



# APPENDIX **D**

## Security

---

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

### Contents

- [Cisco PAM TCP Port Requirements for Firewall Connections, page D-1](#)
- [Related Security Documentation, page D-1](#)
- [Disabling the Cisco PAM TFTP Server, page D-2](#)

## Cisco PAM TCP Port Requirements for Firewall Connections

[Table D-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 D-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/](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>

# Disabling the Cisco PAM TFTP Server

The Cisco PAM appliance includes a TFTP server that is enabled by default. This TFTP server is used primarily to store firmware images for upgrading Gateway modules, as described in [Upgrading Gateway Firmware Images Using Cisco PAM, page C-12](#).

To disable the TFTP server, complete the following steps.



## Note

If the TFTP server is disabled, you must upgrade the Gateway firmware using image files stored on an external TFTP server. See [Upgrading Gateway Firmware Images Using Cisco PAM, page C-12](#) for more information.

- Step 1** Log in to the Cisco PAM Server Administration utility.  
See [Logging on to the Cisco PAM Server Administration Utility, page 3-2](#).
- Step 2** Select the **Monitoring** tab and then select **Status**.
- Step 3** Verify that the TFTP Service is **Up**, click **Stop**, as shown in [Figure D-1](#).
- Step 4** After the confirmation message appears, verify that TFTP Service is **Down**.

**Figure D-1** TFTP Service in “Up” State

The screenshot shows the Cisco PAM Server Administration web interface. The 'Monitoring' tab is selected, and the 'Status' page is displayed. The 'Server' section shows the Admin State as 'Up' with a 'Stop' button. The 'Services' section shows the TFTP Service as 'Up' with a 'Stop' button, and the Web Service API as 'Enabled' with a 'Disable' button. A red box highlights the TFTP Service row. The footer indicates copyright information for Cisco Systems, Inc. from 2008-2012.

Server		
Admin State:	Up	Stop
Server Mode:	Active	
Version:	1.4.1	
Serial Number:	003048BA2B6A	
High Availability Audit:	enabled	
Peer Address:	10.78.177.196	
Peer Hostname:	HA-STANDBY	
Synchronization Status:	Synchronized	

  

Services		
TFTP Service	Up	Stop
Web Service API	Enabled	Disable

(Web Services license not applied)

© 2008-2012 Cisco Systems, Inc. All Rights Reserved.



## Tip

Once the TFTP Service is **Down**, the button changes to **Start**. Click **Start** to enable the TFTP server.