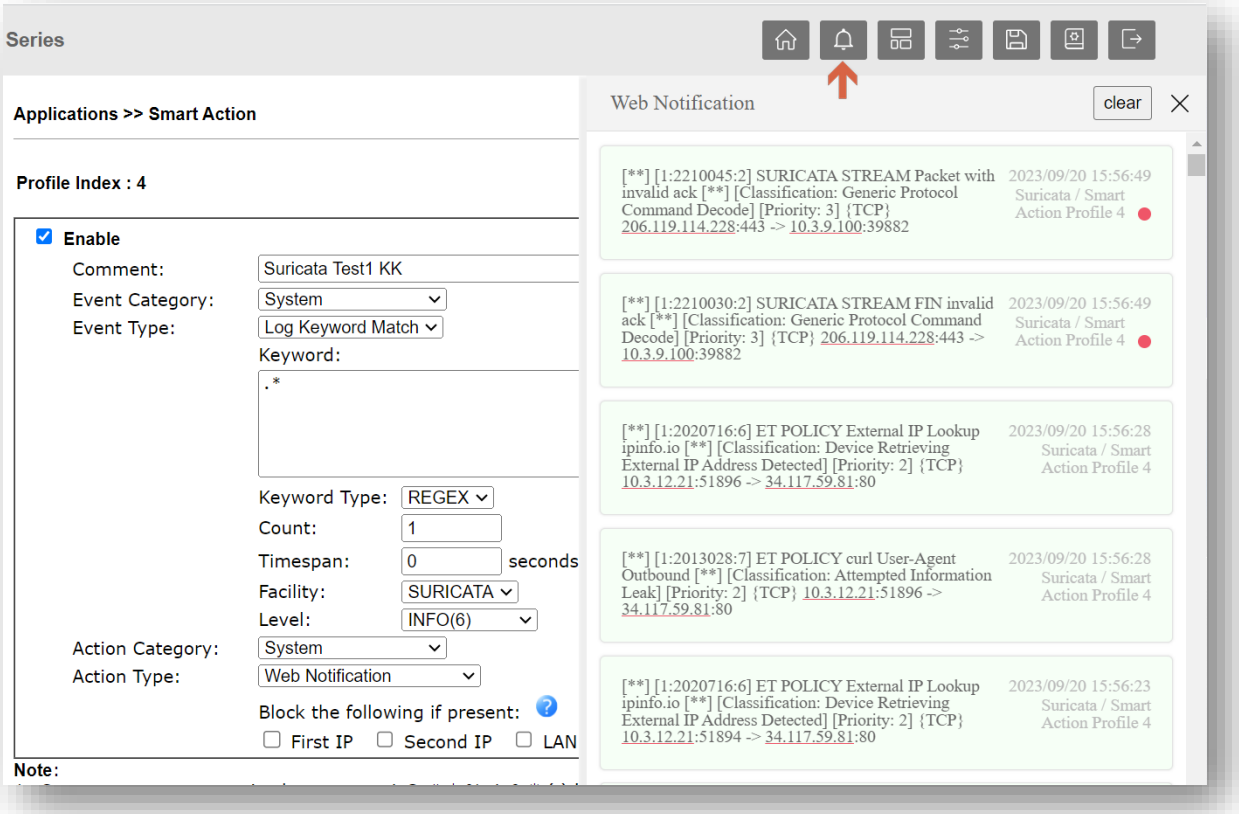
5. (optional) Enable Smart Action to receive the Suricata notifications



a) -Select System for the Event Category
b) -Select Log Keyword Match for the Event Type
c) -Enter .* in the Keyword Content. That means any log.

d) -Keyword Type REGEX or TEXT REGEX stands for Regular Expression, which allows us to use the defined pattern to search. TEXT is the string, usually not used with the special characters.
e) -Count 1 Time Span 0 second means to send web notification for any event.
f) -Select SURICATA for Facility
g) -Select INFO(6) for Level.
h) -Select System for the Action Category
i) -Select Web Notification for the Action Type

6. Monitoring
The little bell button indicates about any new notifications.

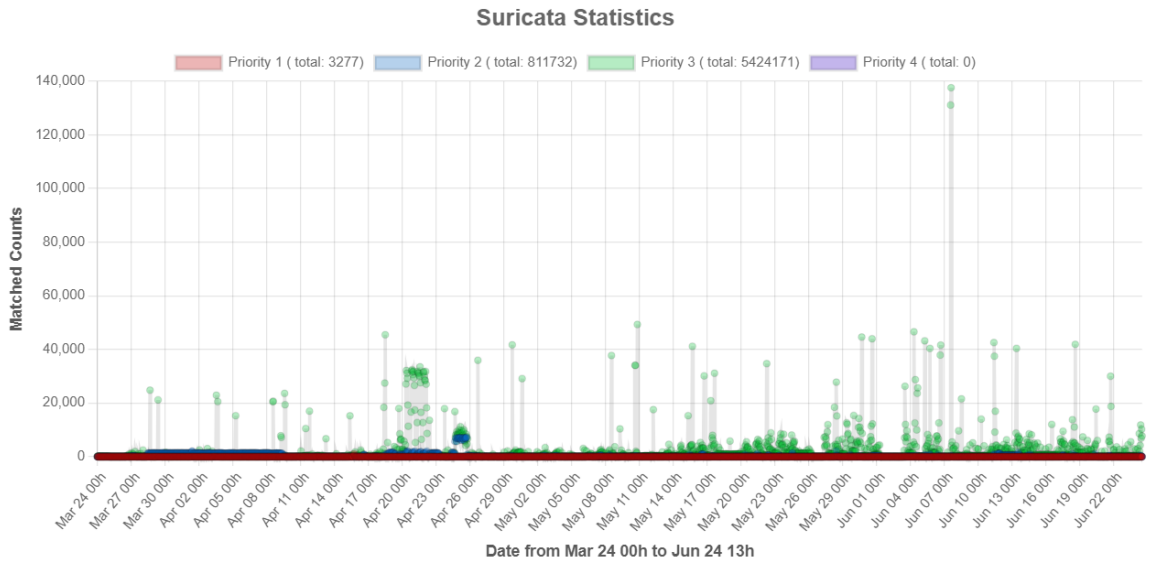


We can see all the Suricata rule matched counts in the network on the **Statistics** page.

Linux Applications >> Suricata

General Setup	Statistics

Show Chart: All All



Refresh