CHAPTER 5

Configuring Firewall Devices

Revised: November 10, 2007

This chapter describes how to bootstrap firewall devices and add them to MARS as reporting devices. Firewall devices come in several form factors: hardware appliances, software applications running on a host, modules that are installed in switches and routers, and modules that install in multifunction security devices.

Multifunction security devices, such as the Cisco Adaptive Security Appliance (ASA), also support non-firewall modules, such as intrusion detection or prevention systems (IDS/IPS). This chapter does not focus on configuring non-firewalling modules. Such discussions are provided in Configuring Network-based IDS and IPS Devices, page 7-1.

This chapter explains how to bootstrap and add the following firewall devices to MARS:

Cisco Firewall Devices (PIX, ASA, and FWSM)

MARS support for Cisco firewall devices includes the following:

- PIX Security Appliance
- Cisco Adaptive Security Appliance (ASA)
- Cisco Firewall Services Modules (FWSM)

For the complete list of supported software releases by platform, refer to the latest *Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller* document.

Because these PIX software is mostly backward compatible, the commands required to bootstrap PIX security appliance remain consistent across the releases. In addition, Cisco ASA and FWSM have much in common with PIX command set.

The taskflow required to configure MARS to monitor a Cisco firewall device is as follows:

1. Configure the Cisco firewall device to accept administrative sessions from MARS (to discover settings).

   For Cisco ASA, PIX 7.0 and 8.0, and FWSM device types, you configure the admin context to accept these sessions.

Note To be monitored by MARS, the Cisco ASA, PIX 7.0 and 8.0, and FWSM device types have the following two requirements: each context requires a unique routable IP address for sending syslog messages to MARS, and each context must have a unique name (hostname+ domain name).

2. Configure the Cisco firewall device to publish its syslog events to MARS.

   For Cisco ASA, PIX 7.0 and 8.0, and FWSM device types, you must configure the admin context and each security context.

Note MARS uses syslog events to discover information about the network topology. It uses SNMP to discover CPU utilization and related information.

3. Within MARS, define the Cisco firewall device by providing the administrative connection information.

Note Before you can add an FWSM module in a switch, you must add and configure the base module (the Cisco switch) in MARS. For more information, Cisco Switch Devices, page 4-9.

   For Cisco ASA, PIX 7.0 and 8.0, and FWSM, the basic device type represents the admin context. However you must also define or discover each security context and any installed Advanced Inspection and Prevention (AIP) modules running IPS 5.0.

To configure MARS to accept syslog event data and to pull device configurations settings from a Cisco firewall device, you must perform the following tasks:

- Bootstrap the Cisco Firewall Device, page 5-2
- Add and Configure a Cisco Firewall Device in MARS, page 5-14

Bootstrap the Cisco Firewall Device

You should configure your Cisco firewall devices to act as reporting devices and manual mitigation devices because they perform multiple roles on your network. MARS can benefit from the proper configuration of specific features:

- **IDS/IPS signature detection.** While it does not boast the most efficient or comprehensive set of signatures, the built-in IDS and IPS signature matching features of the Cisco firewall device can be critical in detecting an attempted attack.
- **Accept/Deny Logs.** The logging of accepted as well as denied sessions aids in false positive analysis.
- **Administrative Access.** Administrative access ensure MARS access to several key pieces of data:
  - *Route and ARP tables*, which aid in network discovery and MAC address mapping.
  - *NAT and PAT translation tables*, which aid in address resolution and attack path analysis, exposing the real instigator of attacks.
  - *OS Settings*, from which MARS determines the correct ACLs to block detected attacks, which paste into a management session with the Cisco firewall device.

To bootstrap the Cisco firewall device, you must identify the MARS Appliance as an administrative host Enabling administrative access allows MARS to discover the Cisco firewall device configuration settings. To enable administrative access, you must make sure that the MARS Appliance is granted Telnet or SSH administrative access to the firewall device. If you use FTP access type, make sure that you have added its configuration file to an FTP server to allow MARS access to the FTP server.

In addition to configuring specific event types and administrative access, syslog messages should be sent to the MARS Appliance. To prepare the Cisco firewall device to send these messages to the MARS Appliance, you must configure the logging settings associated with each firewall device on your network. To prepare a firewall device to generate the syslog messages and direct them to a specific MARS Appliance, you must:

1. Enable logging on the firewall device.

   Before a firewall device can generate syslog messages, you must enable logging for one or more interfaces. In addition, if you configured your firewall device in a failover pair, you can specify the standby firewall device to generate syslog messages as well. You can enable the device to ensure that the standby unit's syslog messages stay synchronized if failover occurs. However, this option results in twice as much traffic on the MARS Appliance.

2. Select the log facility and queue size.

   To generate meaningful reports about the network activity of a firewall device and to monitor the security events associated with that device, you must select the appropriate logging level. The logging level generates the syslog details required to track session-specific data. After you select a logging level, you can define a syslog rule that directs traffic to the MARS Appliance.

3. Do one of the following:

   - Select the log level to debug, or
   - Change the severity level of required events to a level other than debug and select that log level.

   The debug log level generates syslog messages that assist you in debugging. it also generates logs that identify the commands issued during FTP sessions and the URLs requested during HTTP sessions. It includes all emergency, alert, critical, error, warning, notification, and information messages. Alternatively, you can change the severity level of the required messages using the **logging message** command described in Device-Side Tuning for Cisco Firewall Device Syslogs, page 5-6.

   Note Full URLs, such as `www.cisco.com/foo.html`, are included in HTTP session logs and FTP command data is logged only if web filtering (N2H2\SecureComputing or WebSense) is enabled on the reporting device. If web filtering is not enabled, then the HTTP session log does not include the hostname (although the destination host's IP and the Request-URI are included, such as `192.168.1.1:/foo.htm`) and FTP command data is not logged at all. Caveats exist with HTTP session logging, such as if the HTTP session request is broken across packets, then the hostname data might not be included in the log data.

4. Identify the target MARS Appliance and the protocol and port pair that it listens on.

   By directing syslog messages generated by a firewall device to MARS, you can process and study the messages.

Tip When monitoring a failover pair of Cisco firewall devices, you should designate the primary Cisco firewall device as the device to be monitored. If failover occurs, the secondary device assumes the IP address of the primary, which ensures that session correlation is maintained after the failover. The same focus on the primary is true for performing any bootstrap operations. The secondary device will synchronize with the configuration settings of the primary.

To enable administrative connections to the firewall device, select from the following options:

- Enable Telnet Access on a Cisco Firewall Device, page 5-4
- Enable SSH Access on a Cisco Firewall Device, page 5-4
- Send Syslog Files From Cisco Firewall Device to MARS, page 5-4

To configure log settings, see Send Syslog Files From Cisco Firewall Device to MARS, page 5-4.

Enable Telnet Access on a Cisco Firewall Device

Step 1 Log in to the Cisco firewall device with administrator's privileges.

Step 2 Enter the command:

```
telnet <MARS IP address> <netmask of MARS IP address> <interface name>
```

where *interface* name can be inside, outside, DMZ.

Enable SSH Access on a Cisco Firewall Device

Step 1 Log in to the Cisco firewall device with administrator's privileges.

Step 2 Enter the command:

```
ssh <MARS IP address> <netmask of the MARS IP address> <interface name>
```

where *interface* name can be inside, outside, DMZ.

Send Syslog Files From Cisco Firewall Device to MARS

When preparing a Cisco firewall device to publish syslog messages, consider the following restrictions:

- In releases prior to 4.2.1, do not customize the priority of any syslog messages. If you do, MARS fails to parse those messages.
- **Do not** configure EMBLEM format for syslog messages. Make sure that the format EMBLEM extension is not used on the following command in the configuration:

  ```
  logging host <interface name> <PN-MARS's IP address> format EMBLEM
  ```

To send syslog messages to the MARS Appliance, you must enable logging, select the log facility and queue size, and specify the log level to debug.

Step 1 Log in to the Cisco firewall device with administrator's privileges.

Step 2 To enable logging, enter one of the following commands:

- (PIX and Cisco ASA) **logging enable**
- (FWSM) **logging on**

Step 3 To specify the MARS Appliance as a target logging host, enter the following command:

```
logging host <interface name> <MARS IP address>
```

Step 4 To set the log level to debug, which ensures that HTTP and FTP session logs are generated, enter the following command:

```
logging trap debugging
```

Tip Alternatively, you can tune the event settings as defined in Device-Side Tuning for Cisco Firewall Device Syslogs, page 5-6.

The debug messages contain the HTTP URL address information. Therefore, you can create keyword-based rules matching against the firewall message itself. For example, if the debug messages are enabled and users were logging to “http://mail.cisco.com”, you could create keyword-based rules that matched against “mail.yahoo.com.”

Note Full URLs, such as `www.cisco.com/foo.html`, are included in HTTP session logs and FTP command data is logged only if web filtering (N2H2\SecureComputing or WebSense) is enabled on the reporting device. If web filtering is not enabled, then the HTTP session log does not include the hostname (although the destination host's IP and the Request-URI are included, such as `192.168.1.1:/foo.htm`) and FTP command data is not logged at all. Caveats exist with HTTP session logging, such as if the HTTP session request is broken across packets, then the hostname data might not be included in the log data.

Debug messages are also preferred for troubleshooting. You can define inspection rules that match on on debug-level keywords, which send notifications to the appropriate group. Refer to PIX debug messages for interesting keywords.

Cisco recommends enabling debug for optimal use of your STM solution. If a Cisco firewall device is unable to sustain debug-level messages due to performance reasons, the informational level should be used. In non-debug mode, the URL information is not available; only the 5 tuple is available for queries and reports.

Step 5 For FWSM, enter the following command:

```
logging rate-limit <eps rate desired> 1
```

Step 6 For Cisco ASA, PIX 7.0 and 8.0, and FWSM, repeat Step 2 through Step 5 for each context defined, admin and security.

Step 7 (Cisco ASA only) If an Advanced Inspection and Prevention (AIP) module is installed, you need to prepare that module as you would any IPS 5.0 module. For more information, see Cisco IPS Modules, page 8-16.

Device-Side Tuning for Cisco Firewall Device Syslogs

The default level for many of the events that are studied by MARS is the debug level, which can generate a high volume of additional events that are not used by MARS. If you are experiencing an influx of these other events, you can use the **logging message** command to either turn off events or change the severity level of the event to a level that generates required messages but not as many as debug.

This topic identifies the commands to use to change the log level from the command line, as well as identifies those messages consumed by MARS and their default severity level.

Logging Message Command

The following references provide details for using the logging message command on the appropriate firewall device:

Cisco ASA and Cisco PIX

- "Changing the Severity Level of a System Log Message" in *Cisco Security Appliance Command Line Configuration Guide, Version 7.2*

  http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/monitor.html#wp1065731
- "Disabling a System Log Message" in *Cisco Security Appliance Command Line Configuration Guide, Version 7.2*

  http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/monitor.html#wp1065706
- "Logging Message Command" in *Cisco Security Appliance System Log Messages, Version 7.2*

  http://www.cisco.com/en/US/docs/security/asa/asa72/command/reference/l2_72.html#wp1689570
- *Cisco Security Appliance System Log Messages, Version 7.2*

  http://www.cisco.com/en/US/docs/security/asa/asa72/system/message/logmsgs.html

Cisco FWSM

- "Changing the Severity Level of a System Log Message" in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 3.1*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm32/configuration/guide/monitr_f.html#wp1099894
- "Disabling a System Log Message" in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 3.1*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/configuration/guide/monitr_f.html#wp1099869
- "Logging Message Command" in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference, 3.1*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/command/reference/l2.html#wp1565791
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages, 3.1*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/system/message/fwsm_log.html

List of Cisco Firewall Message Events Processed by MARS

The following list of events are processed by MARS. By changing the severity level for these events to ensure they are within the logging level you have selected, you can typically reduce the load on your firewall logging by 5-15%. However, the primary consumer of resources will remain the session detail events, which are processed and analyzed by MARS.

Starting with MARS version, the system can correctly parse syslogs at customized logging levels. Therefore, you can move the syslogs processed by MARS to a lower level and then set the log to that level, for example *logging level 6*. Use the command **logging message** *message-id* **level** *level* on the ASA, or PIX, to move a syslog message to a new level.

The following syslog message IDs are those required for proper sessionization. If you change the logging level of the firewall, ensure that the following messages IDs are generated at the new level so the MARS Appliance receives them.

Note The syslog message IDs listed below are required for sessionization. However, other logs at the debug or informational levels may exist that you may require for other purposes. for example, a specific URL accessed by one user if you are doing URL filtering on the security appliance. Refer to the Logging Message Command, page 5-6 for pointers to the full message list for each firewall device type.

- 101001-101005
- 102001
- 103001-103007
- 104001-104004
- 105001-105011
- 105020-105021
- 105031-105032
- 105034-105040
- 105042-105048
- 106001-106002
- 106006-106007
- 106010-106027
- 106100-106101
- 107001-107003
- 108002-108003
- 108005
- 108007
- 109001-109003
- 109005-109008
- 109010-109014
- 109016-109034
- 110001-110003
- 111001

- 111003-111005
- 111007-111009
- 111111
- 112001
- 113001
- 113003-113023
- 114001-114021
- 199001-199003
- 199005-199009
- 199011
- 199012
- 199907-199908
- 201002-201006
- 201008-201013
- 202001
- 202005
- 202011
- 208005
- 209003-209005
- 210001-210003
- 210005-210008
- 210010
- 210020-210022
- 211001
- 211003
- 212001-212006
- 213001-213006
- 214001
- 215001
- 216003
- 216004
- 217001
- 218001-218004
- 219002
- 302001
- 302003-302004
- 302007-302010
- 302012-302023

- 302033
- 302034
- 302302
- 303002-303005
- 304001-304009
- 305005-305012
- 308001-308002
- 311001-311004
- 312001
- 313001
- 313003-313005
- 313008
- 314001-314006
- 315004
- 315011
- 316001
- 316002
- 317001-317006
- 318001-318009
- 319001-319004
- 320001
- 321001-321004
- 322001-322004
- 323001-323006
- 324000-324007
- 324300-324301
- 325001-325003
- 326001-326002
- 326004-326017
- 326019-326028
- 327001-327003
- 328001
- 329001
- 331001-331002
- 332001-332004
- 333001-333010
- 334001-334009
- 335001-335014

- 336001-336011
- 400000-400050
- 401001-401005
- 402101-402103
- 402106
- 402114-402120
- 402121-402127
- 403101-403104
- 403106-403110
- 403500-403507
- 404101-404102
- 405001-405002
- 405101-405107
- 405201
- 405300-405301
- 406001-406002
- 407001-407003
- 408001-408003
- 409001-409013
- 409023
- 410001-410004
- 411001-411004
- 412001-412002
- 413001-413006
- 414001-414002
- 415001-415020
- 416001
- 417001
- 417004
- 417006
- 417008-417009
- 418001
- 419001-419002
- 420001-420006
- 421001-421007
- 422004-422006
- 423001-423005
- 424001-424002

- 425001-425006
- 428001
- 431001-431002
- 446001
- 450001
- 500001-500004
- 501101
- 502101-502103
- 502111-502112
- 503001
- 504001-504002
- 505001-505016
- 506001
- 507001-507002
- 508001-508002
- 509001
- 602101-602104
- 602201-602203
- 602301-602304
- 603101-603109
- 604101-604104
- 605004-605005
- 606001-606004
- 607001-607002
- 608001-608005
- 609001-609002
- 610001-610002
- 610101
- 611101-611104
- 611301-611323
- 612001-612003
- 613001-613003
- 614001-614002
- 615001-615002
- 616001
- 617001-617004
- 620001-620002
- 621001-621003

- 621006-621010
- 622001
- 622101-622102
- 634001
- 701001-701002
- 702201-702212
- 702301-702303
- 702305
- 702307
- 703001-703002
- 709001-709007
- 710001-710006
- 711001-711002
- 713004
- 713006
- 713008-713010
- 713012
- 713014
- 713016-713018
- 713020
- 713022
- 713024-713037
- 713039-713043
- 713047-713052
- 713056
- 713059-713063
- 713065-713066
- 713068
- 713072-713076
- 713078
- 713081-713086
- 713088
- 713092
- 713094
- 713098-713099
- 713102-713105
- 713107
- 713109

- 713112-713124
- 713127-713149
- 713152
- 713154-713172
- 713174
- 713176-713179
- 713182
- 713184-713187
- 713189-713190
- 713193-713199
- 713203-713206
- 713208-713226
- 713228-713251
- 713254
- 713900-713906
- 714001-714007
- 714011
- 715001
- 715004-715009
- 715013
- 715019-715022
- 715027-715028
- 715033-715042
- 715044-715072
- 715074-715079
- 716001-716056
- 717001-717049
- 718001-718081
- 718082-718088
- 719001-719026
- 720001-720073
- 721001-721019
- 722001-722041
- 723001-723014
- 724001-724002
- 725001-725015
- 726001
- 730001

- 730002-730005
- 730010
- 731001-731003
- 732001-732003
- 733100
- 733102
- 733103
- 734002-734004

Add and Configure a Cisco Firewall Device in MARS

The process of adding a PIX security appliance, Cisco ASA, or FWSM to MARS involves many of the same steps, regardless of the version of software that is running. The process is exactly the same for PIX software versions 6.0, 6.1, 6.2, and 6.3. However, Cisco ASA, PIX 7.0 and 8.0, and FWSM provide the ability to define multiple security contexts, or virtual firewalls.

