

# 如何在 Vigor3912S 執行 Suricata

Suricata 是一套開放碼的入侵偵測及防預系統的軟體, 提供超過 60000 筆的規則及 6000 筆以上的病毒碼可針對網路威脅, 巨集病毒, 網路入侵, 阻斷式攻擊等提供服務.

因 Vigor3912S 有支援 Linux Applications with Docker, 用戶可以直接執行 Suricata



## Configuration

1. 確認 Vigor3912S 已經可以上網.
2. 到 Linux Applications >> General Setup, 自行輸入一組 IP 給 Linux(同區網空的 IP), 再指定 Gateway IP address, 選 LAN 介面, 再啓用 Linux SSH 服務.

## Linux Applications >> General Setup

---

### Setup Linux IP and Gateway ?

Linux IP address	Linux Gateway IP address	Linux Network
<input type="text" value="10.3.0.13"/>	<input type="text" value="10.3.0.3"/>	<input type="text" value="LAN2 10.3.0.3/255.255.0.0"/> <input type="text" value="VLAN1"/>

### Setup Linux Service

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

3. 到 Linux Applications >> Suricata, 選啓用 Suricata. 成功後會變綠色表示執行中.

## Linux Applications >> Suricata

---

### Status

Suricata Core Status: **running**  
Suricata Core Version: **v3912-r1-20230829080739**  
Suricata Rule Last Updated: **2023-09-18T06:30:46**  
Suricata Rule Last Changed: **2023-09-18T06:30:46**

### General Setup

Enable

- Suricata Core Auto Update
- Suricata Rule Auto Update

Priority:

Highest (1)  High (2)  Medium (3)  Low (4)

Or by the Advanced Class Type Setup.

### Advanced Class Type Setup

<p>Misc Activities</p> <p>Select/Clear All</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Not Suspicious Traffic</li> <li><input checked="" type="checkbox"/> A TCP connection was detected</li> <li><input checked="" type="checkbox"/> Generic Protocol Command Decode</li> <li><input checked="" type="checkbox"/> Generic ICMP event</li> </ul>
<p>Unauthorized Access Attempts</p> <p>Select/Clear All</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Attempted Information Leak</li> <li><input checked="" type="checkbox"/> Information Leak</li> <li><input checked="" type="checkbox"/> Large Scale Information Leak</li> <li><input checked="" type="checkbox"/> Attempted User Privilege Gain</li> <li><input checked="" type="checkbox"/> Unsuccessful User Privilege Gain</li> <li><input checked="" type="checkbox"/> Successful User Privilege Gain</li> <li><input checked="" type="checkbox"/> Attempted Administrator Privilege Gain</li> <li><input checked="" type="checkbox"/> Successful Administrator Privilege Gain</li> <li><input checked="" type="checkbox"/> An attempted login using a suspicious username was detected</li> <li><input checked="" type="checkbox"/> A client was using an unusual port</li> <li><input checked="" type="checkbox"/> Detection of a non-standard protocol or event</li> <li><input checked="" type="checkbox"/> Attempt to login by a default username and password</li> <li><input checked="" type="checkbox"/> Device Retrieving External IP Address Detected</li> <li><input checked="" type="checkbox"/> Successful Credential Theft Detected</li> </ul>
<p>Denial of Service (DoS) and Network Attacks</p> <p>Select/Clear All</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Attempted Denial of Service</li> <li><input checked="" type="checkbox"/> Denial of Service</li> <li><input checked="" type="checkbox"/> Detection of a Network Scan</li> <li><input checked="" type="checkbox"/> Detection of a Denial of Service Attack</li> <li><input checked="" type="checkbox"/> Misc Attack</li> </ul>
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Unknown Traffic</li> <li><input checked="" type="checkbox"/> Potentially Bad Traffic</li> <li><input checked="" type="checkbox"/> Decode of an RPC Query</li> <li><input checked="" type="checkbox"/> Executable code was detected</li> </ul>

## Linux Applications >> Suricata

---

### 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**



## 檢查 Logs

5. Go to Linux Applications >> Log Collector. 可自行定義範圍,檢視 SURICATA, 會呈現已分類的顯示. 此部份為 Suricata 本身軟體而已, **尚未被阻擋**. 如需阻擋需再進行下一步 Smart Action 將 Suricate 與 Vigor3912S 串連.

