



CHAPTER 22

NetScreen ScreenOS Devices

MARS can monitor NetScreen ScreenOS devices running versions 4.0, 5.0, 5.4, and 6.0. To prepare a NetScreen device to be monitored, you must:

1. Provide MARS with SNMP, SSH or Telnet administrative access to NetScreen device.
2. Define the SNMP RO community strings to be shared between the NetScreen device and MARS.
3. Select the syslog messages to published to MARS.
4. Add the Netscreen Device to the MARS web interface.

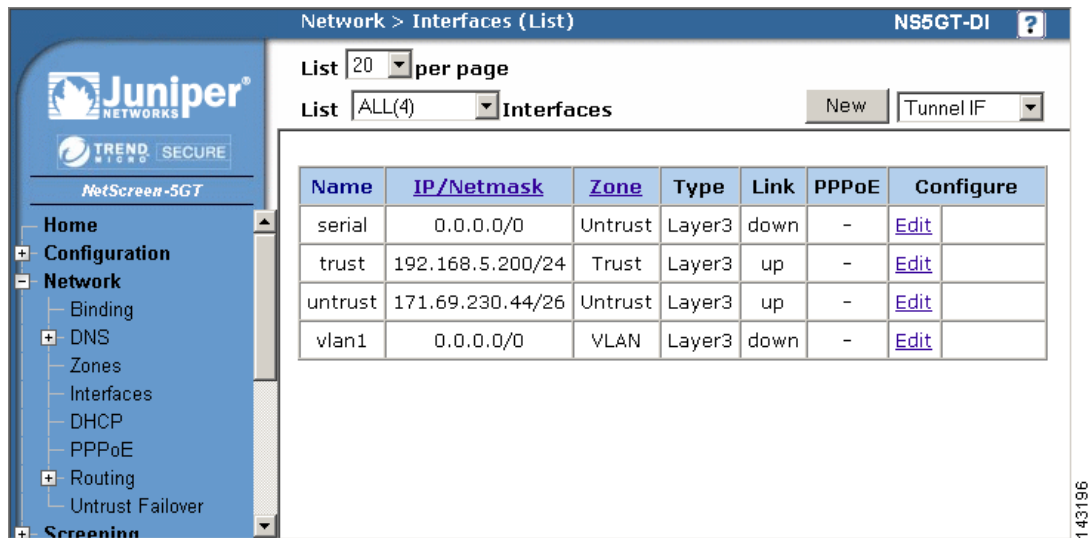
To accomplish these requirements, you must perform two procedures:

- [Bootstrap the NetScreen Device, page 22-1](#)
- [Add the NetScreen Device to MARS, page 22-5](#)

