

Setting Up PIX Syslog

Document ID: 15248

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

How Syslog Works

- Logging Facility
- Levels

Configure the PIX to Send Syslog

- PIX 4.0.x–4.1.x
- PIX 4.2.x and Later
- PIX 4.3.x and Later

How to Set Up a Syslogd Server

Debugging Syslog

Information to Collect if You Open a TAC Case

Related Information

Introduction

Note: This document is only related to PIX 4.x. Refer to these documents for information on software versions 5.x, 6.x, and 7.x:

- PIX/ASA 7.x with Syslog Configuration Example
- Cisco Security Appliance System Log Messages, Version 7.x
- Cisco PIX Firewall System Log Messages, Version 6.x
- Cisco PIX Firewall System Log Messages Version , Version 5.x

Messages produced by the PIX that usually go to the console can be collected when you send these messages to a device that runs a syslogd daemon (syslogd). Syslogd listens on UDP port 514, the syslog port. Syslogging enables you to gain information about PIX traffic and performance, analyze logs for suspicious activity, and troubleshoot problems.

Syslogd can run on a number of operating system platforms. Syslogd is installed when you install UNIX, but you have to configure it. Syslogd usually is not native to Windows-based systems, but syslogd software is available for Windows NT. Examples include PIX Firewall Manager (PFM), PIX Firewall Syslog Server (PFSS), Private-I, or other syslog software of your choice.

Note: If there is any other application in the network that uses port number 514, syslog messages might not reach the syslog server successfully.

This document describes how syslog works, how to set up the PIX to send syslog messages to a device that runs syslogd, and how to set up a UNIX-based syslogd server.

Actual meanings of PIX syslog messages are in the PIX documentation.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on Cisco Secure PIX Software Releases 4.0.x and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

How Syslog Works

All syslog messages have a logging facility and a level. The logging facility can be thought of as where and the level can be thought of as what.

Logging Facility

The single syslog daemon (syslogd) can be thought of as having multiple pipes. It uses the pipes to decide where to send incoming information based on the pipe on which the information arrives. In this analogy, the logging facilities are the pipes by which the syslogd decides where to send information it receives.

The eight logging facilities commonly used for syslog are local0 through local7.

```
local0
local1
local2
local3
local4
local5
local6
local7
```

Levels

There are also different degrees of importance attached to incoming messages. You can think of the levels as what. The PIX can be set to send messages at different levels (these are listed from highest to lowest importance):

Level	Numeric Code
emergency	0
alert	1
critical	2
error	3

warning	4
notification	5
informational	6
debug	7

When a PIX is set up to send syslog messages, levels of lower importance include levels of higher importance. For example, if the PIX is set for warning, then error, critical, alert, and emergency messages are also sent in addition to warning. A debug setting includes messages at all eight levels.

Configure the PIX to Send Syslog

PIX 4.0.x–4.1.x

The syslog syntax is:

syslog host #.#.#.# (where #.#.#.# is the syslog servers address)

syslog output X.Y (where X is the logging facility and Y is the level)

How does the X number translate to logging facility?

Break down the X number into binary. The last four bits comprise the local facility.

- 16 = 00010000 = local0
- 17 = 00010001 = local1
- 18 = 00010010 = local2
- 19 = 00010011 = local3
- 20 = 00010100 = local4
- 21 = 00010101 = local5
- 22 = 00010110 = local6
- 23 = 00010111 = local7

As an example, since 22 = 00010110, and the last four bits=0110=decimal 6, this is local6. (A shortcut is to take the X value and subtract 16. For example, 22–16=6, or local6.)

The Y number is the level. As an example, if Y=2, messages sent would include those at level 2 (critical), level 1 (alert), and level 0 (emergency). The PIX levels are 0–7; these should not be confused with the logging facilities (which are local0–local7).

Examples in PIX 4.0.x–4.1.x

- **syslog 20.7**

20 equals local4 logging facility.

.7 is the level. 7 means debug to the PIX (all messages are logged).

- **syslog 23.2**

23 equals local7 logging facility

.2 is the level. 2 means critical to the PIX (critical, alert, and emergency messages are logged).

PIX 4.2.x and Later

The syntax for syslog changed in PIX Software releases 4.2.x. Instead of the **syslog host #.#.#.#** command, use the new **logging host #.#.#.#** command. In 4.2.x, the logging facility and level definitions are the same, but instead of using the syslog output X.Y command, you need to have these two statements:

- **logging facility X**
- **logging trap Y**

The level is no longer expressed as a number. It is expressed as the name of the level. This is an example:

- *old syntax*

syslog output 20.7

- *new syntax*

logging facility 20 (*local4*)

logging trap debugging (*debugging through emergency*)

PIX 4.3.x and Later

In 4.3.x and later, you can avoid having particular syslog messages sent, and you can timestamp messages that are sent.

