Monitoring the Security Appliance

This chapter describes how to monitor the security appliance, and includes the following sections:

Using System Log Messages

The security appliance provides extensive system log messages. See the *Cisco Security Appliance Logging Configuration and System Log Messages* to configure logging and to view system log message descriptions.

Using SNMP

This section describes how to use SNMP and includes the following topics:

SNMP Overview

The security appliance provides support for network monitoring using SNMP V1 and V2c. The security appliance supports traps and SNMP read access, but does not support SNMP write access.

You can configure the security appliance to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the MIBs on the security appliance. MIBs are a collection of definitions, and the security appliance maintains a database of values for each definition. Browsing a MIB entails issuing an SNMP get request from the NMS. Use CiscoWorks for Windows or any other SNMP V1, MIB-II compliant browser to receive SNMP traps and browse a MIB.

Table 35-1 lists supported MIBs and traps for the security appliance and, in multiple mode, for each context. You can download Cisco MIBs from the following website.

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

After you download the MIBs, compile them for your NMS.

Table 35-1 SNMP MIB and Trap Support

MIB or Trap Support	Description
SNMP core traps	The security appliance sends the following core SNMP traps: • authentication—An SNMP request fails because the NMS did not authenticate with the correct community string. • linkup—An interface has transitioned to the "up" state. • linkdown—An interface is down, for example, if you removed the **nameif** command. • coldstart—The security appliance is running after a reload.
MIB-II	The security appliance supports browsing of the following groups and tables: • system
IF-MIB	The security appliance supports browsing of the following tables: • ifTable • ifXTable
RFC1213-MIB	The security appliance supports browsing of the following table: • ip.ipAddrTable
SNMPv2-MIB	The security appliance supports browsing the following: • snmp
ENTITY-MIB	The security appliance supports browsing of the following groups and tables: • entPhysicalTable • entLogicalTable The security appliance supports browsing of the following traps: • snmp-server enable traps entity {config-change|fru-insert|fru-remove}
CISCO-IPSEC-FLOW-MONITOR-MIB	The security appliance supports browsing of the MIB. The security appliance supports browsing of the following traps: • snmp-server enable traps ipsec {start|stop}
CISCO-REMOTE-ACCESS-MONITOR-MIB	The security appliance supports browsing of the MIB. The security appliance supports browsing of the following traps: • snmp-server enable traps remote-access {session-threshold-exceeded}
CISCO-CRYPTO-ACCELERATOR-MIB	The security appliance supports browsing of the MIB.
ALTIGA-GLOBAL-REG	The security appliance supports browsing of the MIB.
Cisco Firewall MIB	The security appliance supports browsing of the following groups: • cfwSystem The information is cfwSystem.cfwStatus, which relates to failover status, pertains to the entire device and not just a single context.

Table 35-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
Cisco Memory Pool MIB	The security appliance supports browsing of the following table: • ciscoMemoryPoolTable—The memory usage described in this table applies only to the security appliance general-purpose processor, and not to the network processors.
Cisco Process MIB	The security appliance supports browsing of the following table: • cpmCPUTotalTable
Cisco Syslog MIB	The security appliance supports the following trap: • clogMessageGenerated You cannot browse this MIB.

Enabling SNMP

The SNMP agent that runs on the security appliance performs two functions:

- Replies to SNMP requests from NMSs.
- Sends traps (event notifications) to NMSs.

To enable the SNMP agent and identify an NMS that can connect to the security appliance, follow these steps:

Step 1 To identify the IP address of the NMS that can connect to the security appliance, enter the following command:

```
hostname(config)# snmp-server host interface_name ip_address [trap | poll] [community
text] [version 1 | 2c] [udp-port port]
```

Specify **trap** or **poll** if you want to limit the NMS to receiving traps only or browsing (polling) only. By default, the NMS can use both functions.

SNMP traps are sent on UDP port 162 by default. You can change the port number using the **udp-port** keyword.

Step 2 To specify the community string, enter the following command:

```
hostname(config)# snmp-server community key
```

The SNMP community string is a shared secret between the security appliance and the NMS. The key is a case-sensitive value up to 32 characters in length. Spaces are not permitted.

Step 3 (Optional) To set the SNMP server location or contact information, enter the following command:

```
hostname(config)# snmp-server {contact | location} text
```

Step 4 To enable the security appliance to send traps to the NMS, enter the following command:

```
hostname(config)# snmp-server enable [traps [all | feature [trap1] [trap2]] [...]]
```

By default, SNMP core traps are enabled (**snmp**). If you do not enter a trap type in the command, **syslog** is the default. To enable or disable all traps, enter the **all** option. For **snmp**, you can identify each trap type separately. See Table 35-1 on page 35-2 for a list of traps.

Step 5 To enable system messages to be sent as traps to the NMS, enter the following command:

```
hostname(config)# logging history level
```

You must also enable **syslog** traps using the preceding **snmp-server enable traps** command.

Step 6 To enable logging, so system messages are generated and can then be sent to an NMS, enter the following command:

```
hostname(config)# logging on
```

The following example sets the security appliance to receive requests from host 192.168.3.2 on the inside interface.

```
hostname(config)# snmp-server host 192.168.3.2
hostname(config)# snmp-server location building 42
hostname(config)# snmp-server contact Pat lee
hostname(config)# snmp-server community ohwhatakeyisthee
```