Adding a Cisco ASA, PIX 7.0 and 8.0, and FWSM to MARS has two distinct steps. First, you must define the settings for the admin context. Then, if multiple context mode is enabled, you define or discover the settings for its security contexts. These Cisco firewall device have two type of contexts: one admin context, which is used for configuration of the device itself, and one or more security contexts. For Cisco ASA, you can also define or discover any modules that are installed in the appliance.

To be monitored by MARS, the Cisco ASA, PIX 7.0 and 8.0, and FWSM device types have the following additional requirements:

- each context requires a unique routable IP address for sending syslog messages to MARS
- each context must have a unique name (hostname+ domain name)

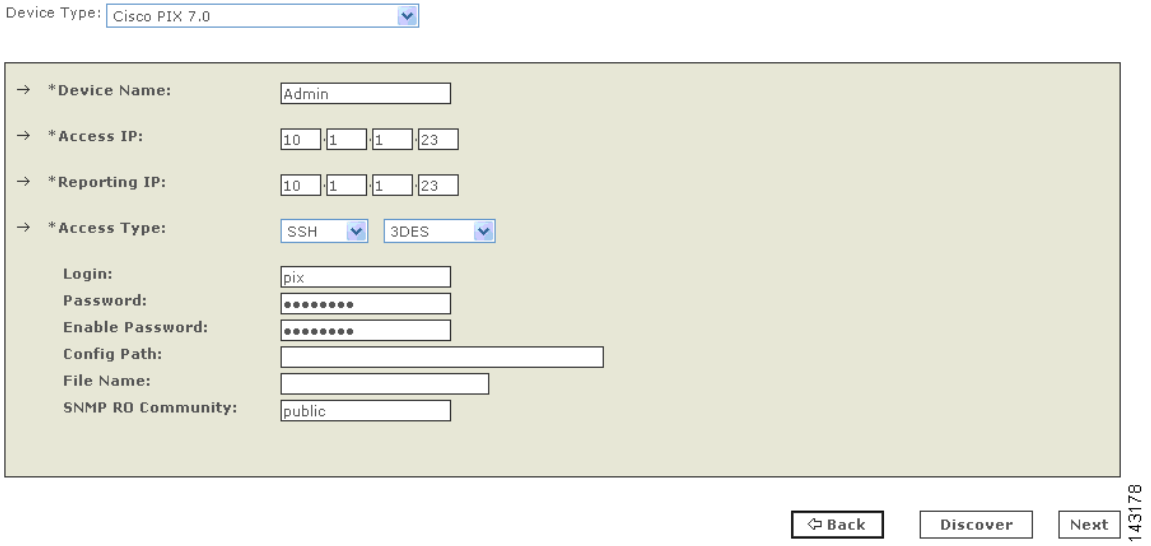
Note The Cisco ASA, PIX 7.0 and 8.0, and FWSM can run in single context mode, which means that the system context acts as both the admin context and a security context.

To add and configure a Cisco firewall device, follow these steps:

Step 1 Do one of the following:

- If you are adding an FWSM, you must be on the main page of the Cisco switch to which you are adding it. On that page, click **Add Module**, and select one of the following options from the Device Type list:
  - Cisco FWSM 1.1
  - Cisco FWSM 2.2
  - Cisco FWSM 2.3
  - Cisco FWSM 3.1
  - Cisco FWSM 3.2
- If you are adding a PIX security appliance or a Cisco ASA, an Select **Admin > System Setup > Security and Monitor Devices > Add**, and select one of the following options from the Device Type list:

- Cisco ASA 7.0
- Cisco ASA 7.2
- Cisco ASA 8.0
- Cisco PIX 6.0
- Cisco PIX 6.1
- Cisco PIX 6.2
- Cisco PIX 6.3
- Cisco PIX 7.0
- Cisco PIX 7.2
- Cisco PIX 8.0



Step 2 Enter the name of the firewall 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 3 (Optional) To enable MARS to discover settings from this firewall device, enter the administrative IP address in the Access IP field.

Note If the device is running Cisco ASA, PIX 7.0 and 8.0, or FWSM, this address corresponds to IP address from which the syslog messages of the admin context are sent.

To learn more about the access IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.

Step 4 Enter the IP address of the interface that publishes syslog messages or SNMP notifications, or both in the Reporting IP field.

Note If the device is running Cisco ASA, PIX 7.0 and 8.0, or FWSM, this address corresponds to the address from which the admin context syslog messages are published.

To learn more about the reporting IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.

Step 5 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 2-12
- Configure SSH Access for Devices in MARS, page 2-12
- Configure FTP Access for Devices in MARS, page 2-12

Note If you select the FTP access type and you are defining a Cisco ASA, PIX 7.0 and 8.0, or FWSM, you cannot discover the non-admin context settings. Therefore, this access type is not recommended.

For more information on determining the access type, see Selecting the Access Type, page 2-10.

Step 6 (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.

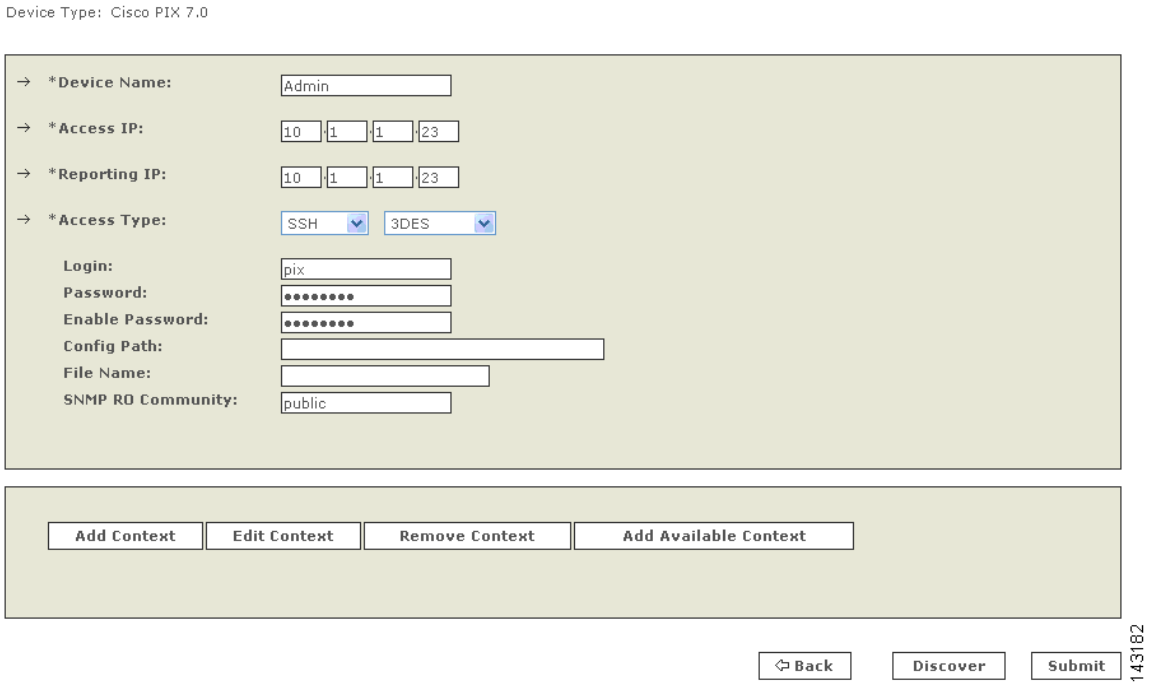
Step 7 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

Result: MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 2-42.

Step 8 (Cisco ASA, FWSM, and PIX 7.0 and 8.0 Only) do one of the following:

- Click **Discover** to let MARS contact the device and conduct a topology and context configuration discovery. Information about the security contexts is presented in the Context section of the main page. To edit discovered contexts, continue with Edit Discovered Security Contexts, page 5-19.
- Click **Next** to commit your changes and allow for manual definition of security contexts or modules. Continue with Add Security Contexts Manually, page 5-17, Add Discovered Contexts, page 5-18, or Add an IPS Module to a Cisco Switch or Cisco ASA, page 8-18.

  For PIX and FWSM, you can add one or more security contexts. For Cisco ASA, you can add one or more security contexts or Advanced Inspection and Prevention (AIP) modules, running the Cisco IPS 5.x software.



Step 9 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings, including any security contexts and their settings.

Result: 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 2-40.

Step 10 To add this device to the MARS database, click **Submit**.

Result: 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 11 Click **Activate**.

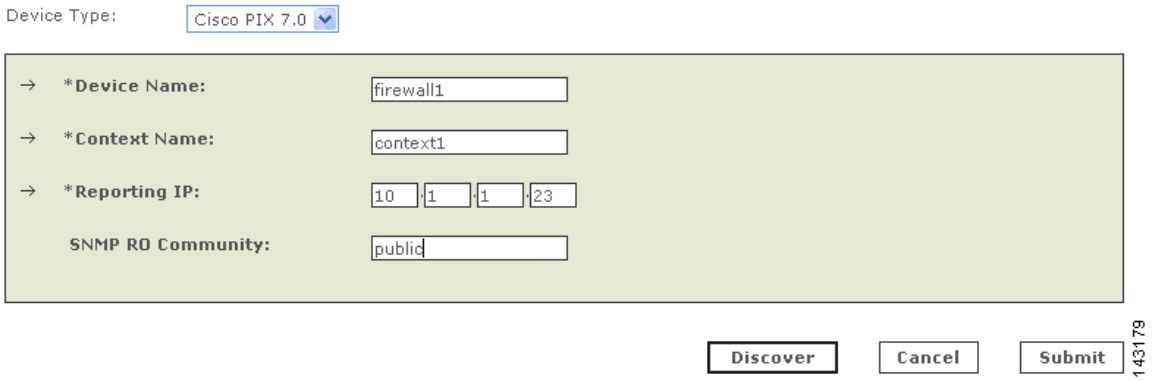
Result: MARS begins to sessionize events generated by this device and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 2-28.

Add Security Contexts Manually

You can manually define security contexts in PIX 7.0 and 8.0, Cisco ASA, or FWSM.

Step 1 Do one of the following:

- (PIX 7.0 and 8.0 and FWSM) Click **Add Context**.
- (Cisco ASA) Click **Add Module**.



Step 2 In the Device Type list, do one of the following:

- For Cisco ASA, select **Cisco ASA 7.0** or **Cisco ASA 8.0**.
- For PIX, select **Cisco PIX 7.0** or **Cisco PIX 8.0**.
- For FWSM, select **Cisco FWSM *x.y***, where *x.y* is the version number of the software running on the module.

Step 3 Enter the name of the firewall 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 Enter the name of the security context in the Context Name field.

This name must exactly match the context name defined on the device.

Step 5 Enter the IP address of the security context from which syslog messages or SNMP notifications, or both are published 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 2-8.

Step 6 (Optional) To enable MARS to retrieve MIB objects for this security context, 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 security context's CPU usage, network usage, and device anomaly data and to discover device and network settings.

Step 7 To discover the settings of the defined context click **Discover**.

This discovery collects all of the route, NAT, and ACL-related information. In addition, the name of the device may change to the *hostname.domain* format if it was not already entered as such.

Step 8 To save your changes, click **Submit**.

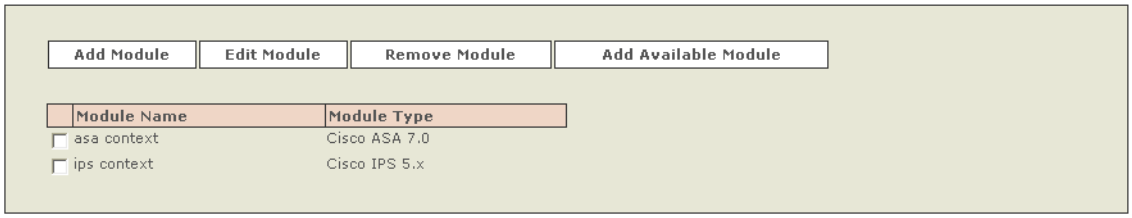
Add Discovered Contexts

When you select Discover on a Cisco ASA, PIX 7.0 and 8.0 or FWSM, MARS discovers the contexts that are defined for that firewall device. However, you must still manually add discovered contents.

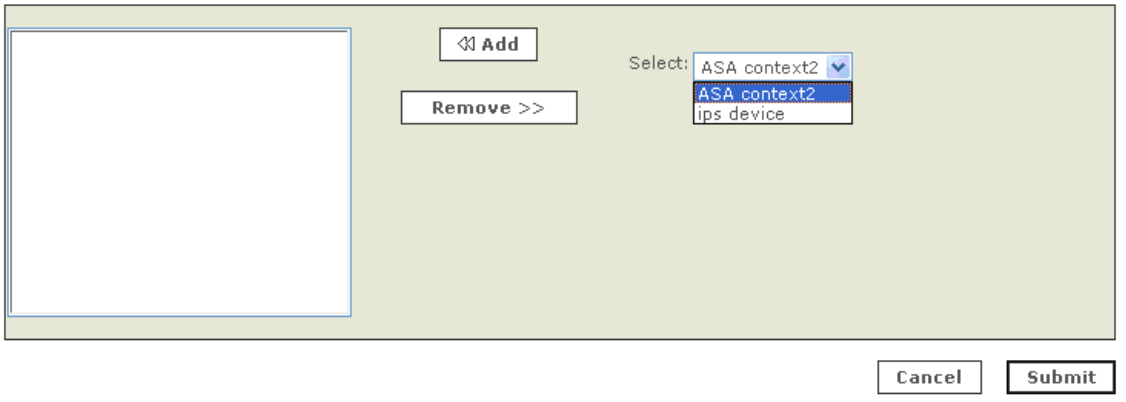
Note You cannot discover a module install in a Cisco ASA; you must manually define IPS modules. However, the discovered contexts do appear under the Module area on the main page.

Step 1 Do one of the following:

- (PIX 7.0 and 8.0 and FWSM) Click **Add Available Context**.
- (Cisco ASA) Click **Add Available Module**.



Step 2 Select a security context from the Select list.



Step 3 Click **Add**.

Step 4 Repeat for other contexts.

Step 5 To save your changes, click **Submit**.

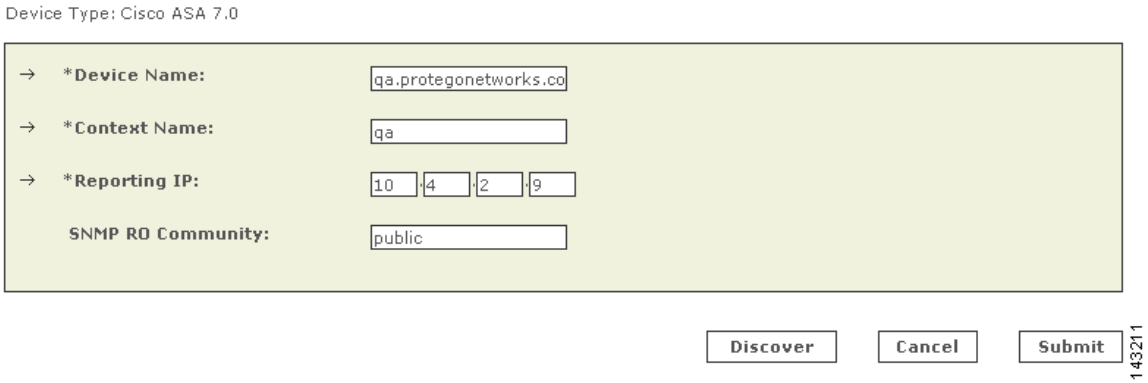
After you add discovered contexts, you must edit them to provide the contact information required by MARS. Continue with Edit Discovered Security Contexts, page 5-19.

Edit Discovered Security Contexts

Note You must edit all discovered contexts to specify the reporting IP address and the SNMP RO community string.

Step 1 From the list of discovered contexts, select the one that you want to edit and select the action appropriate to the device type:

- (PIX 7.0 and 8.0) Click **Edit Context**.
- (Cisco ASA and FWSM) Click **Edit Module**.



Step 2 Enter the IP address from which the syslog messages of the security context are sent in the Reporting IP field.

Step 3 (Optional) To enable MARS to retrieve MIB objects for this context, 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 4 (Optional) To enable MARS to monitor this context for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

Result: MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 2-42.

Step 5 To save your changes, click **Submit**.

Step 6 Repeat for each discovered context.