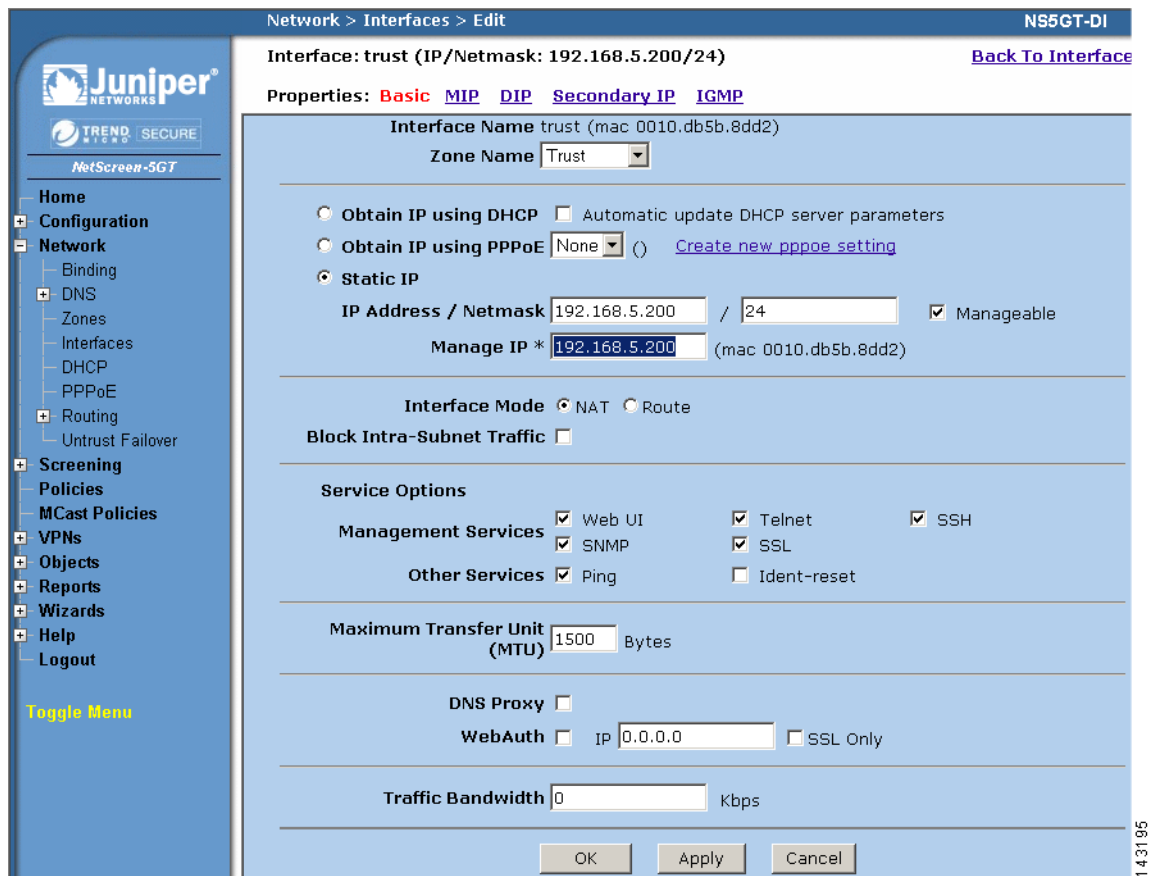
Bootstrap the NetScreen Device

To prepare the NetScreen device to be monitored by MARS, follow these steps:

-
- Step 1** Login to the NetScreen with appropriate username and password.
 - Step 2** In the main screen, on the left hand column click **Network > Interfaces**.



- Step 3** Click **Edit** next to the appropriate interface to configure for MARS to have access to SNMP and Telnet/SSH.



- Step 4** Under Service Options, select one of the following values:

- SNMP

- Telnet
- SCS (4.0 only)
- SSH (5.0 and later)

MARS can only use one of the access methods to perform configuration discovery. This value will also be selected in the Access Type value of [Add the NetScreen Device to MARS, page 22-5](#).

Step 5 Click **Apply** then click **OK**.

Step 6 Configure the SNMP information by selecting **Configure > Report Settings > SNMP**.

Configuration > Report Settings > SNMP NS5GT-DI

Juniper NETWORKS
TREND MICRO SECURE
NetScreen-5GT

Home
Configuration
Date/Time
Update
Admin
Auth
Report Settings
Log Settings
Email
SNMP
Syslog
WebTrends
Network
Screening
Policies
MCast Policies
VPNs
Objects

New Community

SNMP Report Settings

System Name NS5GT-DI
System Contact
Location
Listen Port 161
Trap Port 162
Enable Authentication Fail Trap

Apply Cancel

Communities:

Name	Write	Trap	Traffic	Hosts	Configure
No entry available					

143200

Step 7 Add the MARS IP address in the Host List by clicking **Edit**.

Step 8 Enter the MARS IP address and verify that the Community Name value matches the community string entered in the MARS web interface when adding this device.

Step 9 (Optional) If the community string does not match, click **New Community** to define one that matches the one defined in MARS.

Step 10 Configure the Syslog information by selecting **Configure > Report Settings > Syslog**.

Step 11 Verify that the **Enable Syslog Messages** and **Include Traffic Log** boxes are checked.