172.17.5.3

Vigor3912 Series

Linux Applications >> Log collector

From: 2023/09/19 上午 10:19 | Till: 2023/09/20 上午 10:29 | Facility: SURICATA | Level: INFO(6) | Filter: | Count: 100

Time	Facility	Level	Message
Wed Sep 20 2023 09:52:12 GMT+0800 (台北標準時間)	SURICATA	INFO	09/20/2023-09:52:12.426848 [**] [1:2038646:1] ET INFO Observed Collaboration/File Sh Domain (www .notion .so in TLS SNI) [**] [Classification: Potentially Bad Traffic] [Priority: 10.3.17.2:62715 -> 172.64.148.154:443
Wed Sep 20 2023 09:52:33 GMT+0800 (台北標準時間)	SURICATA	INFO	09/20/2023-09:52:32.858071 [**] [1:2013028:7] ET POLICY curl User-Agent Outbound [* [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.3.12.21:49524 -> 34.1
Wed Sep 20 2023 09:52:33 GMT+0800 (台北標準時間)	SURICATA	INFO	09/20/2023-09:52:32.858071 [**] [1:2020716:6] ET POLICY External IP Lookup ipinfo.io [ [Classification: Device Retrieving External IP Address Detected] [Priority: 2] {TCP} 10.3.12 34.117.59.81:80
Wed Sep 20 2023 09:52:39 GMT+0800 (台北標準時間)	SURICATA	INFO	09/20/2023-09:52:37.880633 [**] [1:2013028:7] ET POLICY curl User-Agent Outbound [* [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.3.12.21:49526 -> 34.1
Wed Sep 20 2023 09:52:39 GMT+0800 (台北標準時間)	SURICATA	INFO	09/20/2023-09:52:37.880633 [**] [1:2020716:6] ET POLICY External IP Lookup ipinfo.io [ [Classification: Device Retrieving External IP Address Detected] [Priority: 2] {TCP} 10.3.12 34.117.59.81:80

6. 在其它應用-->聰明動作 Application-->Smart Action 找到 Suricata notifications.

- 選 System for the Event Category
- 選 Log Keyword Match for the Event Type
- 輸入 \* in the Keyword Content. 代表所有 log
- 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.

- Count 1 Time Span 0 second 代表所有事件
- 選 SURICATA for Facility
- 選 INFO(6) for Level.
- 選 System for the Action Category
- 選 Web Notification for the Action Type

或依下圖設定即可

DrayTek Vigor3912 Series

其他應用 >> 聰明動作

設定檔索引編號: 1

啟用

註解: IDS

事件分類: 系統

事件類型: Log Keyword Match

Keyword: \*

Keyword Type: TEXT

Count: 1

Timespan: 0 seconds

Facility: SURICATA

Level: INFO(6)

動作分類: 系統

動作類型: Web Notification

Block the following if present:  First IP  Second IP  LAN IP  WAN IP

\* 號代表所有符合關鍵字

表示無限次數

只攔外部IP, 避免內網上不了

有無動作也可按小鈴鐺進行檢視

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 IP

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

## 封鎖 Blocking

7. Suricata 屬第三方軟體, 可以偵測威脅入侵等, 但需再由 Vigor3912S 的 Smart Action 設定檔去執行, 才二者串連起來, 執行自動阻擋.

以下為 syslog 範例:

```
10/03/2023-08:30:57.219557 [**] [1:2025900:4] ET MOBILE_MALWARE iOS/Bahamut DNS  
Lookup 10 [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP}  
192.168.1.100:33406 -> 192.168.1.1:53
```

表示 Suricata 偵測到 MALWARE 事件, 位址是由 192.168.1.100 到 192.168.1.1.

當我們想由 Smart Action 主動封鎖的話, 可以自行設定如下: (算進階選項, 新手可跳過)

- Event Type: Log Keyword Match
- Keyword: MALWARE
- Keyword Type: TXT
- Action: Web Notification
- Blocking the following if present:
- If we want to block the source IP when detecting this kind of event, select First IP or LAN IP.
- If we want to block the destination IP when detecting this kind of event, we can select second IP or WAN IP

自動封鎖的動作資料可以查 Debug Log.