NetScreen ScreenOS Devices

MARS can monitor NetScreen ScreenOS devices, versions 4.0 and 5.0. To enable this monitoring, you must:

1. Provide MARS with SNMP, SSH or Telnet administrative access to NetScreen device.
2. Define the SNMP RO community strings to shared between the NetScreen device and MARS.
3. Specify which 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:

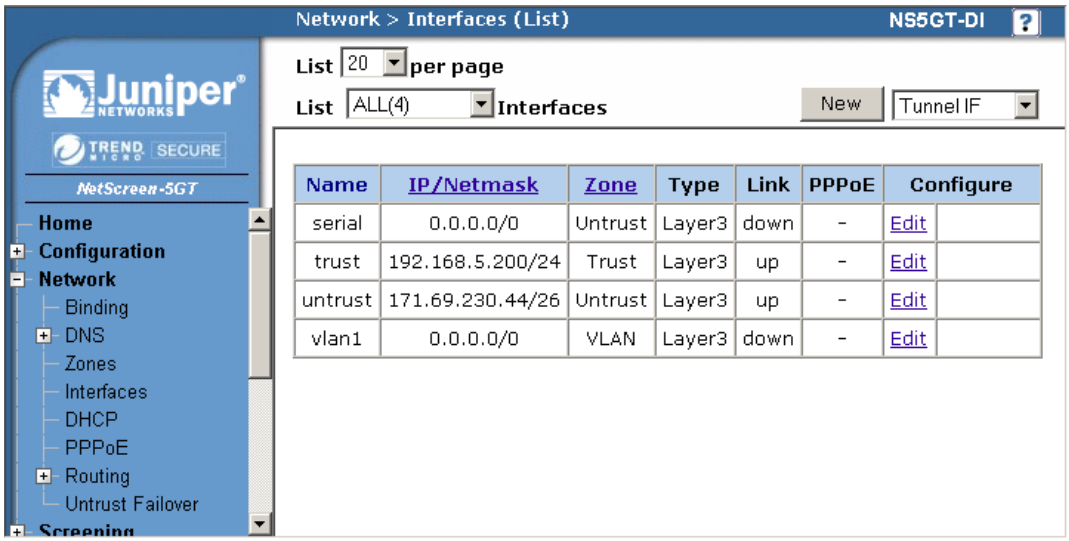
- Bootstrap the NetScreen Device, page 5-21
- Add the NetScreen Device to MARS, page 5-26

Bootstrap the NetScreen Device

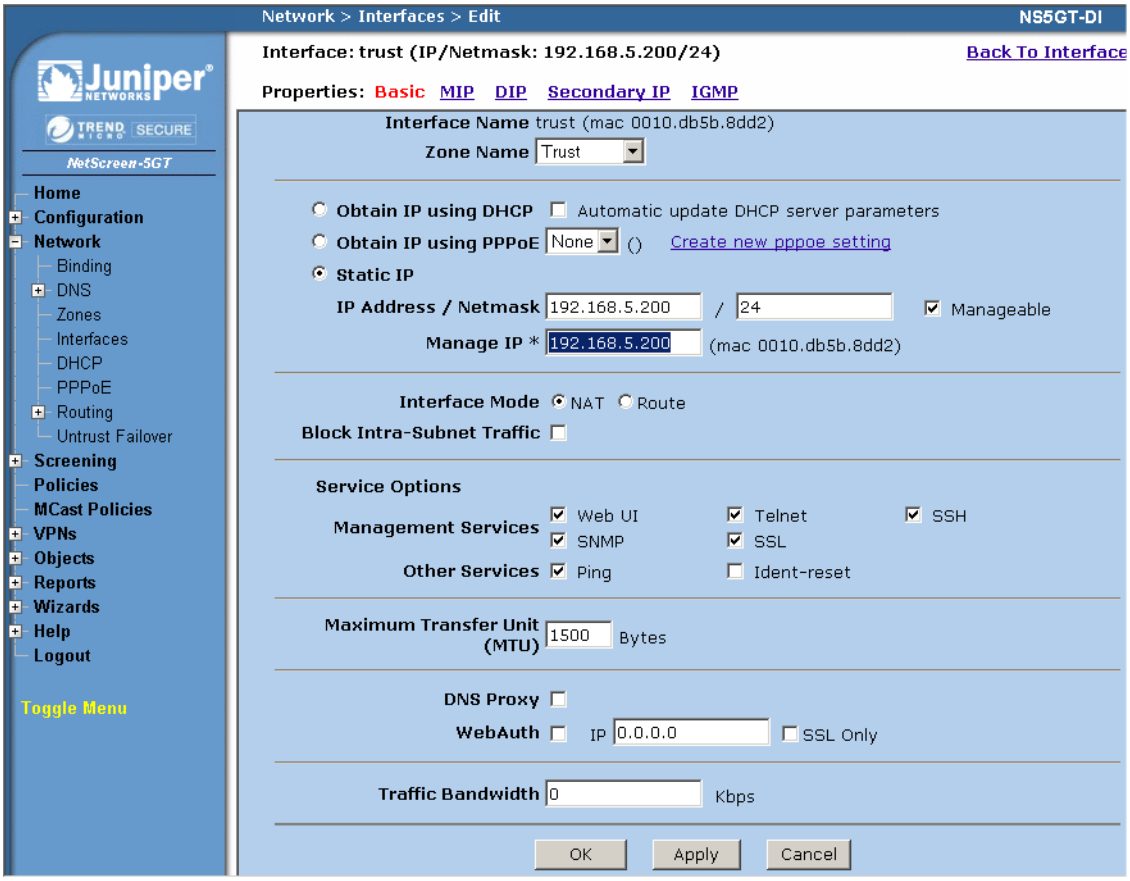
To prepare the NetScreen device to be monitored by MARS, follow these steps:

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.



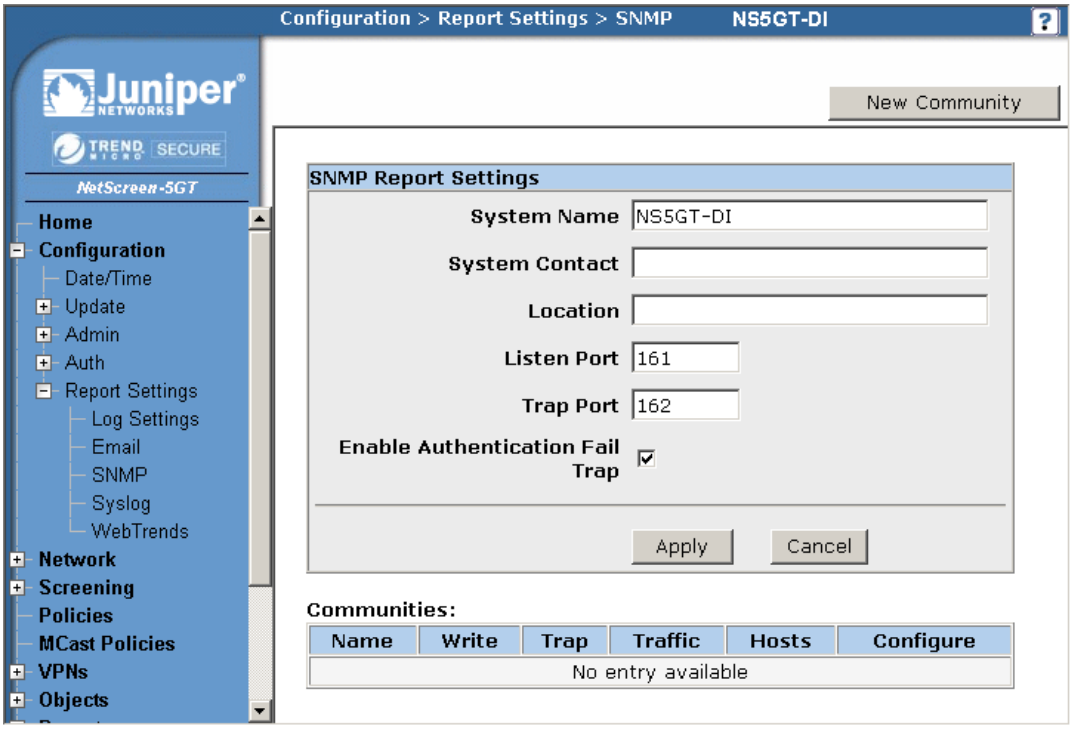
Step 4 Under Service Options, select one of the following values:

- 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 5-26.

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

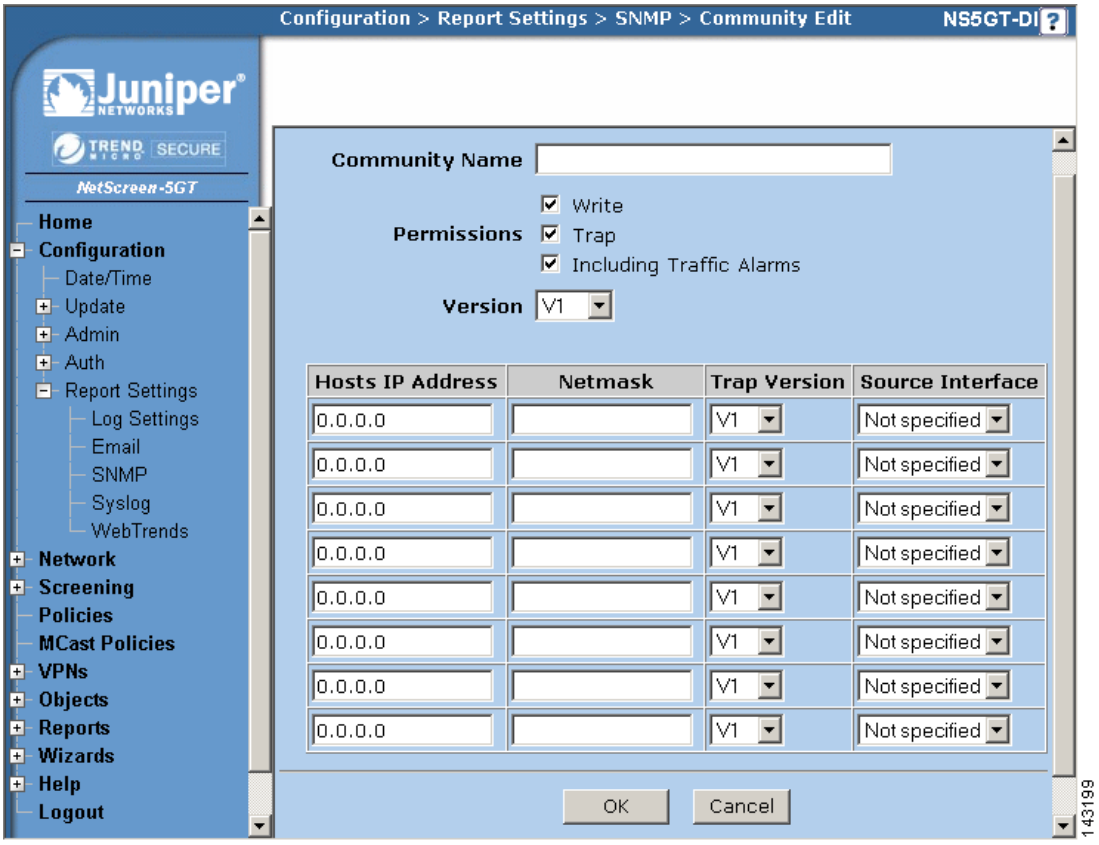
Step 6 Configure the SNMP information by selecting **Configure > Report Settings > SNMP**.



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

Step 8 Enter the MARS IP address and verify that this Community Name in this window is the same 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 on 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.

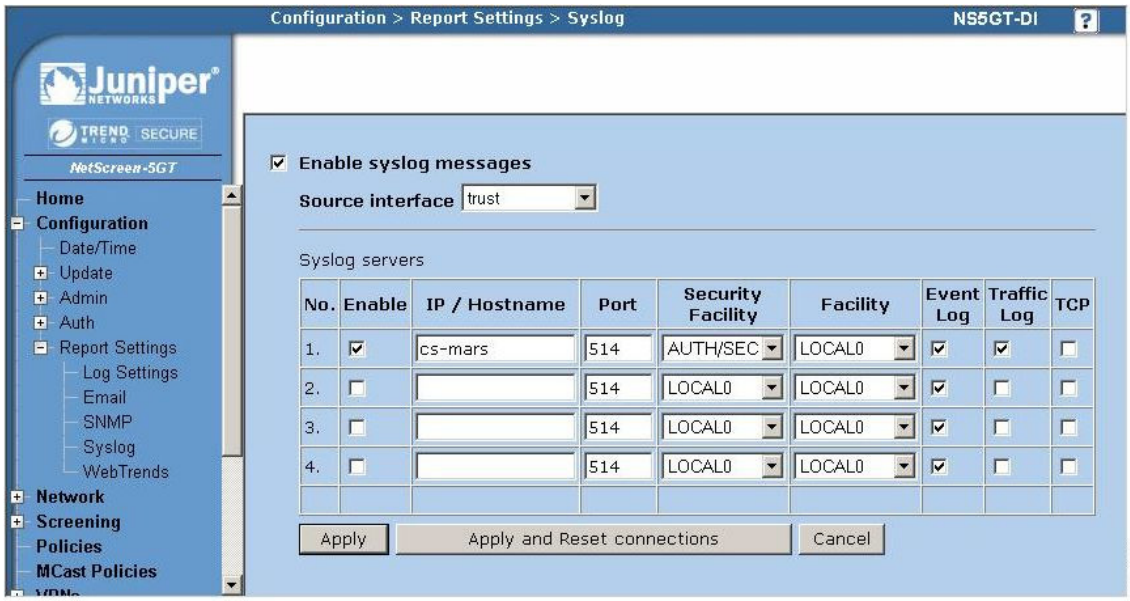
Step 12 Enter the IP address of the MARS Appliance that will listen for events from this device

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

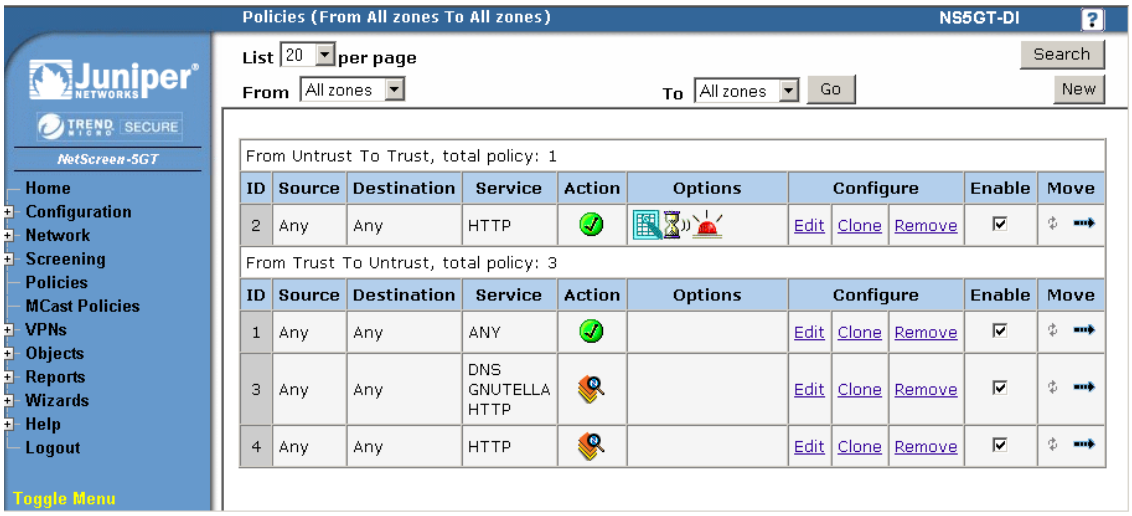
Step 14 Select the **AUTH/SEC** for **Security Facility** and **LOCAL0** for **Facility**.

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

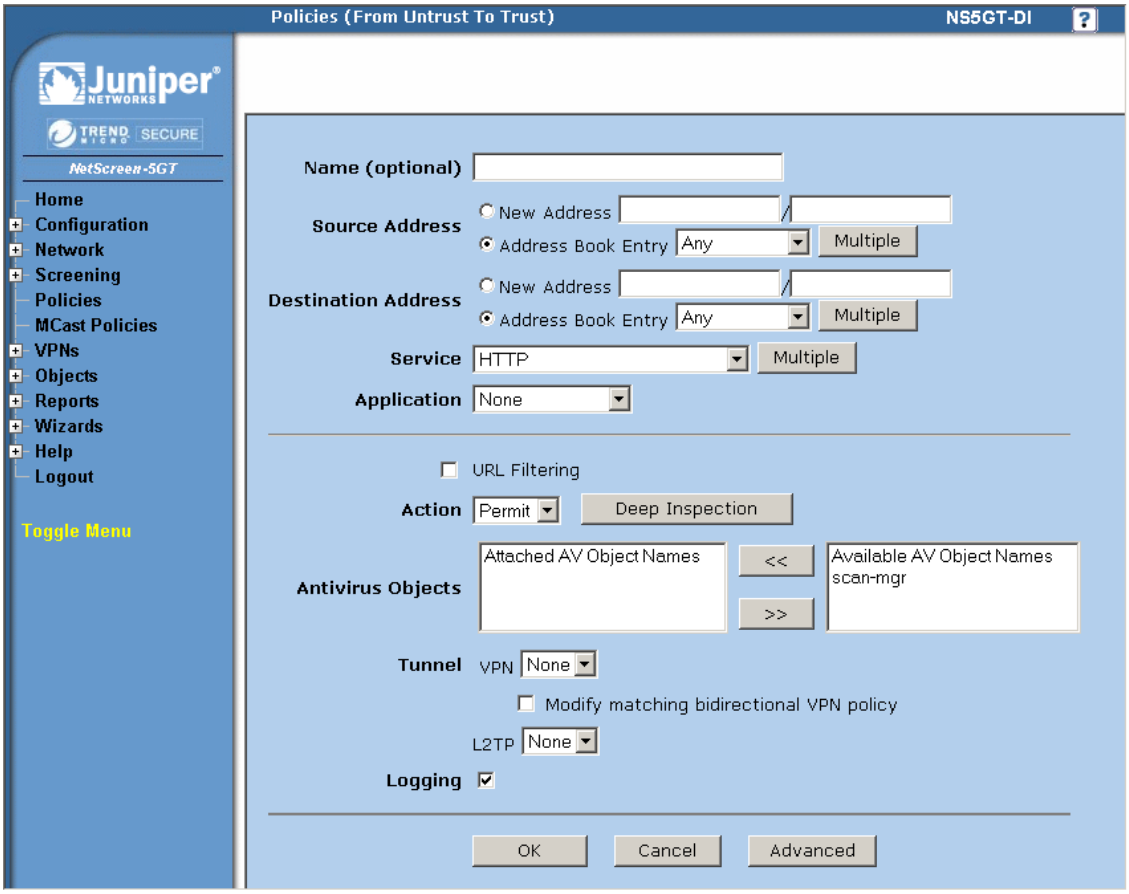
Step 16 Click **Apply**.



