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.

 Configuration of the Linux Application layer on the router The [Linux Application] > [General Setup] page should be configured so that preinstalled 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.

etup Linux IP and Ga	teway 😯	
Linux IP address 192.168.1.254	Linux Gateway IP address 192.168.1.1	Linux Network LAN1 192.168.1.1/255.255.255.0 VLAN0 V
Setup Linux Service	service SSH Port 22	(default: 22)

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

Setup Linux Service			
Enable Linux SSH service	SSH Port 22	(default: 22)	
	ОК		

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.

General Setup	
General Setup 😨	
Enable 🕜	
Suricata Core Auto Update	Core Base: v3912-r1 v
🗹 Suricata Rule Auto Update	Core Status: loading
Bestart Surjeta	Core Version: v3912-r1a
Residit Suncata	Core Last Updated: 2024
	Rule Last Updated: 2024
	Pule Last Changed: 202/

## 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).

Select/Clear All (1) Select	/Clear All (2) Select/Clear All (3) Select/Clear All (4)
	Not Suspicious Traffic (3)
Misc Activities	A TCP connection was detected (4)
Select/Clear All	Generic Protocol Command Decode (3)
	Generic ICMP event (3)
	Attempted Information Leak (2)
	Information Leak (2)
	Large Scale Information Leak (2)
	Attempted User Privilege Gain (1)
	✓ Unsuccessful User Privilege Gain (1)
	Successful User Privilege Gain (1)
Unauthorized Access Attempts	Attempted Administrator Privilege Gain (1)
Select/Clear All	Successful Administrator Privilege Gain (1)
	An attempted login using a suspicious username was detected (2)
	A client was using an unusual port (2)

## 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.

#### Status

Suricata Core Status: stopped Suricata Core Version: unavailable Suricata Rule Last Updated: 2023-09-20T06:30:30 Suricata Rule Last Changed: 2023-09-20T06:30:30

 $\mathbf{J}$ 

S	tatı	us	

Suricata Core Status: loading Suricata Core Version: v3912-r1-20230829080739 Suricata Rule Last Updated: 2023-09-20T06:30:30 Suricata Rule Last Changed: 2023-09-20T06:30:30

J

#### Status

Suricata Core Status: running Suricata Core Version: v3912-r1-20230829080739 Suricata Rule Last Updated: 2023-09-20T06:30:30 Suricata Rule Last Changed: 2023-09-20T06:30:30

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.

Linux Applications >> Log	collector							
From	Till	Facility	Level	Filter	0	Count		
24/06/2024 14:48	24/06/2024 14:58	SURICATA •	✓ INFO(6) ✓			100	Search	Download
Time	Faciltiy	Level			Mes	sage		
2024-6-24 14:57:58	SURICATA	INFO	06/24/2024-14:57: [Classification: Gene 172.217.163.35:443	57.605817 [* eric Protocol C	*] [1:22310 Command D	000:1] SURICATA QU ecode] [Priority: 3]	UIC failed decry {UDP} <u>10.3.7.1</u>	pt [**] .:43041 ->
2024-6-24 14:57:58	SURICATA	INFO	06/24/2024-14:57: [Classification: Gene 172.217.163.35:443	57.592376 [* ric Protocol C B	*] [1:22310 Command D	000:1] SURICATA Q ecode] [Priority: 3]	UIC failed decry {UDP} <u>10.3.7.1</u>	pt [**] .:43041 ->
2024-6-24 14:57:58	SURICATA	INFO	06/24/2024-14:57: [Classification: Gene 172.217.163.35:443	57.591867 [* eric Protocol C 3	*] [1:22310 Command D	000:1] SURICATA Q ecode] [Priority: 3]	UIC failed decry {UDP} <u>10.3.7.1</u>	pt [**] .:43041 ->
2024-6-24 14:57:56	SURICATA	INFO	06/24/2024-14:57: [Classification: Gene 142.251.43.20:443	55.815736 [* ric Protocol C	*] [1:22310 Command D	000:1] SURICATA QI ecode] [Priority: 3]	UIC failed decry {UDP} <u>10.3.7.1</u>	pt [**] .:34014 ->
2024-6-24 14:57:56	SURICATA	INFO	06/24/2024-14:57: [Classification: Gene 142.251.43.20:443	55.809754 [* eric Protocol C	*] [1:22310 Command D	000:1] SURICATA Q ecode] [Priority: 3]	UIC failed decry {UDP} <u>10.3.7.1</u>	pt [**] .:34014 ->
2024-6-24 14:57:56	SURICATA	INFO	06/24/2024-14:57: [Classification: Gene 142.251.43.20:443	55.809579 [* ric Protocol C	*] [1:22310 Command D	000:1] SURICATA Q ecode] [Priority: 3]	UIC failed decry {UDP} <u>10.3.7.1</u>	pt [**] .:34014 ->
2024-6-24 14:57:56	SURICATA	INFO	06/24/2024-14:57: [Classification: Gene 8.8.4.4:443	55.794603 [* eric Protocol C	**] [1:22310 Command D	000:1] SURICATA QU ecode] [Priority: 3]	UIC failed decry {UDP} <u>10.3.7.1</u>	pt [**] .:38365 ->

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

rofile Index : 4	
Enable	
Comment:	Suricata Test1 KK
Event Category:	System V
Event Type:	Log Keyword Match 🗸
	Keyword:
	Keyword Type: REGEX V
	Count: 1
	Timespan: 0 seconds
	Level:
Action Category:	System V
Action Type:	Web Notification V
	Block the following if present:

- 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.

Applications >> Smart Action	on	Web Notification	clear >
Profile Index : 4		[**] [1:2210045:2] SURICATA STREAM Packet with invalid ack [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 206 110 12 02: 443 -> 10.3 9100:3982	2023/09/20 15:56:49 Suricata / Smart Action Profile 4
Enable		<u>200.117.114.220</u> .443 ~ <u>10.3.7.100</u> .37662	
Comment:	Suricata Test1 KK		
Event Category: Event Type:	Log Keyword Match	[**] [1:2210030:2] SURICATA STREAM FIN invalid ack [**] [Classification: Generic Protocol Command	2023/09/20 15:56:49 Suricata / Smart
Event Type.	Keyword:	Decode] [Priority: 3] {TCP} <u>206.119.114.228</u> :443 -> <u>10.3.9.100</u> :39882	Action Profile 4 🛛
	•*		
		[**] [1:2020716:6] ET POLICY External IP Lookup ipinfo.io [**] [Classification: Device Retrieving External IP Address Detected] [Priority: 2] {TCP}	2023/09/20 15:56:28 Suricata / Smart Action Profile 4
	Keyword Type: REGEX 🗸	<u>10.3.12.21</u> :51896 -> <u>34.117.59.81</u> :80	
	Count: 1 Timespan: 0 seconds	[**] [1:2013028:7] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information	2023/09/20 15:56:28 Suricata / Smart
	Facility: SURICATA ~	Leak] [Priority: 2] {TCP} <u>10.3.12.21</u> :51896 -> 34.117.59.81:80	Action Profile 4
Action Category:	Level: INFO(6) V		
Action Type:	Web Notification		2022/00/20 15:55:22
<i>,</i> ,	Block the following if present: 3	ipinfo.io [**] [Classification: Device Retrieving	2023/09/20 15:56:23 Suricata / Smart
	□ First IP □ Second IP □ LAN	External IP Address Detected [[Priority: 2] { ICP } <u>10.3.12.21</u> :51894 -> <u>34.117.59.81</u> :80	Action Profile 4
Note:			

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

