



CHAPTER 5

Configuring VPN Devices

VPN devices provide MARS with information about remote hosts, login in requests and denials, and access times. With this data, MARS can provide end-to-end attack path analysis and identify the VPN device through which attacks are launched.

This chapter explains how to bootstrap and add the following VPN device to MARS:

- [Cisco VPN 3000 Concentrator, page 5-1](#)

Cisco VPN 3000 Concentrator

MARS can receive and process events from the Cisco VPN 3000 Concentrator, versions 4.0.1 and 4.7. To enable communications, you must perform two tasks:

- [Bootstrap the VPN 3000 Concentrator, page 5-1](#)
- [Add the VPN 3000 Concentrator to MARS, page 5-2](#)

Bootstrap the VPN 3000 Concentrator

To configure a Cisco VPN 3000 Concentrator to generate and publish events to the MARS Appliance, you must verify that the correct events are generated in the correct format, and you must direct the Cisco VPN 3000 Concentrator to publish syslog events to the MARS Appliance.

To configure Cisco VPN 3000 Concentrator to send syslog events to MARS, follow these steps:

-
- Step 1** Open your browser and log in to the Cisco VPN 3000 Concentrator Series Manager.
- Step 2** From the tree on the left, select **Configuration > System > Events > General**.

Configuration | System | Events | General

This section lets you configure default event handling.

Save Log on Wrap	<input type="checkbox"/>	Check to save the event log to a file on wrap.
Save Log Format	Multiline	Select the format of the saved log files.
FTP Saved Log on Wrap	<input type="checkbox"/>	Check to automatically FTP the saved log to a remote destination.
E-mail Source Address		Enter the e-mail address that appears in the From: field.
Syslog Format	Original	Select the format of Syslog messages.
Events to Log	Severities 1-5	Select the events to enter in the log.
Events to Console	Severities 1-3	Select the events to display on the console.
Events to Syslog	Severities 1-5	Select the events to send to a Syslog Server.
Events to E-mail	None	Select the events to send to an E-mail Recipient.
Events to Trap	Severities 1-3	Select the events to send to an SNMP Trap Destination.

143210

- Step 3** Verify that the Syslog Format is Original.
- Step 4** Select **Severities 1-5** in the Events to Syslog field.
- Step 5** From the tree on the left, select **Configuration > System > Events > Syslog Servers**.
- Step 6** Click **Add** to define a target syslog server.

Configuration | System | Events | Syslog Servers | Add

Add a syslog server.

Syslog Server	cs-mars	Enter the IP address or hostname of the syslog server.
Port	514	Enter the port used by the syslog server.
Facility	Local 7	Select the syslog facility tag for events sent to this server.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

143209

- Step 7** In the Syslog Server field, enter the IP address or hostname of the MARS Appliance.
- Step 8** Click **Add** to save the syslog server settings.
- Step 9** Click **Save** in the top-right corner to save all changes.

Add the VPN 3000 Concentrator to MARS

To add the VPN 3000 Concentrator to MARS, follow these steps:

- Step 1** Select **Admin > Security and Monitor Devices > Add**.
- Step 2** Select either **Cisco VPN Concentrator 4.0.1** or **Cisco VPN Concentrator 4.7** from the Device Type list.

Device Type:

→ *Device Name:

→ Access IP: ...

→ Reporting IP: ...

→ *Access Type:

SNMP RO Community:

→ Monitor Resource Usage:

143208

- Step 3** Enter the name of the VPN Concentrator in the Device Name field.
- Step 4** Enter the IP address used to administer the VPN Concentrator in the Access IP field.
- Step 5** Enter the IP address from which the syslog messages are sent to MARS in the Reporting IP field.
- Step 6** Select **SNMP** from the Access Type list.
- Step 7** (Optional) To enable MARS to retrieve MIB objects for this Concentrator, enter the device's read-only community string in the SNMP RO Community field.
- MARS uses the SNMP RO string to read MIBs related to the reporting device's CPU usage and other device anomaly data.
- Step 8** Click **Discover**.
- Step 9** Click **Submit**.
-