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.



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 the appropriate version of NetScreen ScreenOS from the Device Type list.

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 2-8.

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 2-8.

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

- Configure SNMP Access for Devices in MARS, page 2-11
- Configure Telnet Access for Devices in MARS, page 2-12
- Configure SSH Access for Devices in MARS, page 2-12

For more information on determining the access type, see Selecting the Access Type, page 2-10.

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.

Result: 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 2-40.

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

Result: 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**.

Result: 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 2-28.

Check Point Devices

The Check Point security product family can be distributed and tiered. As such, you must understand the deployment method, components, and release versions of this product family, their relationships, and how MARS interacts with them. You must also understand the many acronyms and abbreviations associated with this product family. Table 5-1 lists the abbreviations and acronyms used in the topics that follow.

Table 5-1 Check Point Abbreviations and Acronyms

Abbreviation	Expansion	Additional Information
ASYMSSLCA	Secure Sockets Layer Certificate Authority using an asymmetric key cipher	Communications protocol used for establishing secure sessions.
CLM	Customer Log Modules	Standalone log server for collecting log data from the Check Point enforcement modules.
CMA	Customer Management Add-ons	A a virtual instance of SmartCenter and only exists within the context of a Provide-1/SiteManager-1 infrastructure.
CPMI	Check Point Management Interface	Communications protocol used for configuration discovery.
LEA	Log Export API	Communications protocol used for retrieving audit and firewall logs.
MDG	Multi Domain GUI	GUI used for managing Provider-1/ SiteManager-1 deployments. The MDG is the parent GUI that can launch specific SmartDashboard GUIs for a CMA.
MDS	Multi Domain Server	Is the umbrella manager for the CMA instances in a Provider-1/SiteManager-1 deployment.
MLM	Multi Domain Log Module	Usually found in Provider-1/ SiteManager-1 deployments and provides the ability to create multiple instances of a CLM on a single logging server.
NG AI	Next Generation with Application Intelligence	All current trains of Check Point are released under the NG AI umbrella with specific release numbers, such as NG AI R55 and NG AI R60.
NG FP3	Next Generation Feature Pack 3	—
NGX	Next Generation eXtension	NGX is also NG AI R60
OPSEC	Open Platform for Security	An alliance, certification and integration methodology for products and solutions that integrate into a Check Point infrastructure.
P-1	Check Point Provider-1	—
SSLCA	Secure Sockets Layer Certificate Authority, using a symmetric key cipher (protocol)	—
SIC	Secure Internal Communication	—
SIC DN	SIC Distinguished Name	—

Table 5-1 Check Point Abbreviations and Acronyms

Abbreviation	Expansion	Additional Information
VIPs	Virtual IP Addresses	Usually used in a Provider-1/ SiteManager-1 deployment to assign unique IP addresses for CMA instances.
VPN-1	Check Point VPN-1 Pro and Edge	VPN-1 Pro is the Check Point enforcement gateway that does the inspection, firewalling, VPN encryption and QoS tagging. VPN-1 Edge is treated as a normal enforcement point.

To understand what MARS supports, we must first clarify the product terminology used by Check Point. NG refers to the 5.x product family, and it included three feature packs: FP1, FP2, and FP3. NG is different from NG AI in that NG AI improved upon, and renamed, the SmartDefense feature set that was introduced in NG FP2. NG AI also provides a larger number of application-aware inspections,; hence the name Application Intelligence. NG AI included releases R54 and R55. NGX refers to the 6.x product family and began with the R60 release.

MARS supports and has been tested with the following releases:

- NG FP3
- NG AI (R55)
- NGX (R60)

The different security platforms, Provider-1, SiteManager-1, SmartCenter, and SmartCenter Pro are bundles of the technologies released under the NG, NG AI, and NGX release trains. From this perspective, MARS works with any of the security platforms as long as it belongs to one of the supported release trains.

Check Point Provider-1 is a security management system for the managed security service providers (MSSP) and multi-site enterprises, respectively. Service providers are able to manage the Check Point gateways (firewall and VPN gateways) on their customer sites. The security policies and the system configurations are stored on the MDS. Each per-customer security policy is managed through a CMA, which also reside on the MDS. The Provider-1 system allows the service provider and the end customers to maintains separate log servers, using the MLM and CLM respectively. The user interface for Provider-1 is called the MDG. This system also support a tiered fault-tolerant configuration via redundancy at the gateway, CMA, or MDS level.

The Provider-1 system ensures secure and private communication between its components and Check Point gateways. Each CMA has its own internal certificate authority that issues certificates for secure communication between the CMA, log servers, and its own network. All communication between MDSs is authenticated and secured, and every MDS communicates securely with the CMAs that it houses.

The SiteManager-1 system operates much the same as Provider-1; however, it is targeted toward large enterprise customers. The Check Point components are the same as those found in Provider-1.

SmartCenter and SmartCenter Pro are security management systems also targeted toward enterprise customers. They can support the Provider-1 system, serving as a backup server at the CMA level. However, their primary function is to provide centralized security and VPN policy and security event management through SmartDashboard, which is the user interface for both systems. From the MARS perspective, SmartCenter has the ability to extend the view of the network by managing the policies and events associated with gateway and desktop nodes:

- VPN-1 perimeter security gateways,
- InterSpect internal security gateways
- Connectra Web security gateways
- SecureClient, a personal firewall running on desktops and servers.

MARS monitors the primary management servers, such as the MDS in Provider-1 and SiteManager-1 and the SmartCenter Server in SmartCenter and SmartCenter Pro. These management servers are where the actual security and audit policies are centrally managed and stored. If the Check Point deployment requires, MARS also monitors those components managed by the management stations, such as individual firewalls, VPN gateways, and log servers. Whether you configure MARS to monitor these remote components depends on whether their security event logs are propagated to the centralized management servers (SmartCenter or CMA). If the logs are not forwarded to the primary management server, then you must define where the log repository exists, whether local to the enforcement module, or forwarded to a separate logging module (CLM).

In addition to understanding the components, it is important to understand how Check Point components use Secure Internal Communications (SIC) to securely communicate with each other and with third-party OPSEC applications. SIC is the process by which MARS Appliance authenticates to the SmartCenter Server and other Check Point components. SIC uses a shared secret as the seed for negotiating session keys. This shared secret is referred to as an activation key. The authentication and communication setup works as follows:

1. Using a username and password pair, MARS authenticates to the SmartCenter Server and other Check Point components, such as remote log servers, using TCP port 18210.
2. If authenticated, the peers swap the activation key and each other's SIC using TCP port 18190.
3. If each peer validates the authenticity of the other, the Check Point component establish an encrypted session over TCP port 18184 with the MARS Appliance. It is over this channel that the Check Point components to sends encrypted log data to MARS.

The following topics support the integration of MARS into a Check Point environment:

- Determine Devices to Monitor and Restrictions, page 5-30
- Bootstrap the Check Point Devices, page 5-31
- Add and Configure Check Point Devices in MARS, page 5-44
- Troubleshooting MARS and Check Point, page 5-61

Determine Devices to Monitor and Restrictions

To configure Check Point devices, you must identify the central management server and managed components, bootstrap them, and add and configure them in the MARS web interface. The Check Point product line and release, as well as the number of devices managed, determines which tasks you must perform to configure MARS to monitor your Check Point devices.

Representing a Check Point device in MARS involve two steps:

1. **Define a primary management station.** This primary management station represents the central management server that manages remote components, such as firewalls, VPN gateways, and log servers.
2. **Define one or more child enforcement modules.** Child enforcement modules are the remote components managed by the primary management station. They represent firewalls, VPN gateways, and log servers.

When managing SmartCenter and SmartCenter Pro, the primary management station is the SmartCenter server. When managing Provider-1/SiteManager-1 releases NG FP3, NG AI (R55), and NGX (R60), the primary management station is not the MDS, but each CMA defined under the MDS. In other words, you must define each CMA as a separate primary management station. The child enforcement modules are those gateways and logs servers (CLMs) managed as part of that customer or site as defined by the CMA.

Part of what you must determine is where the security event logs are stored. Two options exist:

- **Central Event Correlation.** The MLM or SmartCenter server pulls logs from all remote components.
- **Distributed Event Correlation.** In addition to the MLM or SmartCenter Server, one or more remote log servers exist where aggregation to the central management server does not occur. These severs, the CLMs, must also be represented and configure so that MARS can pull the events from them.

If the security events are stored in a distributed fashion, you must plan to define and establish SIC communication between the MARS Appliance and each Check Point log module. For SmartCenter and SmartCenter Pro, the server SIC DN is the one assigned to the primary management station. However, for Provider-1 and SiteManager-1, the server SIC DN varies based on release. For Provider-1 and SiteManager-1 NG FP3 and NG AI (R55), the server SIC DN is the one associated with the CMA. For Provider-1 and SiteManager-1 NGX (R60), you can use the SIC assigned to the MDS for all CMAs and CLMs that you define.

One other restriction exists with the Provider-1 and SiteManager-1 products. For Provider-1 and SiteManager-1 NG FP3 and NG AI (R55), you must define an OPSEC application representing the MARS Appliance in each CMA (using the CMAs SmartDashboard user interface). For Provider-1 and SiteManager-1 NGX (R60), you can define one OPSEC application representing the MARS Appliance and push that definition to all CMAs and CLMs managed by the MDS.

Bootstrap the Check Point Devices

Bootstrapping the Check Point devices involves preparing those devices to send data to the MARS Appliance, as well as enabling the MARS Appliance to discover the Check Point configuration settings. In addition to preparing the Check Point devices, you must gather the information required to represent the Check Point devices in the MARS web interface.

You bootstrap the central Check Point management server, whether it be a CMA or a SmartCenter server by defining the MARS Appliance as a target log host and OPSEC Application object.

1. Using Check Point SmartDashboard or the Check Point Provider-1/SiteManager-1 MDG, add the MARS Appliance as a host.
2. Create and install an OPSEC Application object for the defined host, import the authorization key, and generate the client SIC DN. This SIC DN is the one used by OPSEC applications, including the management server, to validate the MARS Appliance. You specify this client SIC DN in the MARS web interface. When a session is established between the MARS Appliance and the Check Point management server, the appliance publishes this SIC to the management server to ensure non-repudiation of the appliance.
3. Obtain the server SIC DN of the Check Point management server. You specify this sever SIC in the MARS web interface. The MARS Appliance validates the server SIC DN against the SIC published to the appliance by the management server during session setup. This validation ensures non-repudiation of the server.
4. Create the policies to permit SIC traffic between the defined host (MARS Appliance), the Check Point management server, and any remote servers. After you identify the devices, you must verify that the network services they use for SIC-based management and reporting are permitted on the

reporting device. To enable these traffic flows, you must verify or update the policies that enable the SIC traffic to flow between each reporting device and the MARS Appliance. Once you have updated these policies, you must install the policies.

5. Define the log settings to push the correct events to the defined host. You must ensure that all of the security, firewall, user authentication, and audit events are logged and configured to be published to the MARS Appliance.
6. Install the policies. Once the policies are defined, you must update the Check Point components with the policies. Policy installation include an object database push that make the Check Point modules aware of the OPSEC Application representing the MARS Appliance. Without this step, the modules will not forward any log information via LEA.

To perform this task, you need a Check Point user account with administrative privileges. This account must be able to create a new host, define OPSEC application, define and install new policies, and access the settings of each managed Check Point component.

After completing this task, you should have collected the following information:

- The Client and server SIC DNs.
- If you are defining a CMA for Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), then you must have the virtual IP address (VIP) for each CMA and CLM managed by the MDS. Only Provider-1 and SiteManager-1 NGX (R60) requires the physical IP addresses of the MDS and MLM servers.
- Any CLMs, instead of CMAs, to which security logs are being sent. If logs are being sent to CLMs, LEA is only supported using clear text.

To bootstrap the Check Point devices, perform the following procedures:

- Add the MARS Appliance as a Host in Check Point, page 5-32
- Define an OPSEC Application that Represents MARS, page 5-33
- Obtain the Server Entity SIC Name, page 5-36
- Select the Access Type for LEA and CPMI Traffic, page 5-38
- Create and Install Policies, page 5-40
- Verify Communication Path Between MARS Appliance and Check Point Devices, page 5-41

Add the MARS Appliance as a Host in Check Point

Representing the MARS Appliance in Check Point enables the following supporting tasks:

- Generate a client SIC DN for the MARS Appliance.
- Define policies to allow SIC and syslog traffic between the Check Point components and the MARS Appliance.
- Direct log traffic to the MARS Appliance.

To define the MARS Appliance as a host, follow these steps:

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

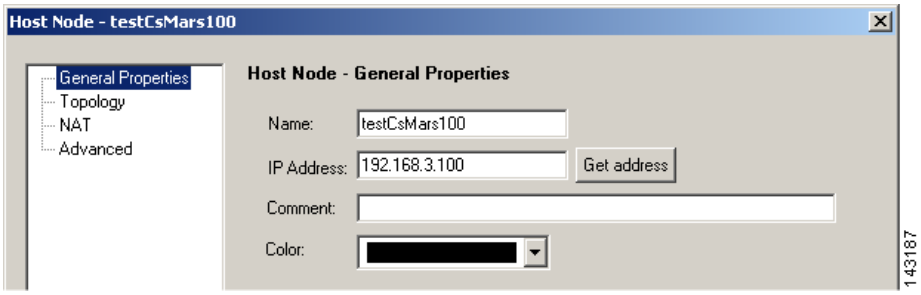
If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.

Step 2 Select **Manage > Network Objects** from the main menu.

Result: The Network Objects dialog box appears.

Step 3 Click the **New** button, and then select **Node > Host** on the menu list.

Result: The Host Node dialog appears, with the General Properties settings selected.



Step 4 Enter the name MARS Appliance in the Name field of the General Properties page

Any Check Point policies defined to enable access or send logs to this appliance will reference the appliance by this name. Cisco best practice recommends using the actual hostname of the MARS Appliance.

Step 5 Enter the IP address of the monitoring interface in the MARS Appliance in the IP Address field

Typically, the monitoring interface is eth0. However, if one or more intermediate gateways are applying NAT rules to the physical IP address, enter the IP address that is exposed to the Check Point central management server.

Step 6 Click **OK** to close the Host Node dialog box.

Step 7 Click **Close** to close the Network Objects dialog box.

Result: The host representing the MARS Appliance is defined. You can now use this host when defining new policies in the Check Point user interface.

Step 8 Continue with Define an OPSEC Application that Represents MARS, page 5-33.

Define an OPSEC Application that Represents MARS

To integrate a third-party OPSEC application with Check Point components, you must define the application and associate it with the host on which the application is running. In addition to identifying this OPSEC application to the Check Point system, this procedure results in the generation of the client SIC DN for the MARS Appliance. Both the client SIC DN and the server SIC DN, obtained in Obtain the Server Entity SIC Name, page 5-36, are required to enable secure communications between the appliance and Check Point components.

This procedure also involves selecting an activation key, or shared secret, that is also required to enable the secure communications. You must record both the activation key and the client SIC DN for use when defining the Check Point devices in the MARS web interface.

