

DrayTek

**Vigor3912S Series
Linux Application
Dockers**



Draytek Vigor3912S Series Linux Application Docker Owner's Manual

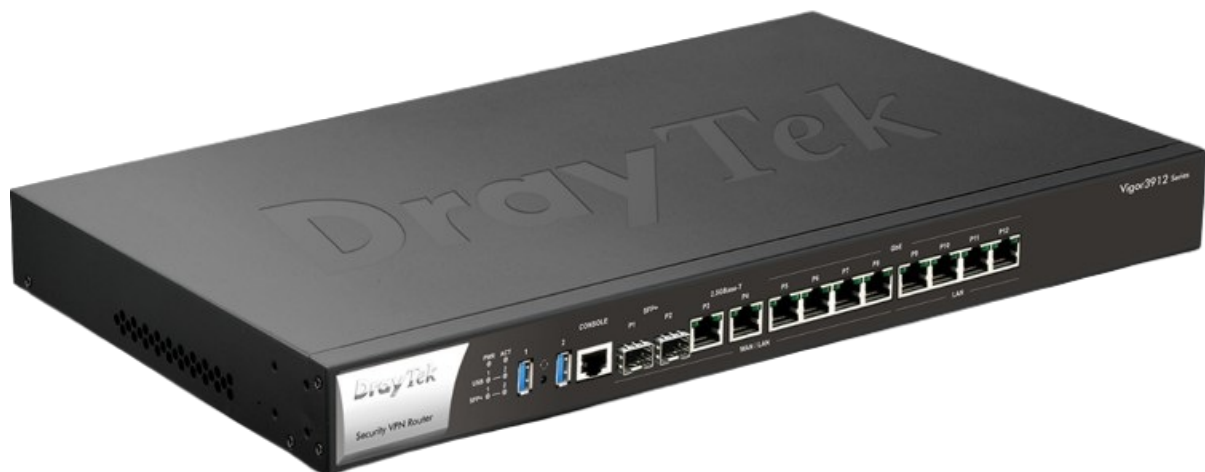
[Home](#) » [DrayTek](#) » Draytek Vigor3912S Series Linux Application Docker Owner's Manual 

Contents

- [1 Vigor3912S Series Linux Application Docker Specifications](#)
- [2 Product Usage Instructions](#)
- [3 FAQs](#)
- [4 Documents / Resources](#)
 - [4.1 References](#)
- [5 Related Posts](#)

DrayTek

Vigor3912S Series Linux Application Docker



Specifications

- Product: Vigor 3912S Router

- Intrusion Detection System: Suricata IDS
- Rules: Over 60,000 rules including 6,000+ CVE definitions
- Priority Levels: 4 levels with 1 being the highest priority

Product Usage Instructions

• Configuration of the Linux Application Layer

- Configure the Linux Application settings on the router by setting the Linux IP address and Linux Gateway IP address.
- Activate the Linux SSH service for enhanced security.

• Suricata Installation

- Navigate to [Linux Applications] > [Suricata] and enable Suricata.
- Enable Suricata Core Auto Update and Suricata Rule Auto Update for automatic updates.

• Rule Selection

- Select the appropriate rules based on priority levels. Use the Select/Clear All buttons to activate specific categories.

• Network Event Monitoring

- Visit [Linux Applications] > [Log Collector] to view network events detected by Suricata.
- Determine if the detected events require action or can be ignored.

• Optional: Smart Action Setup

- Enable Smart Action to receive notifications for events.
- Configure Event Category, Type, Content, Facility, Level, and Action Type as needed.

• Monitoring

- Check for notifications using the bell icon and monitor Suricata rule-matched counts on the Statistics page.

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

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 the router's WUI integration, enabling Suricata is a matter of a few mouse clicks. This article depicts the 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 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.

Setup Linux IP and Gateway ?

Linux IP address	Linux Gateway IP address	Linux Network
<input type="text" value="192.168.1.254"/>	<input type="text" value="192.168.1.1"/>	LAN1 192.168.1.1/255.255.255.0 ▼ VLAN0 ▼

Setup Linux Service

<input type="checkbox"/> Enable Linux SSH service	SSH Port <input type="text" value="22"/> (default: 22)
---	--

OK

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

Setup Linux Service

<input checked="" type="checkbox"/> Enable Linux SSH service	SSH Port <input type="text" value="22"/> (default: 22)
--	--

