



# CHAPTER 6

## Snort Devices

---

MARS can monitor Snort 2.x (2.0, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, and 2.8) via the syslog messages generated by the devices. To enable MARS to monitor Snort devices, configure the Snort syslog plugin to publish messages to the MARS appliance, and then define the Snort device in the MARS web interface.

This chapter contains the following topics:

- [MARS Expectations of the Snort Syslog Format, page 6-1](#)
- [Configure Snort to Send Syslogs to MARS, page 6-1](#)
- [Add the Snort Device to MARS, page 6-2](#)

## MARS Expectations of the Snort Syslog Format

The following example Snort syslog messages are used to illustrate the values that are parsed by the MARS Appliance:

```
<161>snort: [1:2050:1] MS-SQL version overflow attempt [Classification: Misc activity] [Priority: 3]: {UDP}
69.70.113.64:1449 -> 66.243.153.44:1434

<119>Jul 16 10:54:39 SourceFire SFIMS: [1:469:1] ICMP PING NMAP [Classification: Attempted Information Leak]
[Priority: 2] {ICMP} 210.22.215.77 -> 67.126.151.137

<161>Mar 12 18:02:22 snort: [ID 702911 local4.alert] [119:2:1] (http_inspect) DOUBLE DECODING ATTACK {TCP}
10.1.1.21:60312 -> 10.1.1.69:80
```

The MARS parser expects the pattern: “[<generator id>:<snort id>:<revision number>]” to identify the event as one originating from a Snort device. Once that determination is made, MARS looks for either “{<protocol\_string>} <ip>:<port> -> <ip>:<port>” or “{<protocol\_string>} <ip> -> <ip>” to identify the five-tuple values.

## Configure Snort to Send Syslogs to MARS

For Snort, use the syslog as your output plugin. Configure your syslogd to send copies to another host. On most older-style systems (Solaris/Linux), you need to edit */etc/syslog.conf*. (Assuming that the system is based on syslogd, and not any of the newer system logging facilities. The newer logging facilities are not supported by Snort.)

To configure Snort to send syslog messages to the MARS Appliance, follow these steps:

- 
- Step 1** Make Snort's output go to syslog with log facility local4 in snort.conf (you can pick any local facility that's unused.)

```
output alert_syslog: LOG_LOCAL4 LOG_ALERT
```

snort.conf is normally in /etc/snort.

- Step 2** Add a redirector in your /etc/syslog.conf on your Snort box to send syslog to MARS.

```
local4.alert @IPAddrOffMarsbox
```

- Step 3** Restart the Snort daemon and the syslogd daemon on your Snort box.
- 

## Add the Snort Device to MARS

To add the Snort device to MARS, follow these steps:

- 
- Step 1** Click **Admin > System Setup > Security and Monitor Devices > Add**.
- Step 2** From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.
- Step 3** Enter the Device Name and IP addresses if adding a new host.
- Step 4** Click **Apply**
- Step 5** Click **Reporting Applications** tab.
- Step 6** From the Select Application list, select **Snort Snort 2.0**.  
Currently, the Snort Snort 2.0 option applies to the following versions: 2.0, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, and 2.8
- Step 7** Click **Add**
- Step 8** For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:
- To manually define the networks, select the **Define a Network** radio button.
    - a. Enter the network address in the Network IP field.
    - b. Enter the corresponding network mask value in the Mask field.
    - c. Click **Add** to move the specified network into the Monitored Networks field.
    - d. Repeat as needed.
  - To select the networks that are attached to the device, click the **Select a Network** radio button.
    - a. Select a network from in the Select a Network list
    - b. Click **Add** to move the specified network into the Monitored Networks field.
    - c. Repeat as needed.
- Step 9** To save your changes, click **Submit**.

**Step 10** To enable MARS to start sessionizing events from this module, click **Activate**.

---