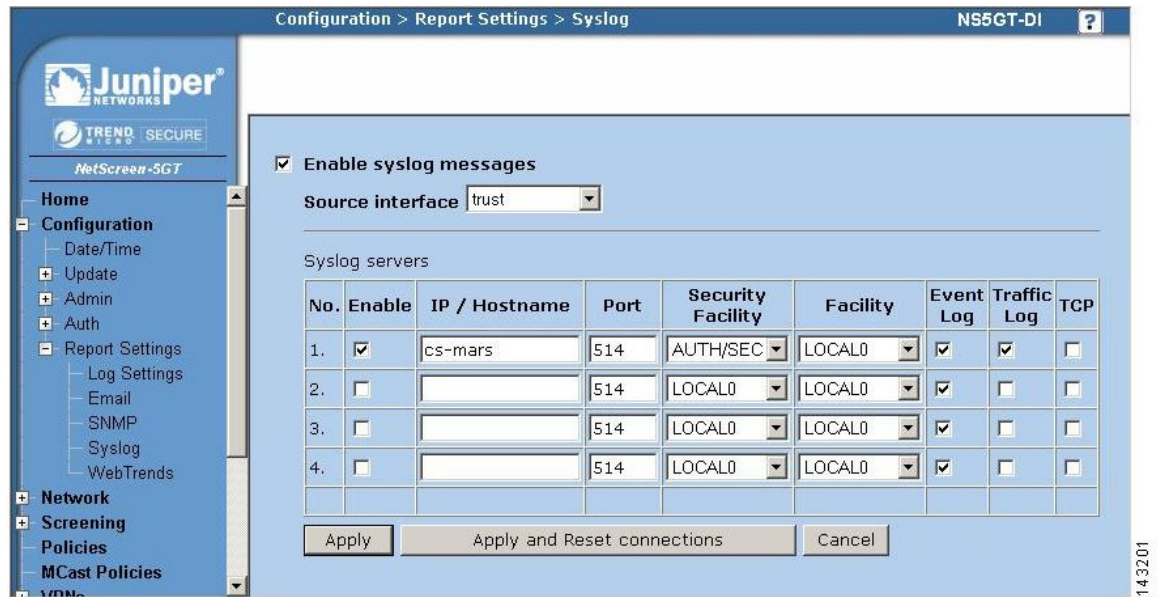
Step 12 Enter the IP address of the MARS Appliance that will listen for events from this device

Step 13 Verify that the default syslog port number of 514 is selected.

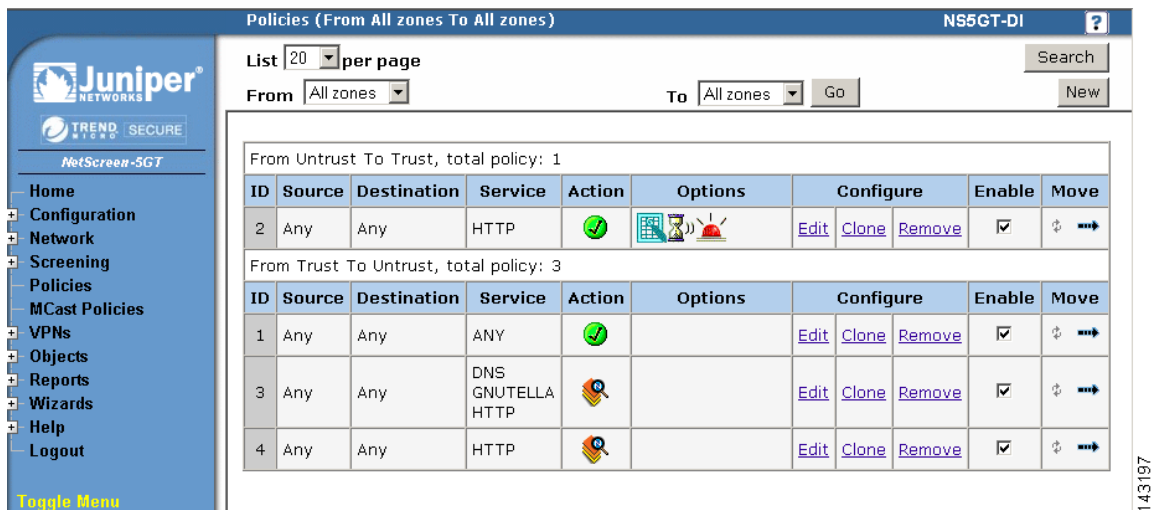
Step 14 Select the **AUTH/SEC** for Security Facility and **LOCAL0** for Facility.