OK

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

Linux Applications >> Suricata

General Setup	
General Setup ?	
<input checked="" type="checkbox"/> Enable ?	
<input checked="" type="checkbox"/> Suricata Core Auto Update	Core Base: <input type="text" value="v3912-r1"/> (
<input checked="" type="checkbox"/> Suricata Rule Auto Update	Core Status: loading
<input type="button" value="Restart Suricata"/>	Core Version: v3912-r1a-
	Core Last Updated: 2024
	Rule Last Updated: 2024-
	Rule Last Changed: 2024-

1. Core Base – two core base options are available. V3912-r1 uses Suricata version 6.0.x; v3912-r2 uses Suricata version 7.0.x; The current Suricata version will be shown next to the Core Base drop-down menu.
 2. 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.
 3. Suricata Core Auto Update – this process should run at around 6:30 am local time (each day). If the core image isn't updated, some Suricata rules may have received an update thanks to the core image SOP process that detects and updates the rules.
- With over 60k rules, including the 6k+ CVE definitions, it is worth selecting the right one.

Rule Setup (classtype) ?

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

Note

Once some rules have been selected, Suricata helps to detect the network activities. If the Suricata rule 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**



Status

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**



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**



- 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 be the bad ones. We have to check which network event triggers 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	Count	
24/06/2024 14:48	24/06/2024 14:58	SURICATA	INFO(6)		100	<div>SearchDownload</div>
Time	Facility	Level	Message			
2024-6-24 14:57:58	SURICATA	INFO	06/24/2024-14:57:57.605817 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.3.7.1:43041 -> 172.217.163.35:443			
2024-6-24 14:57:58	SURICATA	INFO	06/24/2024-14:57:57.592376 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.3.7.1:43041 -> 172.217.163.35:443			
2024-6-24 14:57:58	SURICATA	INFO	06/24/2024-14:57:57.591867 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.3.7.1:43041 -> 172.217.163.35:443			
2024-6-24 14:57:56	SURICATA	INFO	06/24/2024-14:57:55.815736 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.3.7.1:34014 -> 142.251.43.20:443			
2024-6-24 14:57:56	SURICATA	INFO	06/24/2024-14:57:55.809754 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.3.7.1:34014 -> 142.251.43.20:443			
2024-6-24 14:57:56	SURICATA	INFO	06/24/2024-14:57:55.809579 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.3.7.1:34014 -> 142.251.43.20:443			
2024-6-24 14:57:56	SURICATA	INFO	06/24/2024-14:57:55.794603 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.3.7.1:38365 -> 8.8.4.4:443			

- (optional) Enable Smart Action to receive the Suricata notifications

Profile Index : 4

☒ **Enable**

Comment:

Suricata Test1 KK

Event Category:

System

Event Type:

Log Keyword Match

Keyword:

.*

Keyword Type:

REGEX

Count:

1

Timespan:

0

seconds

Facility:

SURICATA

Level:


INFO(6)

Action Category:

System

Action Type:

Web Notification

Block the following if present: 

☐ First IP ☐ Second IP ☐ LAN IP ☐ WAN IP

1. Select System for the Event Category
 2. Select Log Keyword Match for the Event Type
 3. Enter .* in the Keyword Content. That means any log.
 4. 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 special characters.
 5. Count 1 Time Span 0 seconds means to send web notification for any event.
 6. Select SURICATA for the Facility
 7. Select INFO(6) for Level.
 8. Select System for the Action Category
 9. Select Web Notification for the Action Type
- Monitoring The little bell button indicates any new notifications.

Series

Applications >> Smart Action

Profile Index : 4

☒ Enable

Comment: Suricata Test1 KK

Event Category: System

Event Type: Log Keyword Match

Keyword: .*

Keyword Type: REGEX

Count: 1

Timespan: 0 seconds

Facility: SURICATA

Level: INFO(6)

Action Category: System

Action Type: Web Notification

Block the following if present:

☐ First IP
☐ Second IP
☐ LAN

Note:

Web Notification
clear
X

[**] [1:2210045:2] SURICATA STREAM Packet with invalid ack [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 206.119.114.228:443 -> 10.3.9.100:39882
2023/09/20 15:56:49
Suricata / Smart Action Profile 4

[**] [1:2210030:2] SURICATA STREAM FIN invalid ack [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 206.119.114.228:443 -> 10.3.9.100:39882
2023/09/20 15:56:49
Suricata / Smart Action Profile 4

