



CHAPTER 3

NetScreen IDP Device and Server Support

MARS supports multiple versions of NetScreen IDP. How this support is realized within MARS differs based on the version of the sensor that you are running.

- **NetScreen IDP-Management Server**—The NetScreen IDP Management Server is the management software for IDP version 2.x and 3.x sensors. Usually, the IDP-Management Server is installed on the IDP appliance. However, it can be removed from the IDP appliance and installed on a Solaris or Linux server. In MARS, IDP v2.1 and 3.x are both supported as agents on a Linux host running IDP-Management Server.
- **NetScreen Security Manager**— (NSM) provide support for the following NetScreen sensors:
 - NetScreen IDP 4.0
 - NetScreen IDP 4.1



Note It also supports other Juniper Networks devices such as NetScreen-x, ISG-x and SSG-x. These devices are not currently supported in MARS.

IDP sensors running 4.0 and later are supported by NSM running on a Linux host. NSM forwards syslog events to MARS for processing.



Tip

Because MARS does not support multiple reporting devices on the same host (as defined by reporting IP address), IDP-Management Server and NSM cannot co-exist on the same host unless they report to MARS via different IP addresses. However, you can define multiple sensors per management server.

Adding a NetScreen IDP sensor to MARS involves two parts:

1. Bootstrap the management server (or IDP sensor 4.1) that will publish syslog events to MARS.
2. Add and configure the management server (or IDP 4.1 sensor) in the MARS web interface.

This chapter contains the following topics:

- [Bootstrap a NetScreen Security Manager, page 3-2](#)
- [Bootstrap a NetScreen IDP Management Server, page 3-2](#)
- [Add NetScreen Server or Sensor to MARS, page 3-2](#)

Bootstrap a NetScreen Security Manager

MARS can retrieve logs from a NetScreen Security Manager server in support of IDP 4.x sensors. To prepare the NetScreen Security Manager server, you must enable logging and syslog generation for the security policies that are running on IDP sensors that it manages.

Bootstrap a NetScreen IDP Management Server

MARS can retrieve logs from a NetScreen IDP Management Server in support of IDP 2.x and 3.x sensors. To prepare the NetScreen IDP Management Server, you must enable logging and syslog generation for the security policies that are running on IDP sensors that it manages.

To enable logging and syslog generation, follow these steps:

-
- Step 1** Click **NetScreen-Global Pro > IDP Manager > IDP**.
 - Step 2** Log in to the IDP Manager.
 - Step 3** From the main menu, click **Tools > Preferences**.
 - Step 4** In the tree on the left, click **Management Server**, enter the Local Controller's address in the Syslog host field, and click **OK**.
 - Step 5** Click **Security Policies**, and the name of your policy.
 - Step 6** In the Notification column, right-click anywhere in the cell in the field and select **Configure**.
 - Step 7** Check **enable logging** and **syslog** for each policy, and click **OK**. Repeat for all of your policies.
 - Step 8** From the main menu, click **Policy > Install**.
-

Add NetScreen Server or Sensor to MARS

Whether the syslog messages are being sent to MARS from a management server on behalf of sensors or an IDP 4.1 sensor is publishing the syslog messages directly to MARS, you must perform three steps:

1. Define a Linux host that represents the management server
2. Add configuration information about the software on the management server. This information appears as a software-based security application (a management console) running on the Linux host.
3. Add configuration information for the IDP sensors that are managed by the server. These sensors appear as modules of a management console.

To define the IDP sensors, 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** If adding a new host, specify the following values:
 - enter the and IP Addresses, and click **Apply**.
 - **Device Name**—Specify a name for the host that is representing either a management server.

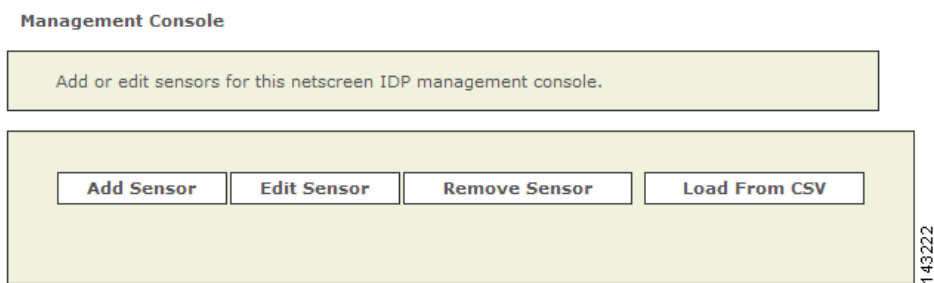
- **Reporting IP Address**—Enter the IP address from which MARS will receive the syslog messages from this device.
- **Operating System**—Select Linux.
- **IP Address and Network Mask**—Under Enter interface information, specify the values of at least one interface. You must define the name, IP address, and network mask for that interface.

Step 4 Click **Apply**, then click **Reporting Applications** tab, and select one of the following values from the Select application list:

- **NetScreen IDP 2.1**—Select this value to add a NetScreen IDP Management Server (IDP 2.1) to this host.
- **NetScreen IDP 3.x**—Select this value to add a NetScreen IDP Management Server (IDP 3.x) to this host.
- **Juniper IDP 4.x**—Select this value to add a NetScreen-Security Manager (IDP 4.x) to this host. This value is also the one that you add to specify a standalone IDP 4.1 sensor (the software version simply instructs MARS as to how to parse the incoming syslog messages).

Step 5 Click **Add**.

The Management Console page appears.



Step 6 To add a sensor, click **Add Sensor**.

The Select the device on which sensor is running or enter a new device page appears.

Step 7 Click **Add New**.

The Add Sensor page appears.

Step 8 Specify the following values:

- **Device Name**—This name is the name that will appear in the list of devices attached to this management console.
- **Sensor Name**—Specify the hostname of the sensor.
- **Reporting IP**—Specify the IP address used by the sensor to send syslog messages to this management console.
- **Interface name, IP address, and network mask**—Specify the name, IP address and network mask values for at least one interface running on the sensor.
- **Monitored Networks**—Specify which networks are monitored by the sensor. This information is used for attack path calculation and mitigation.

Step 9 Click **Submit** to add the sensor the management console.

Step 10 Click **Submit** on the Management Console page to add the application to the host.

Depending on the device type that you added, one of the following values appears under the Device Type list:

- NetScreen IDP Management Server (IDP 2.1)
- NetScreen IDP Management Server (IDP 3.x)
- NetScreen-Security Manager (IDP 4.x)

Step 11 Click **Done** to commit your changes to the database.

Step 12 To enable MARS to start sessionizing events from this module, click **Activate**.