In addition to these commands:

- **logging host #.#.#.#**
- **logging facility X**
- **logging trap Y**

You can issue these commands:

- **clock set 13:18:00 Apr 25 1999**
- **logging timestamp**
- **no logging message 111005**

This results in having all messages, except message 111005 (that is, "End configuration"), sent with timestamps.

Note: Because the 111005 message is a Notification level message, it is not seen if the level on the PIX is set for Emergency, Alert, Critical, Error, or Warning.

This is an example of a time-stamped non-111005 message. (The first timestamp is from our UNIX server and the second is from the PIX.)

```
Apr 25 13:15:35 10.31.1.53 Apr 25 1999 13:23:00: %PIX-5-111007:
      Begin configuration: nobody reading from terminal
```

In PIX Software versions 4.3.x and later, you can also do TCP syslog. PFSS supports this. Most other syslog servers do not support it without reconfiguration. The command to enable PIX to do PFSS TCP logging is **logging host #.#.#.# tcp 1740**.

Note: Because this traffic is TCP (that is, with acknowledgments), if the PFSS goes down, traffic through the PIX **stops**. For this reason, the **tcp syslog** command should not be implemented unless you need this kind of functionality. UDP/514 syslogging does not have this effect.

How to Set Up a Syslogd Server

Because syslogd was originally a UNIX concept, the features available in the syslogd products on non-UNIX systems depend on the vendor implementation. Features can include dividing incoming messages by facility or debug level, or both, resolving the names of the sending devices, reporting facilities, and so on. Refer to the vendor documentation for information on the configuration of the non-UNIX syslog server.

Cisco does make a syslog server called the PIX Firewall Syslog Server (PFSS), which is available for PC platforms. Go to the Downloads (registered customers only) and select **Download PIX Firewall Software** to download the Cisco PFSS.

Complete these steps to configure syslog on UNIX:

1. As root, on SunOS, AIX, HPUX, or Solaris, make a backup of the **/etc/syslog.conf** file prior to modification.
2. Modify **/etc/syslog.conf** to tell the UNIX system how to sort out the syslog messages coming in from the sending devices, that is, which logging_facility.level goes in which file. Make sure there is a tab between the logging_facility.level and file_name.
3. Make sure the destination file exists and is writable.
4. The **#Comment** section at the beginning of **syslog.conf** usually explains syntax for the UNIX system.
5. Do not put file information in the **ifdef** section.
6. As root, restart syslogd to pick up changes.

Examples

- If **/etc/syslog.conf** is set for:

```
local7.warn      /var/log/local7.warn
```

the warning, error, critical, alert, and emergency messages coming in on the local7 logging facility will be logged in the local7.warn file. The notification, informational, and debug messages coming in on the local7 facility will not be logged anywhere.

- If **/etc/syslog.conf** is set for:

```
local7.debug     /var/log/local7.debug
```

the debug, informational, notification, warning, error, critical, alert, and emergency messages coming in on the local7 logging facility will be logged to the local7.debug file.

- If **/etc/syslog.conf** is set for:

```
local7.warn      /var/log/local7.warn
local7.debug     /var/log/local7.debug
```

the warning, error, critical, alert, and emergency messages coming in on the local7 logging facility will be logged to the local7.warn file. The debug, informational, notification, warning, error, critical, alert, and emergency messages coming in on the local7 logging facility will be logged to the local7.debug file. (In other words, some messages will go to both files!).

- If **/etc/syslog.conf** is set for:

```
*.debug         /var/log/all.debug
```


syslogd -d>&<target_file>

Note: Red Hat Linux syslogd must be started with the **-r** option to capture network output.

This table shows typical UNIX syslog extensions defining levels:

UNIX Extension	Meaning
.emerg	System unusable, emergencies
.alert	Take immediate action, alerts
.crit	Critical condition, critical
.err	Error message, errors
.warn	Warning message, warnings
.notice	Normal but significant condition, notifications
.info	Informational messages, informational
.debug	Debug message, debugging

Information to Collect if You Open a TAC Case

If you still need assistance after following the troubleshooting steps above and want to open a case with the Cisco TAC, be sure to include the following information for troubleshooting your PIX Firewall.

- Troubleshooting performed before opening the case
- Output from the **show tech-support** command
- Output from the **show log** command after running with the **logging buffered debugging** command, or console captures that demonstrate the problem (if available)

Please attach the collected data to your case in non-zipped, plain text format (.txt). You can attach information to your case by uploading it using the Case Query Tool (registered customers only). If you cannot access the Case Query Tool, you can send the information in an email attachment to attach@cisco.com with your case number in the subject line of your message.

Related Information

- [PIX Command Reference](#)
 - [PIX Support Page](#)
 - [Downloads – PIX Firewall Software](#) (registered customers only)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