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

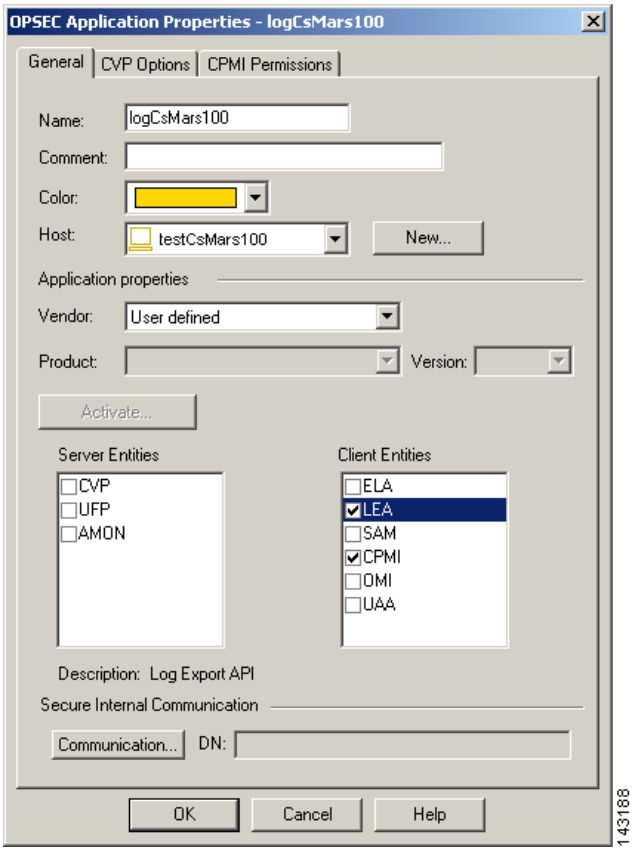
If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.

Step 2 Select **Manage > Servers and OPSEC Applications** from the main menu.

Result: The Servers and OPSEC Application dialog box appears.

Step 3 Click the **New** button, and then click **OPSEC Application** on the menu list.

Result: The OPSEC Application Properties dialog box appears.



Step 4 Specify the name for this object in the Name field.

This value must be different from the name specified in Step 4 of Add the MARS Appliance as a Host in Check Point, page 5-32. Best practice recommends using the actual hostname of the host object plus some other descriptor, which combines for a unique name.

Step 5 In the Host list, select the host that you specified in Step 4 of Add the MARS Appliance as a Host in Check Point, page 5-32.

Step 6 *Result*: This OPSEC application definition is associated with the host that represents the MARS Appliance.

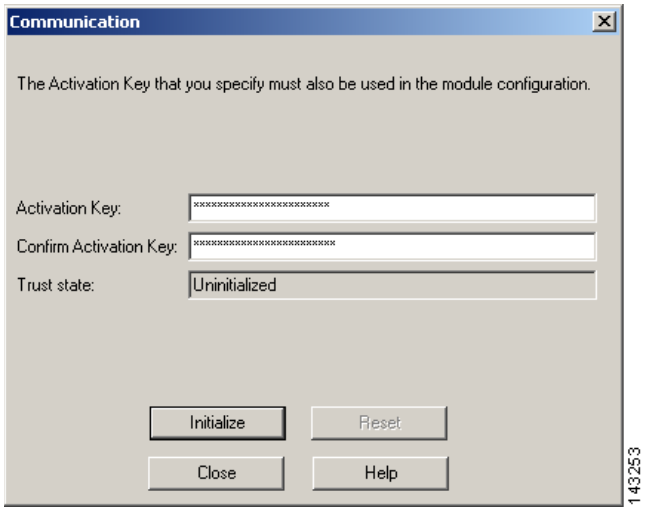
Step 7 Verify that **User defined** is selected in the Vendor field.

Step 8 Select the **LEA** and **CPMI** check boxes under Client Entities.

These values identify the OPSEC services required by the MARS Appliance.

Step 9 Click the **Communication** button under Secure Internal Communication.

Result: The Communication dialog box appears.

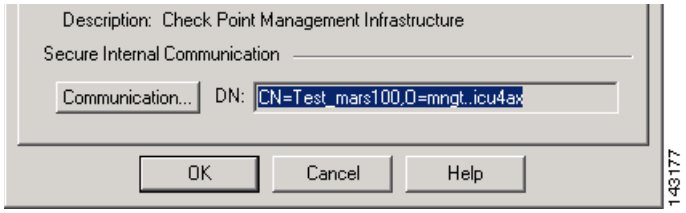


Step 10 Enter the activation key in the Activation Key and Confirm Activation Key fields of the Communication dialog box.

Note Remember this key for future use with MARS.

Step 11 Click **Initialize** to generate the client SIC DN.

Result: The client SIC DN is generated and the Communication dialog box closes, returning to the OPSEC Application Properties dialog box. The new SIC appears in the DN field.



Step 12 Click **Close** to close the Communication dialog box.

Step 13 Record the contents of the DN field that appears under Secure Internal Communication.

This value is used to populate the Client Entity SIC Name field of MARS in Add a Check Point Primary Management Station to MARS, page 5-45.

Tip If possible, you should cut and paste the Secure Internal Communication DN field value into an application, such as Notepad, for later use. Transcribing this field is error prone. Use a mouse to select the contents of read-only field, and then use Ctrl+Insert to copy the field to memory. You can paste the value using Shift+Insert. Be careful to avoid trailing spaces when you paste the value into MARS.

Step 14 Select the **CPMI Permissions** tab and verify that either **Administrator's credentials** or a permissions profile with administrative credentials is selected under Login to SmartCenter with.

Step 15 Click **OK** to close the OPSEC Application Properties dialog box.

Step 16 Click **Close** to close the Servers and OPSEC Application dialog box.

Result: The OPSEC Application that represents MARS is defined and associated to the correct host. You also have obtained the activation key and client SIC DN for later use in Add a Check Point Primary Management Station to MARS, page 5-45.

Step 17 Select **Policy > Install Database** on the main menu.

Result: This operation updates the remote Check Point components (child enforcement modules), such as CMAs, CLMs, log servers, and firewalls. It provides them with the authorization and credentials of the MARS Appliance, as an OPSEC component and SIC client.

Tip Using the Check Point log viewer, you can verify that the OPSEC object was pushed successfully.

Step 18 Continue with Obtain the Server Entity SIC Name, page 5-36.

Obtain the Server Entity SIC Name

The server SIC DN is one of the shared secrets used to provide non-repudiation during a secure communication between a Check Point component and the MARS Appliance. This value is used when defining a primary management station in MARS as defined in Add a Check Point Primary Management Station to MARS, page 5-45.

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX (R60), use the MDG.

Step 2 Select **Manage > Network Objects** on the main menu.

Step 3 Select **Check Points** in the Show list.

Step 4 Select the correct Check Point component in the Network objects list.

Which Check Point component you select depends on which SIC you need and what Check Point system you are using. Specifically, you want to obtain SICs for:

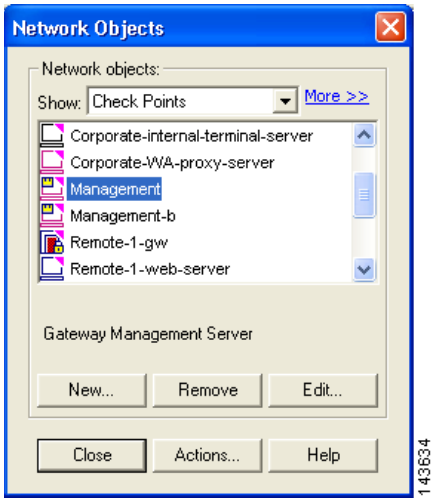
- Each management server to discover configuration settings via CPMI.
- Each management server to which logs are forwarded by remote components.
- Each remote log server that does not forward logs to a central management server, either the MDS or a SmartCenter.

Management servers are the following devices:

- SmartCenter server for standalone SmartCenter and SmartCenter Pro installations.
- Each CMA of a Provider-1 or SiteManager-1 NG FP3 or NG AI (R55) installation.
- The MDS of a Provider-1 or SiteManager-1 NGX (R60) installation.

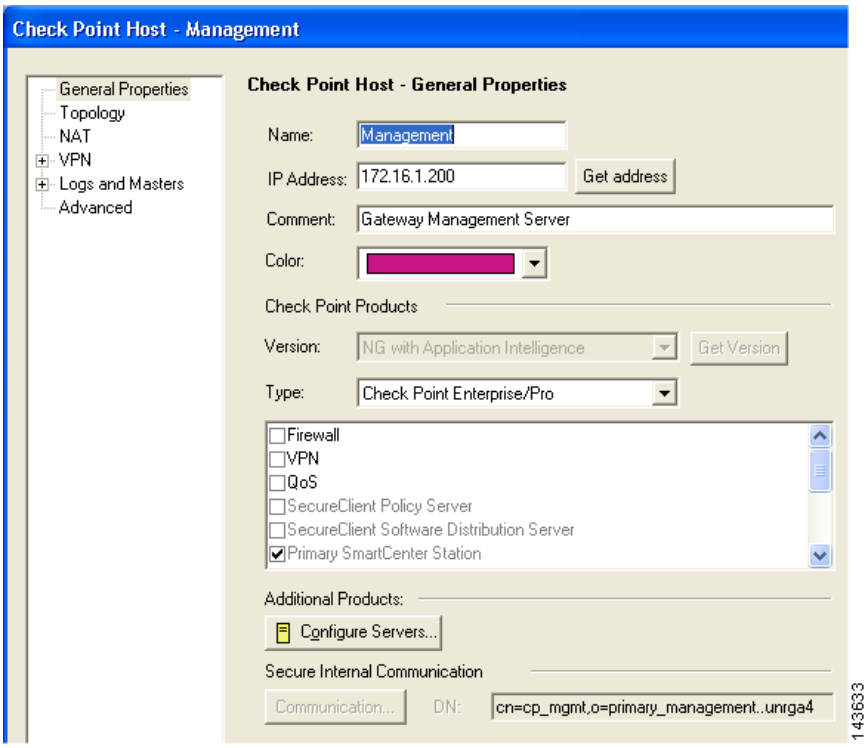
Log servers are the following devices:

- SmartCenter server for standalone SmartCenter and SmartCenter Pro installations.
- Each CLM of a Provider-1 or SiteManager-1 NG FP3 or NG AI (R55) installation.
- The MLM of a Provider-1 or SiteManager-1 NGX (R60) installation.



Step 5 Click **Edit**.

The Check Point Host - Management dialog box appears, with the General Properties page selected.



Step 6 Record the value defined in the DN field under Secure Internal Communication.

This value is used to populate the Server Entity SIC Name field of MARS in either Add a Check Point Primary Management Station to MARS, page 5-45, Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 5-49, or Edit Discovered Firewall on a Check Point Primary Management Station, page 5-55.

Step 7 Click **OK** to close the Check Point Host dialog box.

Step 8 For each additional management or log server in this Check Point installation, select that device in the Network Objects list, and repeat Step 5 through Step 7.

Step 9 Click **Close** to close the Network Objects dialog box.

Step 10 Continue with Select the Access Type for LEA and CPMI Traffic, page 5-38.

Select the Access Type for LEA and CPMI Traffic

Check Point devices use special access types for configuration discovery and event log queries. For configuration discovery, the protocol is CPMI. For event log queries, the protocol is LEA. Each of these protocols has specific configurable attributes, including whether to use bulk encryption, what cipher to use, and what port to use for communications.

You must understand what the supported settings are so that you can verify the Check Point devices are configured correctly. MARS supports only three of the available Check Point authentication mode:

- **CLEAR.** Indicates that the traffic is neither authenticated nor encrypted.
- **SSLCA.** Indicates that the communications need to be authenticated and encrypted using an symmetric key cipher
- **ASYMSSLCA.** Indicates that the communications need to be authenticated and encrypted using an asymmetric key cipher.

These access protocols are configured as follows:

Note Typically, the default values should be used unless your Check Point deployment includes CLMs.

- **<***service***> auth_port <***port_number***>**

  This line is required in the `fwopsec.conf` file. The *service* value is either **LEA_SERVEAR** or **CPMI_SERVER**. Two possible values exist for *port_number*: **0**, which indicates an the server is not listening for authenticated session requests, and the port number of an authenticated and/or encrypted protocol. If the *port_number* value is 0, you must configure the server to listen for session requests in CLEAR mode on a valid port using the **<***service***> port <***port_number***>** settings.

- **<***service***> auth_type <***cipher***>**

  The *service* value is either **LEA_SERVER** or **CPMI_SERVER**. Two possible values are supported for *cipher*: **sslca** for authentication and encryption using a symmetric key cipher, or **asym_sslca** for authentication and encryption using an asymmetric key cipher. If the **auth_port** setting is set to 0 (zero) for this service, then you do not need to specify the auth_type in the `fwopsec.conf` file. You can comment out this line.

- **<***service***> port <***port_number***>**

  This line is required in the `fwopsec.conf` file. The *service* value is either **LEA_SERVER** or **CPMI_SERVER**. The value for *port_number* must match the port number on which the desired network service listens. A *port_number* of **0** (zero) indicates that log server is not listening in CLEAR mode.

  If it is some other number, then any service can come pull the logs without authenticating. For LEA_SERVER, you cannot use port 18184, as it is used for encrypted log communications. For CPMI_SERVER, you cannot use port 18190**.** When CLEAR is enabled, authentication is disabled

for this port. Any host with access to the Check Point component at this port can pull logs. If you chose to enable CLEAR, which is less expensive in terms of overall transaction costs, you define policies that restrict access to the MARS Appliance and other know management hosts.

Note Prior to MARS 4.1 and when using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), you could not use SSLCA mode for log retrieval by the MARS Appliance. Instead, you were required to configure each CMA and CLM to accept LEA session requests using CLEAR mode. It was unnecessary to configure the LEA settings for the MLM.

The following example indicates that LEA is using ASYMSSLCA-based authentication connecting over port 18184 (default), the traffic is encrypted via SSL, and the log server is not listening for requests in cleartext.

```
LEA_SERVER auth_port  18184
LEA_SERVER auth_type  asym_sslca
LEA_SERVER port       0
```

The following example indicates that the log server is listening for requests in cleartext at port 18187. Such requests will be serviced and the sessions will be neither authenticated nor encrypted.

```
LEA_SERVER port       18187
```

Check Point uses the following default settings:

- For LEA, SSLCA is the authentication method and communications occur over TCP 18184.
- For CPMI, SSLCA is the authentication method and communications occur over TCP 18190.

To review or change the access type settings, follow these steps:

Step 1 Log on to the Check Point server.

For Provider-1 and SiteManager-1, this server is the MDS, MLM, or CLM. Otherwise, it is the SmartCenter server.

Step 2 Open the `fwopsec.conf` file found in the subdirectory for each CMA and CLM.

The following example uses the find command to locate the file. Customer1 identifies the CLM.

```
[Expert@logger]# find . -name "fwopsec.conf" -print
./var/opt/CPfw1-R55/conf/fwopsec.conf
./var/opt/CPmds-R55/customers/Cust1Log/CPfw1-R55/conf/fwopsec.conf
[Expert@logger]# cd /var/opt/CPmds-R55/customers/Cust1Log/CPfw1-R55/conf
```

Step 3 Using a text editor, such as vi or Notepad, edit the `fwopsec.conf` file and modify the LEA and CPMI communication settings as needed.

Step 4 Save your changes to the file.

Step 5 Repeat Step 2 through Step 4 for each CLM and CMA.

Step 6 Restart the Check Point server after the changes are made.

Result: The CPMI and LEA servers are restarted, which reloads their configuration information, and ensures they are listening to the correct ports for session requests.

Step 7 Continue with Create and Install Policies, page 5-40.

Create and Install Policies

You must create firewall policies that permit the MARS Appliance to access the relevant ports of the Check Point central management server and any remote log servers. The default ports are as follows:

- **TCP port 18190.** Used by CPMI to discover configuration settings.
- **TCP port 18210.** Used to retrieve the certificate from the Certificate Authority on the SmartCenter, MDS, MLM, CMA, or CLM.
- **TCP port 18184.** Used to pull security event logs from the log servers, such as the MLM or CLM.

However, you must use the CPMI and LEA servers settings specified in Select the Access Type for LEA and CPMI Traffic, page 5-38. When the policies are defined, you must install them on any firewall modules that inspect traffic between the Check Point components and the MARS Appliance.

If the management server has a Check Point firewall installed, follow these steps:

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.

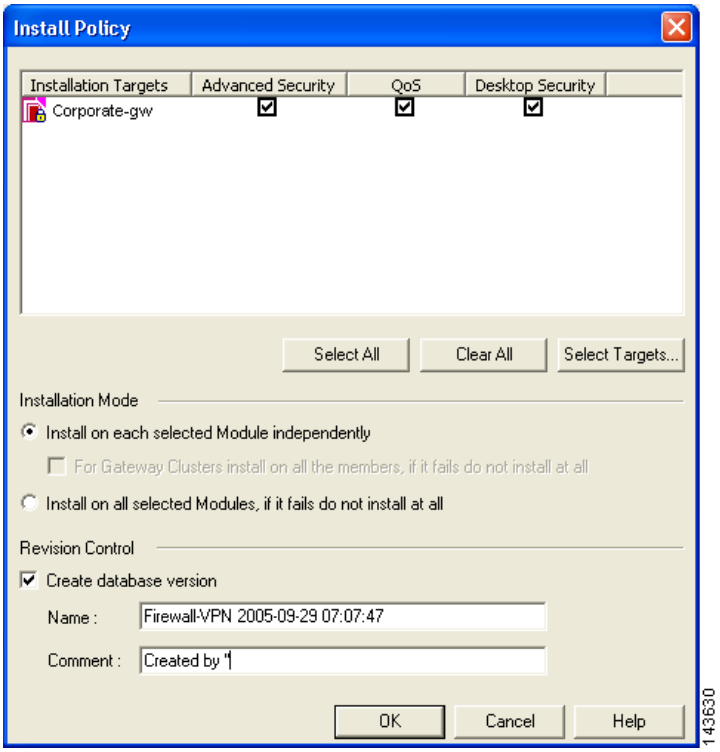
Step 2 If Check Point firewall components reside between the Check Point components (central management and log server) and the MARS Appliance monitoring those components, define the security policies that allow management and log traffic between those devices.