LAN IP/ First IP log:

```
2023-09-21_11:54:03.12358 [DEBUG] [AUTO] 10.3.5.7 was blocked by session limit.
```

WAN IP/ Second IP log:

```
[DEBUG] [BFP] [AUTO] 8.8.8.8 was blocked by Brute Force Protection(暴力攻擊保護)
```

8. 也可以手動封鎖不知名 IP.

The screenshot displays three log entries from Suricata, each with a manual action menu. The first entry is a DNS query from 192.168.1.11:53928 to 192.168.1.1:53, classified as 'Potentially Bad Traffic'. The second entry is an HTTP request from 192.168.1.11:61971 to 111.249.97.104:80, also classified as 'Potentially Bad Traffic'. The third entry is another DNS query from 192.168.1.11:62769 to 8.8.8.8:53, classified as 'Potentially Bad Traffic'. Each entry has a blue plus icon and a number (3, 2, and 2 respectively) indicating the number of items. A red box highlights the 'block' button in the second entry's menu, and a grey box highlights the 'view' button.

```
[**] [1:2046001:1] ET INFO DYNAMIC_DNS Query 2023/10/03 11:42:05  
to a *.ddnsfree .com Domain [**] [Classification: Suricata / Smart  
Potentially Bad Traffic] [Priority: 2] {UDP} Action Profile 1  
192.168.1.11:53928 -> 192.168.1.1:53  
+ 3
```


```
[**] [1:2046002:1] ET INFO DYNAMIC_DNS HTTP 2023/10/03 11:37:11  
Request to a *.ddnsfree .com Domain [**] Suricata / Smart  
[Classification: Potentially Bad Traffic] [Priority: 2] Action Profile 1  
{TCP} 192.168.1.11:61971 -> 111.249.97.104:80  
+ 2  
block view
```

```
[**] [1:2046001:1] ET INFO DYNAMIC_DNS Query 2023/10/03 11:37:10  
to a *.ddnsfree .com Domain [**] [Classification: Suricata / Smart  
Potentially Bad Traffic] [Priority: 2] {UDP} Action Profile 1  
192.168.1.11:62769 -> 8.8.8.8:53  
+ 2
```

可以點 View 去看 BFP(暴力攻擊表).

System Maintenance >> Management

Brute Force Protection: Blocked IP List

Index	IP Address	FTP	HTTP	HTTPS	TELNET	TR069
1	111.249.97.104 					

Showing 1 to 1 of 1 entries

Web Notification

[\*\*] [1:2046002:1] ET INFO DYNAMIC\_DNS HTTP Request to a \*.ddnsfree .com Domain [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.11:51336 -> 111.249.97.104:80  
+ 2

[\*\*] [1:2046001:1] ET INFO DYNAMIC\_DNS Query to a \*.ddnsfree .com Domain [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.11:50790 -> 192.168.1.1:53  
+ 3

**DrayTek** Vigor3912 Series Home | 3 | Settings | Help | Logout

系統維護 >> 管理

自動登出 | IR6

- 登入/登出
- 使用者管理
- 物件設定
- 數位內容安全管理(CSM)
- 頻寬管理
- 其他應用
- 動態DNS
- LAN DNS / DNS 轉發
- DNS 安全性
- 排程
- RADIUS/TACACS+
- Active Directory / LDAP
- UPnP
- IGMP
- 網路喚醒(Wake on LAN)
- 簡訊/郵件警示服務
- Bonjour
- 高可靠性
- 本機802.1X基本設定
- 聰明動作**
- Linux Applications
- VPN 與遠端存取
- 認證管理
- USB 應用
- 系統維護
- 自我診斷

10 每頁之條目

暴力攻擊防護: 阻擋IP清單

索引	IP 位址	FTP	HTTP	HTTPS	TELNET	TR069	SSH	VPN	MANUAL	SMART ACTION	解除封鎖
1	94.102.61.2 									✓	解除封鎖
2	193.163.125.132 									✓	解除封鎖
3	94.102.61.40 									✓	解除封鎖
4	198.235.24.183 									✓	解除封鎖
5	83.147.61.239 									✓	解除封鎖
6	49.51.231.163 									✓	解除封鎖

顯示1至6之6列條目

管理員模式