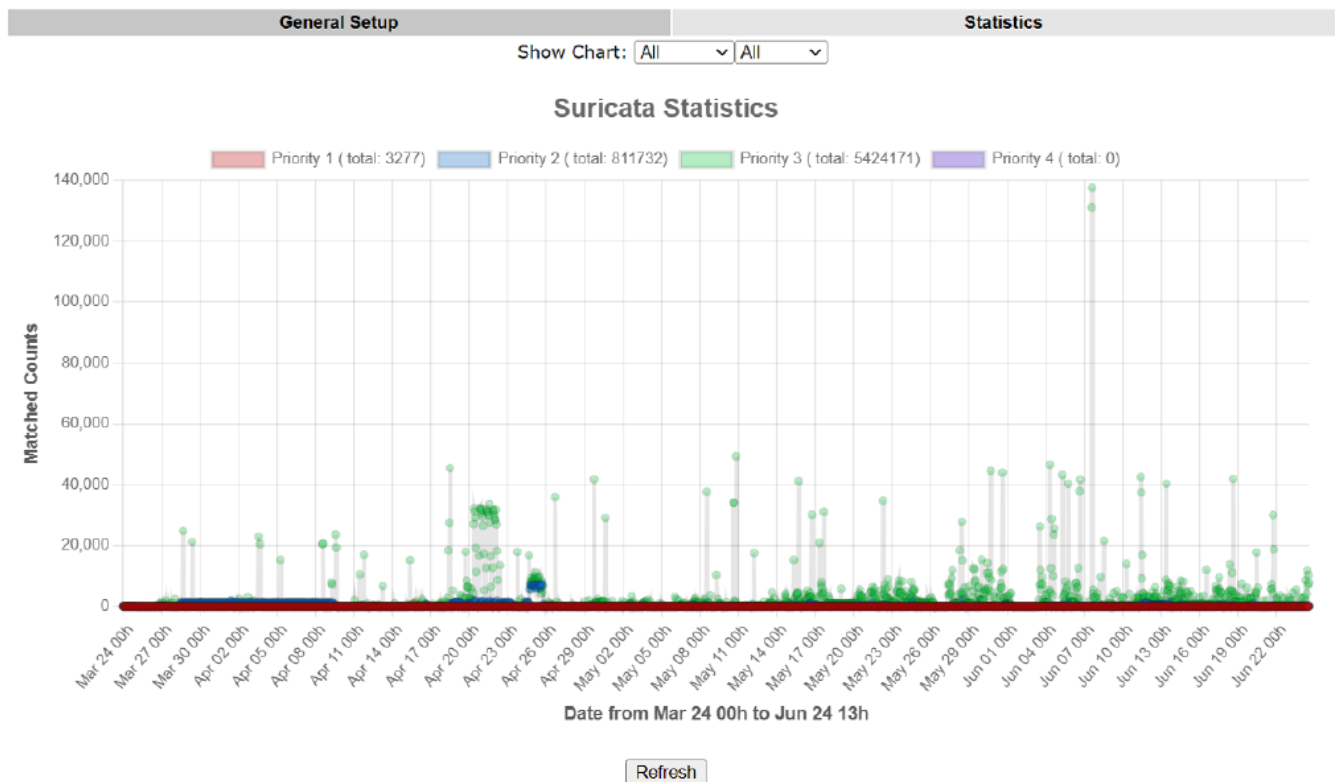
[**] [1:2020716:6] ET POLICY External IP Lookup ipinfo.io [**] [Classification: Device Retrieving External IP Address Detected] [Priority: 2] {TCP} 10.3.12.21:51896 -> 34.117.59.81:80
2023/09/20 15:56:28
Suricata / Smart Action Profile 4

[**] [1:2013028:7] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.3.12.21:51896 -> 34.117.59.81:80
2023/09/20 15:56:28
Suricata / Smart Action Profile 4

[**] [1:2020716:6] ET POLICY External IP Lookup ipinfo.io [**] [Classification: Device Retrieving External IP Address Detected] [Priority: 2] {TCP} 10.3.12.21:51894 -> 34.117.59.81:80
2023/09/20 15:56:23
Suricata / Smart Action Profile 4

- The little bell button indicates any new notifications.

Linux Applications >> Suricata



FAQs

Q: How often does Suricata Core Auto Update run?

Suricata Core Auto Update runs every 24 hours to check for the latest core image.

Q: What should I do if some Suricata rules are not updating?

If the core image isn't updated, some rules may still receive updates through the core image SOP process that detects and updates rules. There are 4 priority levels. Use the Select/Clear All (x) buttons to activate the specific category. Number 1 is the highest priority (out of 4).

Documents / Resources

	<p>Draytek Vigor3912S Series Linux Application Docker [pdf] Owner's Manual Vigor3912S Series, Vigor3912S Series Linux Application Docker, Linux Application Docker, Application Docker, Docker</p>
---	--

References

- [User Manual](#)

Manuals+. Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.