If you have enabled CPMI discovery, the service condition must include CMPI. To enable the log access, the service list must include FW1_lea.

Step 3 Verify that the security policies are set to log.

The Track column of each rule should display the Log action. To enable logging, right-click the Track field of a rule and select **Log** on the shortcut menu.

Step 4 Once you have defined the security policies that enable traffic flows between the Check Point and MARS components, select **Policy > Install** on the main menu.



Step 5 In the Install Policy dialog box, verify the Advanced Security check box is selected for each selected installation target.

The target devices should be those firewalls that reside between the Check Point components and the MARS Appliance.

Step 6 Click **OK** to install the policies on the selected devices.

Result: The security policies on the target firewall devices are updated, enabling CPMI and LEA traffic flows between the Check Point components and the MARS Appliance.

Tip Using the Check Point log viewer, you can verify that the policies were installed successfully.

Verify Communication Path Between MARS Appliance and Check Point Devices

You should verify that the MARS Appliance can reach the Check Point devices, including the SmartCenter server and the remote log servers. Use the telnet command at CLI of the MARS Appliance to verify access to the SmartCenter server and log servers. The ports to check are defined in Select the Access Type for LEA and CPMI Traffic, page 5-38. For more information on accessing the CLI, see Log In to the Appliance via the Console in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

The command syntax is as follows

telnet <*ip_address*> <*port_number*>

If you are unsuccessful, verify the settings of the ports for each Check Point component and verify that no firewalls are blocking the traffic. For more information on **telnet**, see telnet, page A-68 in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

Reset the OPSEC Application Certificate of the MARS Appliance

If you encounter an error when pulling the certificate as part of defining the Check Point devices in the MARS web interface, you must reset the certificate before you can attempt to pull it again. This procedure details how to reset the certificate, or SIC, associated with the OPSEC Application that is associated with the host that represents the MARS Appliance.

To reset the OPSEC application certificate, follow these steps:

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.

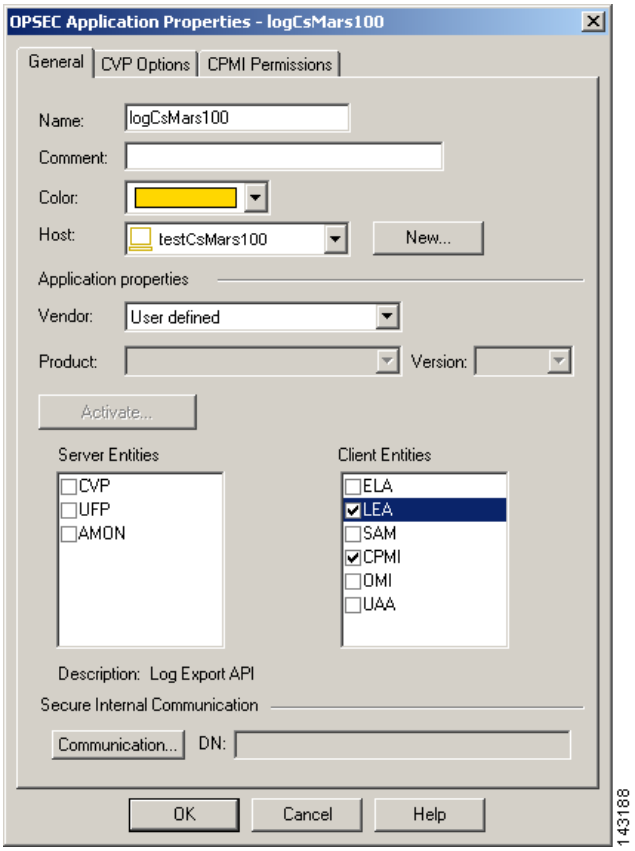
Step 2 Select **Manage > Servers and OPSEC Applications** from the main menu.

Result: The Servers and OPSEC Application dialog box appears.

Step 3 Select **OPSEC Applications** in the Show list.

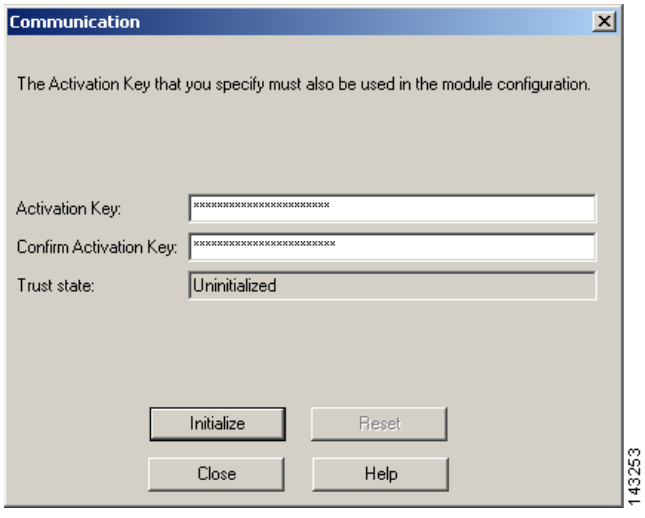
Step 4 Select the OPSEC application that represents the MARS Appliance in the Servers and OPSEC Applications list, and click **Edit**.

Result: The OPSEC Application Properties dialog box appears.



Step 5 Click the **Communication** button under Secure Internal Communication.

Result: The Communication dialog box appears.



Step 6 Click **Reset** to reset the certificate.

Step 7 Click **Close** to close the Communication dialog box.

Result: The client SIC DN is generated and the Communication dialog box closes, returning to the OPSEC Application Properties dialog box. The new SIC appears in the DN field.

Step 8 Click **OK** to close the OPSEC Application Properties dialog box.

Step 9 Click **Close** to close the Servers and OPSEC Application dialog box.

Result: The OPSEC Application that represents MARS is defined and associated to the correct host. You also have obtained the activation key and client SIC DN for later use in Add a Check Point Primary Management Station to MARS, page 5-45.

Add and Configure Check Point Devices in MARS

After you identify and bootstrap the Check Point reporting devices and install the policies that enable the required traffic flows, you must represent those devices in MARS, which uses this information to communicate with the devices. When adding a Check Point device, you add two types of devices:

- **Primary management station.** The primary management station represents the SmartCenter server or CMA that manages other Check Point components. In the web interface, the bases module is defined as a software application (Check Point Management Console application) running on a host.
- **Child enforcement module.** A child enforcement module is a Check Point component, a firewall or log server, that is managed by a primary management station. When viewing the Security and Monitoring Devices list, child enforcement modules appear as children of the hosts that are running the primary management station.

With these definitions in mind, adding and configuring the Check Point device involves the following:

1. Define a host that represents the Check Point primary management station, specifying the hostname and management and reporting IP addresses.
2. Define all of the interfaces of the host.
3. Add the correct Check Point software application to the host. This application represents the primary management station.
4. Specify the communication settings for the primary management station. These settings include identifying which access types are allowed (CPMI, LEA or both) and the authentication type and port to use for each supported access type.
5. (Optional) Define the settings for secure communications. If the access communication are not conducted in CLEAR, then you must specify the client and server SIC DNs and identify the certificate authority.
6. (Optional) Define the routes used by the firewall running on the primary management station. If a firewall is running on the primary management station, the route information is required to enable the path analysis and mitigation features of MARS.
7. Discover the child enforcement modules and the configuration settings of the primary management station. Discovery of child enforcement modules includes any log servers and firewalls managed by the primary management station. MARS discovers configuration settings, such as policies, NAT, modules, and clusters, as well as event information, such as traffic logs, SmartDefense events, and user authentication events.
8. Configure the discovered log servers. To configure these log servers, select the Self option from the Log Info page associated with each server, and specify the access type settings.

9. Define any log servers not managed by the primary management station. These servers are used by one or more of the firewalls that were discovered or by the primary management station.
10. Edit each firewall child enforcement module to select a log server.
11. (Optional) Specify an SNMP RO community string for each firewall child enforcement module for which resource utilization monitoring is desired.
12. (Optional) Define the routes used by each firewall child enforcement module. Route information is required to enable the path analysis and mitigation features of MARS.
13. Click Activate in MARS.

To add a Check Point device in MARS, you must perform the following procedures:

- Add a Check Point Primary Management Station to MARS, page 5-45
- Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 5-49
- Edit Discovered Log Servers on a Check Point Primary Management Station, page 5-53
- Edit Discovered Firewall on a Check Point Primary Management Station, page 5-55
- Verify Connectivity Between MARS and Check Point Devices, page 5-60

If discovery of Check Point configuration settings is not enabled for MARS, you must perform the following manual configuration procedures:

- Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 5-49
- Specify Log Info Settings for a Child Enforcement Module or Log Server, page 5-57

Before You Begin

To perform this procedure, you need the following information:

- A MARS account with Administrative privileges.
- A Check Point CMA or SmartCenter username and password that has READ access (minimum requirement).
- The client and server SIC DNs.
- If you are defining a CMA for Provider-1 or SiteManager-1, you must have the virtual IP address (VIP) for each CMA and CLM managed by the MDS.

Add a Check Point Primary Management Station to MARS

The primary management station represents one of the following:

- The SmartCenter server in a SmartCenter or SmartCenter Pro installation.
- A CMA of a Provider-1 or SiteManager-1 installation.

Note Check Point 4.1, NG FP1, and NG FP2 devices are not officially supported. They cannot be configured to retrieve configuration information using CPMI. However, they can be configured to retrieve logs using LEA. To configure one of these devices to work with the MARS, leave the Access IP field blank on the host that represents the base platform.

You must define each individual CMA of a Provider-1 or SiteManager installation, regardless of the release and version.

Step 1 Select **Admin > System Setup > Security and Monitor Devices > Add**.

Step 2 Do one of the following:

- Select **Add SW Security apps on a new host** from the Device Type list, and continue with Step 3
- Select **Add SW security apps on existing host** from the Device Type list. Select the device to which you want to add the software application and click Add. Continue with Step 7.

Step 3 Specify values for the following fields:

- **Device Name** — Enter the name of the device. This name must exactly match the hostname shown in the Check Point user interface. MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and as the primary management station in the Security and Monitoring Device list.
- **Access IP** — (Optional) This s address is used to pull from a Check Point device using CPMI, enabling MARS to discover settings from this device. This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. To learn more about the access IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.
- **Reporting IP** — Enter the IP address of the interface in the Check Point server from which MARS will pull traffic and audit logs. Check Point audit logs save information regarding user interaction with Check Point devices, such as log in and out of the Check Point user interface, initialize or revoke certificate, install or uninstall policy, create, modify, and delete objects, etc. No additional configuration is needed to turn on audit log on Check Point device.

  This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. To learn more about the reporting IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.

Step 4 Under Enter interface information, enter the interface name, IP address, and netmask value of each interface in the Check Point server from which configuration information will be discovered and from which security event logs will be pulled.

This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. To learn more about the interface settings, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.

Step 5 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

Result: MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 2-42.

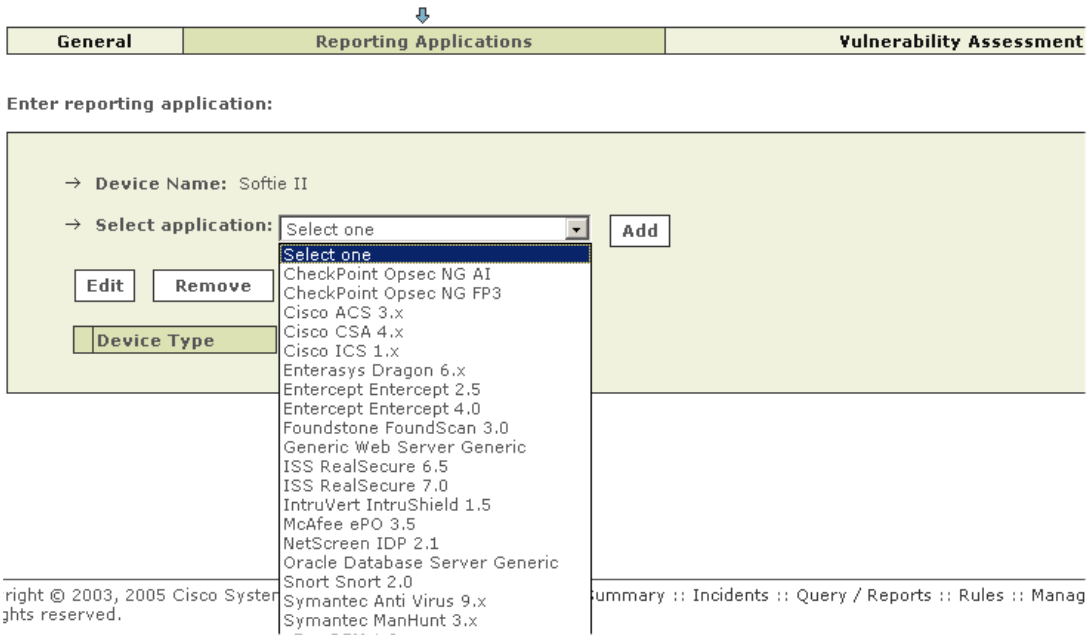
Step 6 Click **Apply** to save these settings.

Step 7 Click **Next** to access the Reporting Applications tab.

Step 8 Select the appropriate version of Check Point Opsec from the Select Application list, and click **Add**.

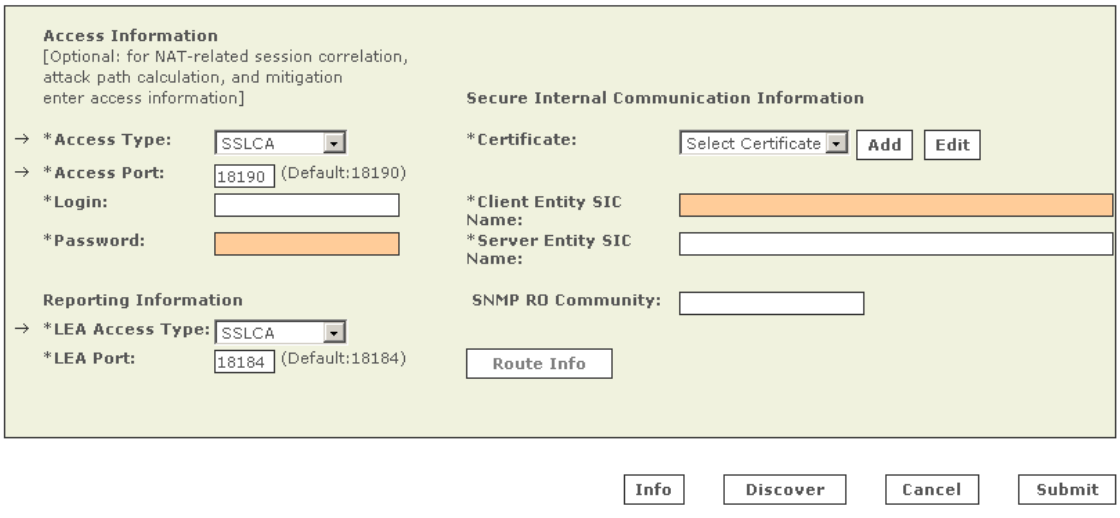
The following options are available:

- **CheckPoint Opsec NG FP3**. Select this option for Check Point NG FP3 devices.
- **CheckPoint Opsec NG AI**. Select this option for Check Point NG AI (R55) and Check Point NGX (R60) devices.



Step 9 If you entered an address in the Access IP field on the host that represents this primary management station, specify values for the following fields:

- **Access Type** — This value identifies the authentication method to use for CPMI traffic, which is the protocol used to discover configuration information. Select **ASYMSSLC**, **CLEAR**, or **SSLCA**. The discovery operation identifies any child enforcement modules managed by this primary management station. It also discovers the NAT and ACL information necessary for NAT-based correlation, attack path calculation, and mitigation analysis. For more information on the access type, see Select the Access Type for LEA and CPMI Traffic, page 5-38.



- **Access Port** — Verify that the port number corresponds to the value specified in the CPMI_SERVER auth_port line of the `fwopsec.conf` file. The default authentication method for configuration discovery is SSLCA and data is passed on port 18190. For more information on this setting, see Select the Access Type for LEA and CPMI Traffic, page 5-38.

- **Login** — Identifies the Check Point administrative account to be used to discover configuration settings.
- **Password** — Identifies the password asscociated with the Login account.

