APPENDIX E

Security

This appendix includes information used to ensure the security of your Cisco PAM appliance.

Contents

Cisco PAM TCP Port Requirements for Firewall Connections

Table E-1 lists the TCP ports used by the Cisco PAM appliance. Cisco PAM desktop clients require access to these ports when connecting to a Cisco PAM appliance that is behind a firewall.

Table E-1 Cisco PAM Appliance Ports: Firewall Requirements

Port	Description
TCP 80	HTTP for video and redirect to HTTPS
TCP 443	HTTPS
TCP 1236	Fixed port for CPAM client to server communications.
TCP 3306	MYSQL
TCP 8020	Default port for Gateway to Cisco PAM communication.
UDP 69	TFTP

Related Security Documentation

Refer to the following documentation for security information related to Cisco PAM.

- *Red Hat Enterprise Linux 4.5.0 Security Guide*
  http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/en-US/Security_Guide/
- Security in MySQL
  http://dev.mysql.com/doc/mysql-security-excerpt/5.0/en/index.html

Manually Disable or Enable the Cisco PAM TFTP Server

You can manually enable or disable the Cisco PAM TFTP server.

Note If the TFTP server is disabled, the Image Manager cannot be used to upgrade Gateway firmware images. You must use image files stored on an external TFTP server instead. See Upgrading Gateway Firmware Images Using Cisco PAM, page B-8 for more information.

To manage the TFTP server, do the following:

Step 1 Connect to the Cisco PAM appliance using a console connection or via SSH.

Step 2 Enter the **cpamadmin** username and password.

Step 3 Enter the following commands:

Stop the TFTP server

```
$ sudo /sbin/chkconfig tftp off
```

Start the TFTP server

```
$ sudo /sbin/chkconfig on
```

Check the status of the TFTP server

```
$ sudo /sbin/chkconfig --list tftp
```