

Installing the PIX Firewall Syslog Server

If you have PIX Firewall version 4.3 or later, the PIX Firewall Syslog Server (PFSS) lets you view PIX Firewall event information from a Windows NT system and includes special features not found on other syslog servers such as:

- Receiving syslog messages via either TCP or UDP
- Full reliability because messages can be sent via TCP

PFSS can receive syslog messages from up to 10 PIX Firewall units.

This chapter includes the following sections:

- Important PFSS Notes
- Installing PFSS
- Changing PFSS Options

Important PFSS Notes

Review the following notes before installing PFSS:

- 1 You must have access to Cisco Connection Online (CCO) to obtain a copy of the PFSS file.
- 2 If a PIX Firewall is set to send messages via TCP and if the Windows NT partition containing the log files becomes full, PFSS causes the PIX Firewall to stop all connections until the Windows NT disk space is freed.
- 3 When you install PFSS on the Windows NT system, write down the values you supply. Once PFSS is installed, the only way you can view the timer durations is by examining the Windows NT registry with regedit and searching for **disk_empty_watch**. Also, if you need to view the information in the registry, do not change it in the registry. The information can only be changed from the **Start>Settings>Control Panel>Services** item.

Once PFSS is installed and running, you can view the pfss.log file to see the settings for the percentage of disk full, and the TCP and UDP ports. The pfss.log file can be found in the same directory in which you locate the log files. (During installation you are prompted for the directory in which to install the log files.)

- 4 Only install PFSS on a Windows NT system version 4.0 system with Service Pack 3 installed. Install PFSS in the NTFS (not the FAT32) partition on your hard disk.
- 5 You can install PFSS from either a user or the Administrator login.
- 6 PFSS log files must reside on the local Windows NT system (not accessed across the network).

- 7 The PIX Firewall Manager (PFM) and PFSS cannot be used together even if installed on different systems. The PFSS or PFM installation script detects the presence of the other program on the same system and advises you to deinstall the other program.
- 8 PFSS creates seven rotating syslog files named monday.log, tuesday.log, wednesday.log, thursday.log, friday.log, saturday.log, and sunday.log. If a week has passed since the last log file was created, it will rename the old log file to *day.mmddyy* where *day* is the current day, *mm* is the month, *dd* is the day, and *yy* is the year. The size of a log file depends on how many connections can occur on each PIX Firewall and the types of messages you permit to be logged. Refer to the *System Log Messages for the PIX Firewall Version 5.0*.

Installing PFSS

To install the PFSS:

- Step 1** Obtain the PFSS installation program from Cisco Connection Online (CCO):
 - (a) Use a network browser, such as Netscape Navigator to access **<http://www.cisco.com>**.
 - (b) If you are a registered CCO user, click **LOGIN** in the upper area of the page. If you have not registered, click **REGISTER** and follow the steps to register.
 - (c) After you click **LOGIN**, a dialog box appears requesting your username and password. Enter these and click **OK**.
 - (d) When you are ready to continue, choose **Software Center** under the **Service & Support** heading.
 - (e) On the Service & Support page, click **Internet Products** from the center column.
 - (f) On the Internet Products page, click **PIX Firewall Software**.
 - (g) On the PIX Firewall Software page, click **Download PIX Firewall Software**.
 - (h) On the Software Center page, choose the software you need. If you are downloading software for the first time and you use a Windows or MS-DOS system, choose the executable file (pfss43n.exe). This file is a self-extracting archive.
 - (i) On the Software Download page, choose how you want to download the software.
 - (j) You will be again prompted for your CCO login password. Enter it and click **OK**.
 - (k) The software then downloads to your system.
- Step 2** If you have not done so already, open the window of the folder containing the downloaded file. Start the installation by double-clicking the downloaded file.
- Step 3** You will be prompted for the following:
 - (a) To start the installation—click **Yes**.
 - (b) To acknowledge the installation Welcome window—click **Next**.
 - (c) Destination target and folder—either accept the default settings or click **Browse** to specify an alternative. You can specify different partitions for the log files that the server creates and the server itself. First you are prompted for where to store the program and then where to put the log files. Make sure that the log files are on the local disk and not a networked disk.

- (d) Port numbers for the TCP syslog server and the UDP syslog server—either accept the defaults of TCP port 1468 and UDP port 514 or specify ports as required by your system. If you enter a port number, it must be between 1024 and 65535.
- (e) Percentage of Disk Full—accept the default value of 90% or specify a new value. This integer value between 1 and 100 is the maximum size that the file system can achieve before the Windows NT system signals the PIX Firewall to stop its connections.
- (f) Disk Empty Watch—specify the duration in seconds that the syslog server waits between checks to see if the disk is still empty. The default is 5 seconds.
- (g) Disk Full Watch—specify the duration in seconds that the syslog server waits between checks to see if the disk is still full. The default is 3 seconds.

Refer to the **logging** command page in the configuration guide for your respective software version listed in the section, “Related Documentation” in “About This Manual.” This command page provides additional important information about configuring the PIX Firewall for use with PFSS.

The PFSS starts immediately after installation. This service can be controlled via the Services Control Panel, which you can use to pause the service, then resume the service, stop, or start the service. The service can also be started with different startup parameters from the Services window.

Changing PFSS Options

After you complete the installation, you can change the option values as follows:

- Step 1** On the **Start>Settings>Control Panel>Services** menu, click the **PIX Firewall Syslog Server** entry. You can add commands to the **Startup Parameters** edit box. After you enter a command, click **Start**. If you press the **Enter** key, the menu closes without information being accepted.
- Step 2** Change the values by entering one of these commands:
- **-a %_disk_full**—The maximum percentage of how full the disk is that you allow the Windows NT system to reach before causing the PIX Firewall to stop transmissions. This is an integer value in the range of 1 to 100. The default is 90.
 - **-t tcp_port**—the port used by the Windows NT system to listen for TCP syslog messages, the default is 1468. If you specify another port, it must be in the range of 1024 to 65535.
 - **-u udp_port**—the port used by the Windows NT system to listen for UDP syslog messages, the default is 514. If you specify another port, it must be in the range of 1024 to 65535.
 - **-e disk_empty_watch_timer**—the duration in seconds that PFSS waits between checks to see if the disk partition is still empty. The default is 5 seconds, the range is any number greater than zero.
 - **-f disk_full_watch_timer**—the duration in seconds that PFSS waits between checks to see if the disk partition is still full. The default is 3 seconds, the range is any number greater than zero.
- Step 3** Refer to the **logging** command page in the configuration guide for a description for how to configure the PIX Firewall to work with the PFSS. You can view this document online for your respective software version in the section, “Related Documentation” in “About This Manual.”