Step 10 Specify values for the following fields:

- **LEA Access Type** — If a log server is running on this primary management station select **ASYMSSLC**, **CLEAR**, or **SSLCA**. You must have entered an address in the Reporting IP field on the host that represents this primary management station. This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. For more information on the access type, see Select the Access Type for LEA and CPMI Traffic, page 5-38.
- **LEA Port** — Verify that the port number corresponds to the value specified in the LEA_SERVER auth_port line of the `fwopsec.conf` file. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184. For more information on this setting, see Select the Access Type for LEA and CPMI Traffic, page 5-38.

Step 11 If this device uses SSLCA or ASYMSSLCA as an authentication method, specify values for the following fields (Otherwise, the authentication method is CLEAR. Skip toStep 12.):

- **Certificate** — Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with Add a Check Point Certificate Server, page 5-52.
- **Client SIC Name** — Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in Define an OPSEC Application that Represents MARS, page 5-33.
- **Server SIC Name** — Enter the SIC DN for this primary management station. This value was obtained in Obtain the Server Entity SIC Name, page 5-36. Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.

Step 12 (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 on host that represents the primary management station and you must configure the Access Information settings on the primary management station. MARS uses the SNMP RO string to perform resource utilization monitoring. Currently, it is not used for configuration or log discovery.

Step 13 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

Before you can enable this feature, you must provide a SNMP RO Community string.

Result: MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 2-42.

Step 14 (Optional) To specify the route information for a firewall running on this primary management station, continue with Define Route Information for Check Point Firewall Modules, page 5-55.

Step 15 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings.

Result: 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 2-40.

Note Sometimes, the discovery operation times out, in which case you should try again. At other times, a message appears that states the discovery is taking a long time and that you should proceed to performing other tasks in MARS.

Step 16 To add this device to the MARS database and continue adding firewall modules manually, click **Submit**.

Result: 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 17 Do one of the following:

- To manually define the child enforcement modules that are managed by this primary management station, continue with Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 5-49.
- To edit the settings of the discovered child enforcement modules, continue with Edit Discovered Firewall on a Check Point Primary Management Station, page 5-55.

Step 18 Click **Activate**.

Result: Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also 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 2-28.

Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station

If you have not enabled configuration discovery on the primary management station or if one or more of the managed firewalls uses a log server that is not managed by the primary management station, you can manually define firewalls or log servers. Your goal should be to represent all of the firewalls managed by this primary management station and all log servers used by those firewalls and the primary management station. While MARS does not discover configuration settings of the firewalls, it uses the defined information to discover topology, calculate attack paths, and identify preferred mitigation points in the network.

For example, if you are defining a primary management station that represents a CMA, you must define the CLM associated with that CMA. Any firewalls managed under that CMA may either act as their own log servers, publish information to the CLM, or publish information to a MLM. In the case of the later, you must define that relationship by defining the firewalls and then specifying which log servers pull their traffic and audit logs. First, however, must also define the MLM settings, as it is a log server that external to the perspective of the CMA, and it cannot be referred by a firewall until it has been defined. The CLM, however, would be considered part of the CMA (assuming the reporting IP and LEA settings are specified), so you would not define a separate child enforcement module to represent it. Instead, you would select the Management option in the Log Info dialog for firewalls that use the CLM as their log server. For more information on selecting the log server option, see Specify Log Info Settings for a Child Enforcement Module or Log Server, page 5-57.

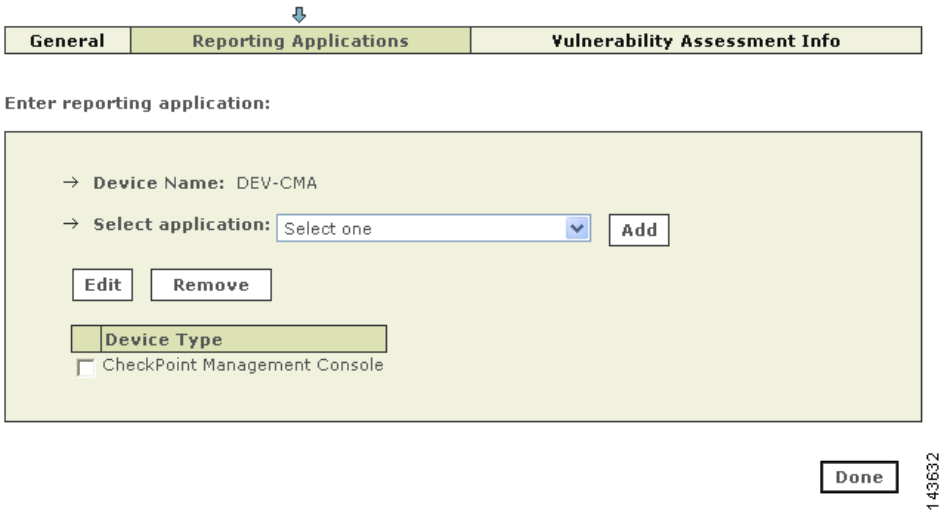
To manually define a child enforcement module that is managed by the primary management station or a log server to which either the primary management station or a child enforcement module publishes its audit and security logs, follow these steps:

Step 1 Select **Admin > System Setup > Security and Monitor Devices**.

Step 2 From the Security and Monitor Devices list, select the host that represents the primary management station and click **Edit**.

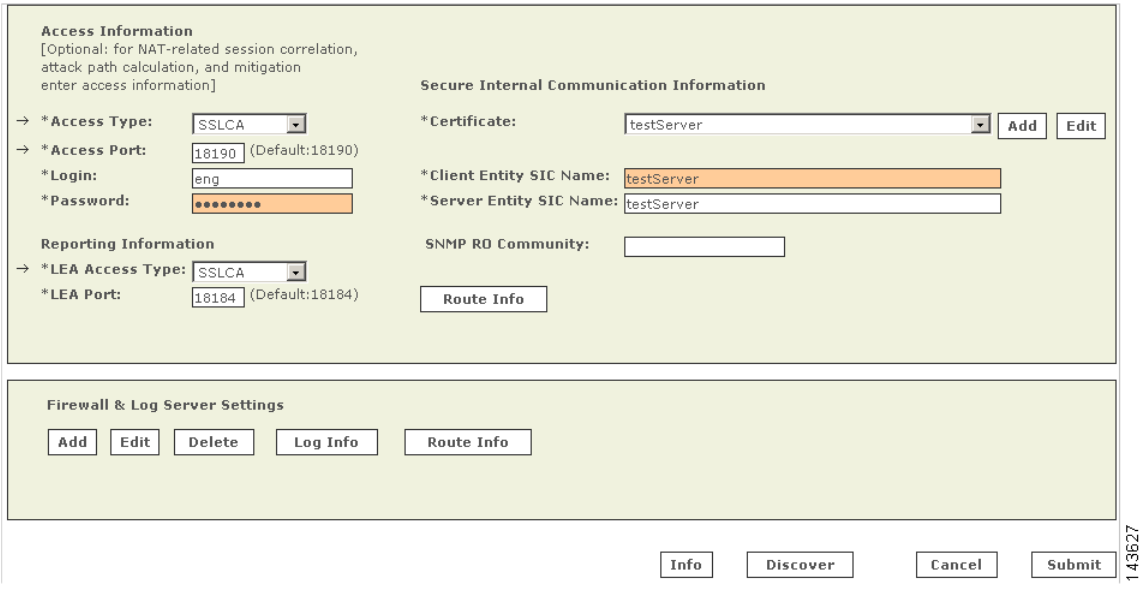
Such devices have CheckPoint Management Console as an entry in the Device Type column.

Step 3 Click **Next** to access the Reporting Applications tab.



Step 4 Select the **CheckPoint Management Console** check box in the Device Type list and click **Edit**.

The Access Information page appears.



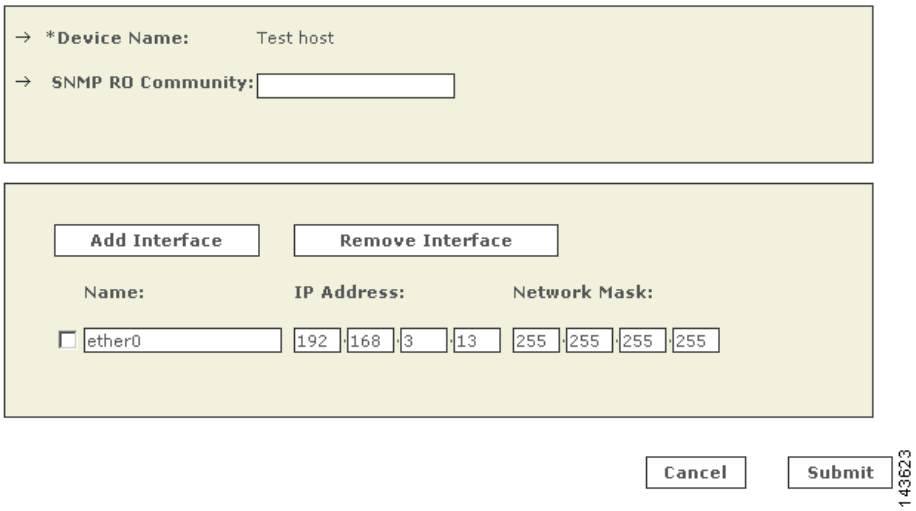
Step 5 Click **Add** under Firewall & Log Server Settings.

Result: The list of available hosts appears.

Step 6 Do one of the following:

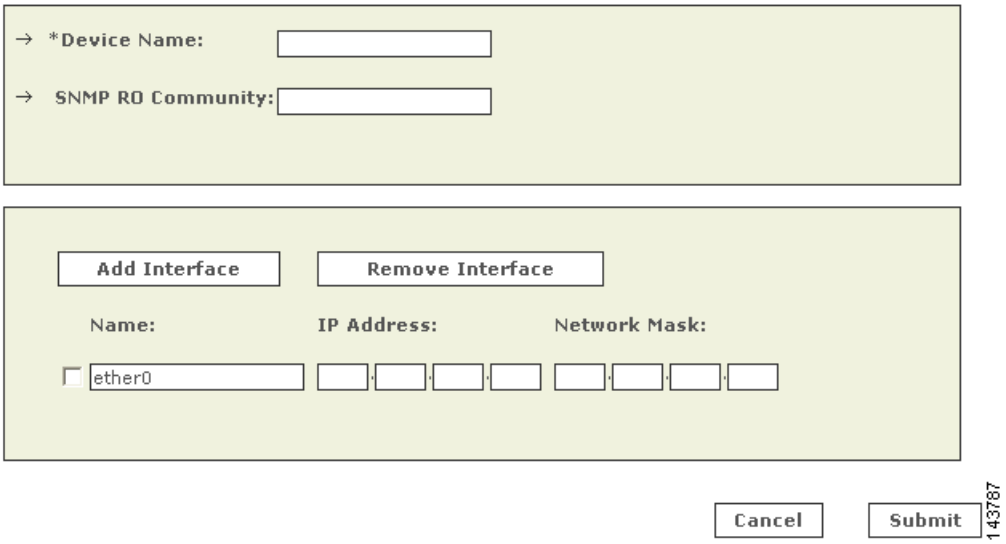
- Select the host on which the child enforcement module is running, click **Change Existing**, and continue with Step 7

  Result: A page with a read-only device name appears, prompting you to specify the SNMP RO Community string.



- Click **Add New** to define a new host, and continue with Step 7

  Result: A page appears, prompting you to specify device name and SNMP RO Community string.



Step 7 Enter the name of the child enforcement module or log server in the Device Name field.

MARS maps this name to the IP address specified in the interfaces. This name is used in topology maps, queries, and appears in the Children column of the base Check Point module in the Security and Monitoring Device list.

Step 8 (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the child enforcement module'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 on host that represents the primary management station. 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 9 Under Enter interface information, enter the interface name, IP address, and netmask value of each interface installed in the child enforcement module or log server.

These interfaces include the ones from which the configuration information will be discovered and security event logs will be pulled. To learn more about the interface settings, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.

Step 10 Click **Submit** to add this module to the primary management station.

Step 11 (Optional) To specify the route information for a firewall child enforcement module, continue with Define Route Information for Check Point Firewall Modules, page 5-55.

Step 12 If the child enforcement module does not propagate its logs to the primary management station or if you are defining a log server that is not managed by this primary management station, you must specify where its logs are stored. Continue with Specify Log Info Settings for a Child Enforcement Module or Log Server, page 5-57.

Step 13 Repeat Step 5 through Step 12 for each child enforcement module that is managed by this primary management station and each log server that is used by the primary management station or child enforcement modules.

Step 14 To add this device to the MARS database, click **Submit**.

Result: 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 15 Click **Done** to close the Reporting Applications tab and return to the Security and Monitoring Devices list.

Step 16 Click **Activate**.

Result: Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also begins to sessionize events generated by this device and its modules 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 2-28.

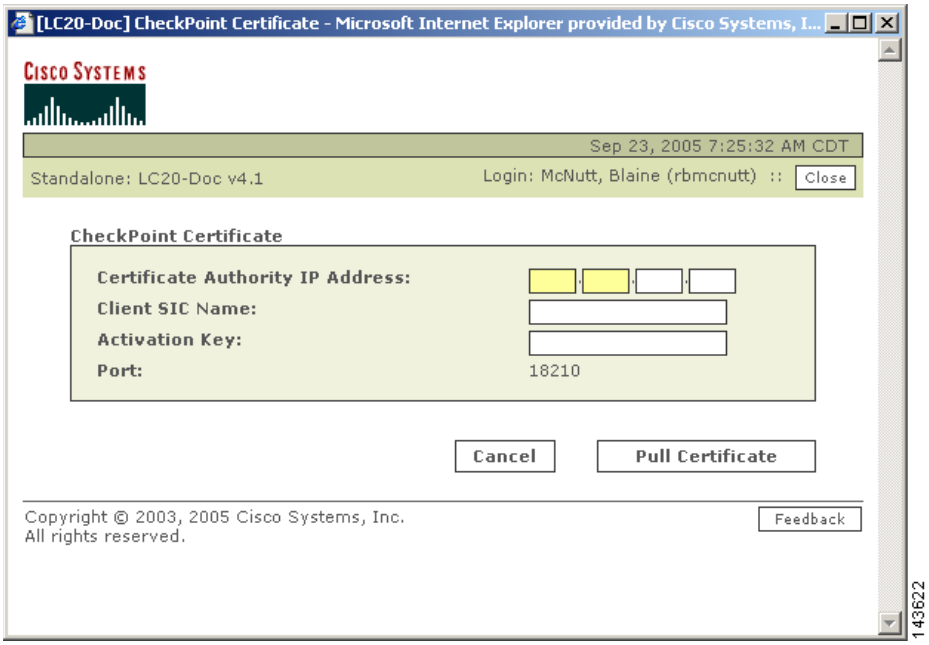
Add a Check Point Certificate Server

When defining a Check Point module that uses secured communications, you must identify the certificate sever that authenticates the SICs provided by the client and the server. Typically, a SmartCenter server or the CMA has its own certificate server, however, your configuration may use a central server. If that is the case, you must define the certificate server as part of a defining a base or child enforcement module.

Note This procedure assumes you have been refer to it, and that you are in the middle of defining a primary management station or child enforcement module.

To define a certificate server, follow these steps:

Step 1 Click **Add** to define the settings for the certificate authority.



Step 2 Specify values for the following fields:

- **Certificate Authority IP Address** — Typically, this IP address is the physical IP address of the SmartCenter server or the virtual IP address of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this IP address represents the physical IP address of the MDS that manages the CMA.
- **Client SIC Name** — Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in Define an OPSEC Application that Represents MARS, page 5-33.
- **Activation Key —** This value was also provided in Define an OPSEC Application that Represents MARS, page 5-33.

Step 3 Click **Pull Certificate**.

Result: A message box appears stating “Discovery is done.”

A certificate can be pulled only once for an OPSEC Application. If for any reason the pull operation fails, you must reset the certificate using the CheckPoint SmartDashboard. For more information, see Reset the OPSEC Application Certificate of the MARS Appliance, page 5-42.

Step 4 Click **Close**.

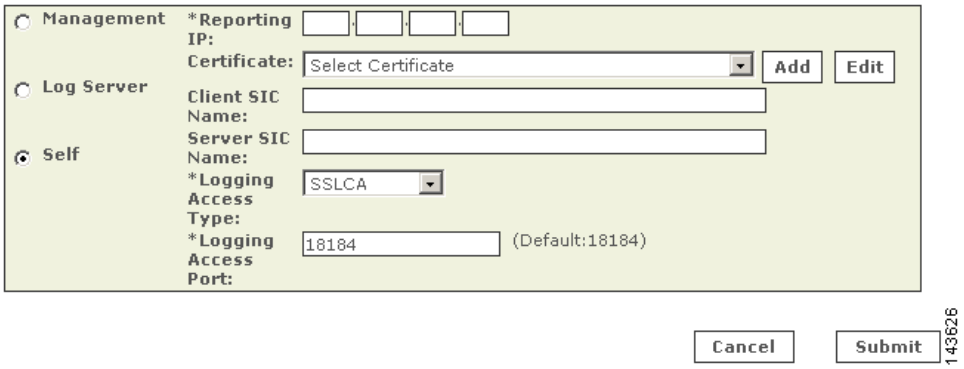
Edit Discovered Log Servers on a Check Point Primary Management Station

After performing a discovery operation, you must edit each discovered log servers. The purpose of editing this log server is to identify that it is its own log server and to provide the SIC communication settings.