Step 15 For NetScreen 5.0, select the **Event Log** in addition to **Traffic Log**.

Step 16 Click **Apply**.



- Step 17** Configure logging for each policy that user wants to send the events to the MARS Appliance. Select **Policies** on the left hand area.



- Step 18** Click **Edit** then **Advance** and verify that **Logging** box is checked. Repeat for all policies which events need to be sent to MARS.

The screenshot displays the 'Policies (From Untrust To Trust)' configuration window in the NetScreen management interface. The window title is 'NS5GT-DI'. On the left, there is a navigation menu with options: Home, Configuration, Network, Screening, Policies, MCast Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. The main configuration area includes the following fields and options:

- Name (optional):** A text input field.
- Source Address:** Radio buttons for 'New Address' and 'Address Book Entry'. The 'Address Book Entry' option is selected, with a dropdown menu set to 'Any' and a 'Multiple' button.
- Destination Address:** Radio buttons for 'New Address' and 'Address Book Entry'. The 'Address Book Entry' option is selected, with a dropdown menu set to 'Any' and a 'Multiple' button.
- Service:** A dropdown menu set to 'HTTP' and a 'Multiple' button.
- Application:** A dropdown menu set to 'None'.
- URL Filtering:** A checkbox that is unchecked.
- Action:** A dropdown menu set to 'Permit' and a 'Deep Inspection' button.
- Antivirus Objects:** Two list boxes: 'Attached AV Object Names' (empty) and 'Available AV Object Names' (containing 'scan-mgr'). Navigation buttons '<<' and '>>' are between them.
- Tunnel:** A dropdown menu set to 'None' with 'VPN' selected. Below it is a checkbox for 'Modify matching bidirectional VPN policy' which is unchecked.
- L2TP:** A dropdown menu set to 'None'.
- Logging:** A checkbox that is checked.

At the bottom of the configuration area are three buttons: 'OK', 'Cancel', and 'Advanced'. A vertical reference number '143198' is visible on the right edge of the screenshot.

- Step 19** Verify that all the Syslog event severity levels that need to be sent to MARS are configured. Verify which Syslog severity levels that are enabled by selecting **Configuration > Report Settings > Log Settings**.

Add the NetScreen Device to MARS

- Step 1** Select **Admin > System Setup > Security and Monitor Devices > Add**.
- Step 2** Select one of the following versions from the Device Type list.
- NetScreen ScreenOS 4.0
 - NetScreen ScreenOS 5.0
 - NetScreen ScreenOS 5.4
 - NetScreen ScreenOS 6.0
- Step 3** Enter the name of the device in the Device Name field.

MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and in the Security and Monitoring Device list. For devices that support the discovery operation, such as routers and firewalls, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the *hostname.domain* format. For devices that cannot be discovered, such as Windows and Linux hosts and host applications, MARS uses the provided value.

Step 4 (Optional) To enable MARS to discover settings from this device, enter the administrative IP address in the Access IP field.

To learn more about the access IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

Step 5 Enter the IP address of the interface that publishes syslog messages or SNMP notifications, or both in the Reporting IP field.

To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).

Step 6 If you entered an address in the Access IP field, select **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- [Configure Telnet Access for Devices in MARS, page 1-13](#)
- [Configure SSH Access for Devices in MARS, page 1-13](#)
- [Configure FTP Access for Devices in MARS, page 1-14](#)

For more information on determining the access type, see [Selection of the Access Type, page 1-11](#).

Step 7 (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the device's read-only community string in the SNMP RO Community field.

Before you can specify the SNMP RO string, you must define an access IP address. MARS uses the SNMP RO string to read MIBs related to a reporting device's CPU usage, network usage, and device anomaly data and to discover device and network settings.

Step 8 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see [Scheduling Topology Updates, page 1-18](#).

Step 9 To add this device to the MARS database, click **Submit**.

The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

Step 10 Click **Activate**.

MARS begins to sessionize events generated by this device and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see [Activate the Reporting and Mitigation Devices, page 1-15](#).