To edit a discovered log server, follow these steps:

Step 1 Under Firewall & Log Server Settings, select the check box next to the desired log server, and click **Log Info**.

Step 2 Select **Self**.



Step 3 Specify values for the following fields:

- **Reporting IP** — Enter the IP address of the interface in the log server from which MARS will pull security event logs. This address represents either a virtual IP address associated with a CLM, an MLM, or another log server. To learn more about the reporting IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.
- **Logging Access Type** — This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. Select **ASYMMSSLC**, **CLEAR**, or **SSLCA**, For more information on the access type and port, see Select the Access Type for LEA and CPMI Traffic, page 5-38.
- **Logging Port** — Verify that the port number in the corresponds to the value specified in the LEA_SERVER auth_port line of the `fwopsec.conf` file on this log server. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184.

Step 4 If this log server uses SSLCA or ASYMMSSLCA as an authentication method, specify values for the following fields (Otherwise, the authentication method is CLEAR. Skip to Step 5):

- **Certificate** — Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with Add a Check Point Certificate Server, page 5-52.
- **Client SIC Name** — Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in Define an OPSEC Application that Represents MARS, page 5-33.
- **Server SIC Name** — Enter the SIC DN for the child enforcement module. This value was obtained in Obtain the Server Entity SIC Name, page 5-36. Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.

Step 5 Click **Submit** to save your changes to this log server.

Step 6 Repeat Step 1 through Step 5 for each discovered log server.

Edit Discovered Firewall on a Check Point Primary Management Station

After performing a discovery operation, you must edit any discovered firewalls. You must specify which log server the firewall uses, define the route information, and if you want to monitor resource utilization, you must specify the SNMP RO community string.

Note When editing a Check Point Firewall, never select a Check Point Firewall from the Security and Monitoring Devices list. Instead, select the Check Point Management Console that acts as the primary management station for that firewall.

Note You must configure the discovered log servers and define any log servers not managed by the primary management station before editing the discovered firewalls. To configure the discovered log servers, see Edit Discovered Log Servers on a Check Point Primary Management Station, page 5-53. To manually define log servers, see Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 5-49.

To edit a discovered firewall, follow these steps:

Step 1 Under Firewall & Log Server Settings, select the check box next to the desired firewall.

Step 2 Click **Edit**.

Step 3 (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the child enforcement module'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 on host that represents the primary management station. 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 4 Click **Submit**.

Step 5 To define the route settings for this firewall, continue with Define Route Information for Check Point Firewall Modules, page 5-55.

Step 6 To select the log server used by this firewall, continue with Specify Log Info Settings for a Child Enforcement Module or Log Server, page 5-57.

Step 7 Repeat Step 1 through Step 6 for each discovered firewall.

Define Route Information for Check Point Firewall Modules

To perform attack path analysis and to provide suggested mitigation configurations, MARS must understand the static routes that are defined on a firewall module. This requirement is true for firewalls running on the primary management station as well as for each firewall child enforcement module managed by the primary management station. To provide this information, you must define the routes manually in the MARS web interface. You will need a list of the routes for all interfaces in the firewall before you attempt to enter this information.

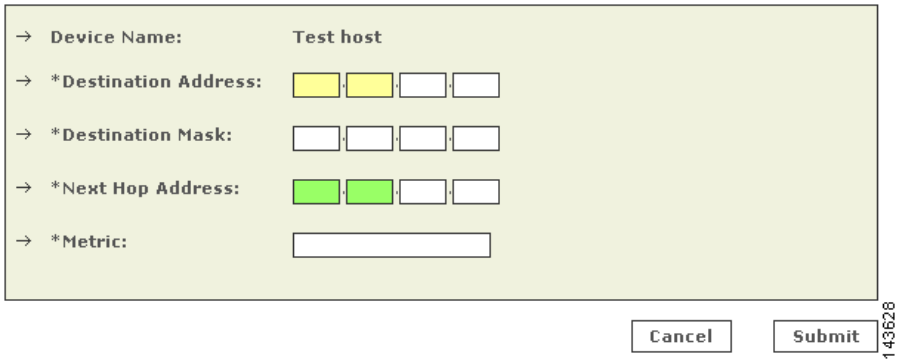
Note You do not need to specify which interface the route is associated with. MARS derives this information based on the interface settings you have specified for the host.

To define the static routes used by a firewall, follow these steps:

Step 1 Do one of the following:

- To specify the route information for the primary management station, click **Route Info** on the primary management station page.
- To specify the route information for a firewall child enforcement module, select the server under Device Type, click **Route Info**.

Result: The Route Information dialog box appears.



Step 2 Specify values for the following fields:

- **Destination Address** — Enter the internal or external destination network address
- **Destination Mask** — Enter the corresponding network mask value.
- **Next Hop Address** — Enter the IP address of the default gateway.
- **Metric** — Identifies the priority for using a specific route. When routing network packets, a gateway device uses the rule with the most specific network within the rule's definition. Only in cases where two routing rules have the same network is the metric used to determine which rule is applied. If they are the same, the lowest metric value takes priority. If no routing rule exists, the network packet is dropped, and if the gateway is not detected (dead), the network packet is dropped.

  A *metric* is a measurement of the cost of a route based on the number of hops (hop count) to the network on which a specific host resides. Hop count refers to the number of networks that a network packet must traverse, including the destination network, before it reaches its final destination. Because the hop count includes the destination network, all directly connected networks have a metric of 1. For the metric value, specify a number between 1 and 15.

Step 3 Click **Submit** to add the route to the list of routes

Step 4 Repeat • through Step 3 for each route defined on the firewall.

Step 5 Click **Close** to return to the Access Information page.

Specify Log Info Settings for a Child Enforcement Module or Log Server

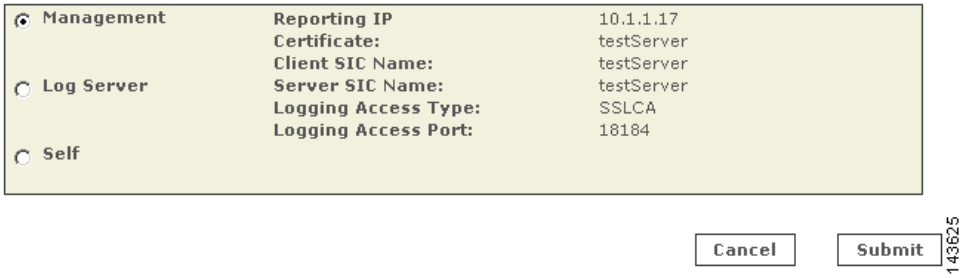
There are two occasions when you must define the log settings manually:

- If you do not discover the settings of the primary management station, which does discover the log settings.
- If the child enforcement module does not propagate its logs up to the primary management station.

Three options exist for manually specifying the log settings:

- **Management.** Identifies that the child enforcement module propagates it logs up to the primary management station, the MLM or the SmartCenter server. You do not specify these settings; they are derived from the settings on the primary management station. However, the option is available if the configuration of a child enforcement module changes. If the primary management station is the log server for a child enforcement module, the log server information is populated when you perform the test connectivity operation.

Figure 5-1 Log Information Published to Primary Management Station



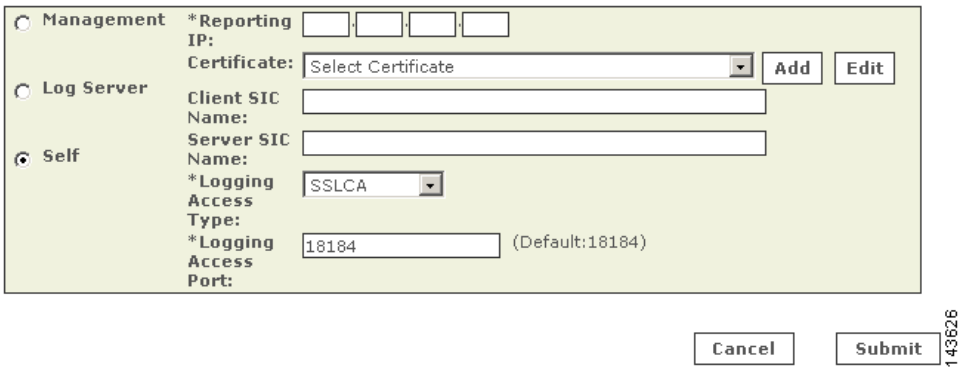
- **Log Server.** Identifies that another log server, such as a CLM, is acting as the log server for this child enforcement module. You must either select a pre-defined log server or define the settings for a new one and select it.
- **Self.** Identifies that the child enforcement module is acting as its own log server. In this case, you must specify the communication settings required to pull the logs from that module or server.

To specify the log server settings of a child enforcement module manually, follow these steps:

Step 1 (Firewall only) If a child enforcement module does not propagate its log information to the primary management station, then select that child enforcement module under Device Type, click **Log Info**, and do one of the following:

- To specify that the child enforcement module is acting as its own log server, select **Self** and continue with Step 3, omitting the Device Name field.

Figure 5-2 Log Information Published to Self



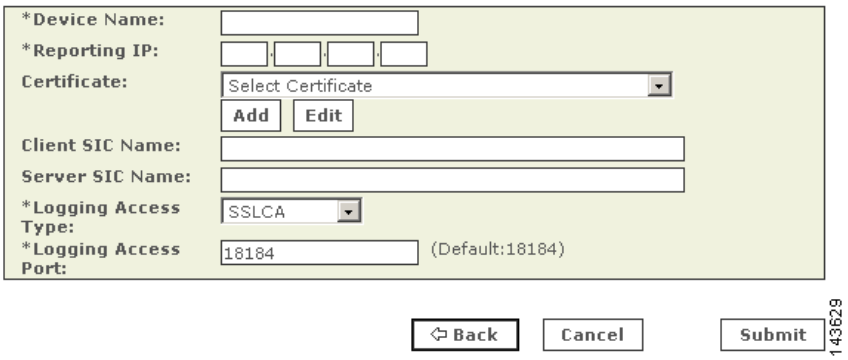
- To specify an alternate log server, select **Log Server**, and continue with Step 2.

Result: The Log Information dialog box appears, and the desired option is selected.

Step 2 Do one of the following:

- Select a predefined log server from the Select list, click **Submit**, and continue with Step 5.

- Click **Add** to define a new log server.



Step 3 Specify values for the following fields:

- **Device Name** — Enter the name of the log server. MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and as the primary management station 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.

- **Reporting IP** —Enter the IP address of the interface in the log server from which MARS will pull security event logs. This address represents either a virtual IP address associated with a CLM, an MLM, or another log server. To learn more about the reporting IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.
- **Logging Access Type** — This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. Select **ASYMSSLC**, **CLEAR**, or **SSLCA**, For more information on the access type, see Select the Access Type for LEA and CPMI Traffic, page 5-38.
- **Logging Port** — Verify that the port number in the corresponds to the value specified in the LEA_SERVER auth_port line of the `fwopsec.conf` file on this log server. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184. For more information on this setting, see Select the Access Type for LEA and CPMI Traffic, page 5-38.

Step 4 If this log server uses SSLCA or ASYMSSLCA as an authentication method specify values for the following fields (Otherwise, CLEAR is the authentication method for Access Type and LEA Access Type, and you should skip to Step 5):

- **Certificate** — Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with Add a Check Point Certificate Server, page 5-52.
- **Client SIC Name** — Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in Define an OPSEC Application that Represents MARS, page 5-33.
- **Server SIC Name** — Enter the SIC DN for the child enforcement module. This value was obtained in Obtain the Server Entity SIC Name, page 5-36. Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.

Step 5 To add this child enforcement module to the primary management station, click **Submit**.

Step 6 To add the primary management station to the MARS database, click **Submit**.

Result: 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 7 Click **Done** to close the Reporting Applications tab and return to the Security and Monitoring Devices list.

Step 8 Click **Activate**.

Result: Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also begins to sessionize events generated by this device and its modules 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 2-28.

Verify Connectivity Between MARS and Check Point Devices

After defining the Check Point device and clicking Activate in the MARS web interface, the MARS Appliance connects to the log servers and pulls the traffic and audit logs stored on them. You can verify that these transactions are successful using the following method:

- Perform an ad hoc query for Event Types/Sessions specify to the Check Point primary management station.

  Result: The netstat command should display two connections per log server.

Remove a Firewall or Log Server from a Check Point Primary Management Station

If the configuration of your network changes so that a firewall or log server is no longer managed by the primary management station under which it is defined, you must remove the child enforcement module.

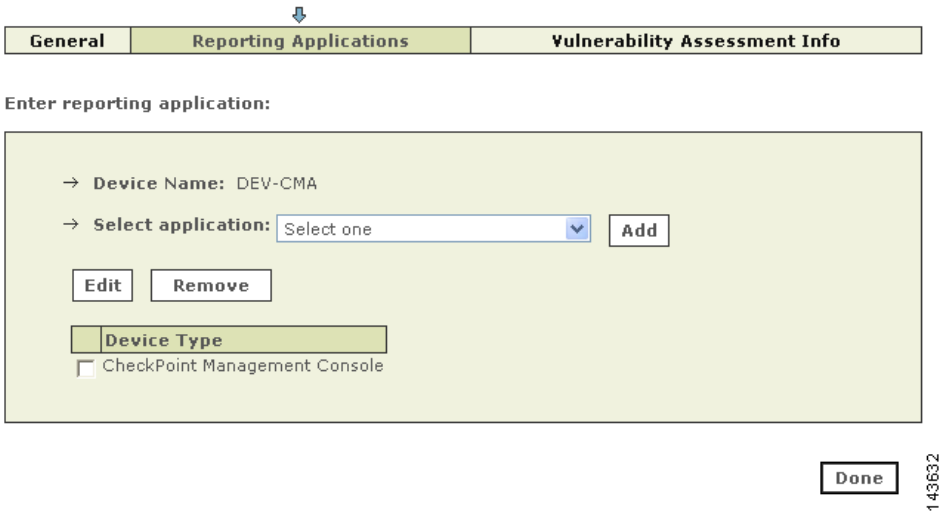
To remove a child enforcement module from the primary management station, follow these steps:

Step 1 Select **Admin > System Setup > Security and Monitor Devices**.

Step 2 From the Security and Monitor Devices list, select the host that represents the primary management station of the Check Point server and click **Edit**.

Such devices have CheckPoint Management Console as an entry in the Device Type column.

Step 3 Click **Next** to access the Reporting Applications tab.



Step 4 Select CheckPoint Management Console from the Device Type list and click **Edit**.

The Access Information page appears.

Step 5 Under Firewall & Log Server Settings, check the box next to the child enforcement module that you want to remove.

Step 6 Click **Remove**.

Result: The Confirmation screen appears.

Step 7 Click **Submit** to remove the child enforcement module from the primary management station.

Troubleshooting MARS and Check Point

The following information can be used to troubleshoot communicate issues between the MARS Appliance and Check Point components.

- To view attack information by user, run a query where the device is a Check Point device.
- If you attempt to discover the certificate and it returns to the CheckPoint Certificate screen instead of displaying the "Discovery done." message box, then the discover operation failed. The likely cause is an incorrect SIC value.

Note A certificate can be pulled only once for an OPSEC Application. If for any reason the pull operation fails, you must reset the certificate using the CheckPoint SmartDashboard. For more information, see Reset the OPSEC Application Certificate of the MARS Appliance, page 5-42.

- If the device discovery operation fails, click the **View Error** button for a detailed error message.

Common reasons for failure of device discovery are as follows:

- client SIC DN name or server SIC DN name is incorrect. Use copy and paste from SmartDashboard to avoid erroneous entry.
- Invalid Certificate used.
- Invalid user name, password, or both used. Verify that the credentials provided for the Access IP match an Check Point account with administrative privileges.
- Unsupported version of Check Point. (Discovery works only with NG FP3 and above. Internally we have tested up to Version R60)
- Invalid authentication method used. The default method is SSLCA. Check the `fwopsec.conf` file to determine which method is used. CS-MARS currently support only three authentication methods for CPMI communication: SSLCA, ASYM_SSLCA and CLEAR. For more information on specifying these settings, see Select the Access Type for LEA and CPMI Traffic, page 5-38.
- Invalid access port. Default port for secured CPMI-based communication is TCP 18180. Check the `fwopsec.conf` to verify the configured port.
- The MARS Appliance does not have access to port 18190, or an alternate specified in `fwopsec.conf` for CPMI. At the CLI of the MARS Appliance, use the **telnet** command to test the access port. For more information on **telnet**, see Verify Communication Path Between MARS Appliance and Check Point Devices, page 5-41.
- The policy database was not installed after creating OPSEC Application in the SmartDashboard.
- Firewall policies were not created and installed that permitted the MARS Appliance to connect to the Check Point primary management station. For information, see Create and Install Policies, page 5-40.

For additional Check Point discovery-related debug information, use the **pnlog** command at the CLI of the MARS Appliance. You can use the cpdebug attribute to specify appropriate debug level. Level 9 presents all debug messages. You can view the debug messages using the **pnlog showlog cpdebug** command at the CLI. For more information on **pnlog**, see pnlog, page A-36 in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.