

Table of Contents

<u>Password Recovery Procedure for the PIX</u>	1
<u>Introduction</u>	1
<u>Before You Begin</u>	1
<u>Conventions</u>	1
<u>Prerequisites</u>	1
<u>Step-by-Step Procedure</u>	2
<u>PIX With a Floppy Drive</u>	2
<u>PIX Without a Floppy Drive</u>	2
<u>Sample Output</u>	3
<u>Related Information</u>	4

Password Recovery Procedure for the PIX

Introduction

Before You Begin

Conventions

Prerequisites

Step-by-Step Procedure

PIX With a Floppy Drive

PIX Without a Floppy Drive

Sample Output

Related Information

Introduction

This document describes how to recover a PIX password for PIX software releases through 6.3. Note that performing password recovery on the PIX erases only the password, not the configuration. If there are Telnet or console **aaa authentication** commands in versions 6.2 and greater, the system will also prompt to remove these.

Note: If you have configured AAA on the PIX and the AAA server is down, you can access the PIX by entering the Telnet password initially, and then "pix" as the username and the enable password (enable password password) for the password. If there is no enable password in the PIX configuration, enter "pix" for the username and press ENTER. If the enable and Telnet passwords are set but not known, you will need to continue with the password recovery process.

The PIX Password Lockout Utility is based on the PIX software release you are running.

In addition to the required files listed in the next section, you will need the following items to follow the password recovery procedure:

- A PC
- A working serial terminal or terminal emulator
- Approximately 10 minutes of PIX and network downtime

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

To use the password recovery procedure, you need the PIX Password Lockout Utility, which includes the following files:

- One of the following files, depending on the PIX software version you are running:
 - ◆ np63.bin (6.3 release)
 - ◆ np62.bin (6.2 release)
 - ◆ np61.bin (6.1 release)

- ◆ np60.bin (6.0 release)
- ◆ np53.bin (5.3 release)
- ◆ np52.bin (5.2 release)
- ◆ np51.bin (5.1 release)
- ◆ np50.bin (5.0 release)
- ◆ np44.bin (4.4 release)
- ◆ nppix.bin (4.3 and earlier releases)
- rawrite.exe (needed only for PIX machines with a floppy drive)
- TFTP Server Software (needed only for PIX machines without a floppy drive) TFTP server software is no longer available from Cisco.com, but you can find many TFTP servers by searching for "tftp server" on your favorite Internet search engine. Cisco does not specifically recommend any particular TFTP implementation.

Step-by-Step Procedure

PIX With a Floppy Drive

To recover your password, follow the steps below:

1. Execute the **rawrite.exe** file on your PC and answer the questions on the screen using the correct password recovery file.
2. Install a serial terminal or a PC with terminal emulation software on the PIX console port.
3. Verify that you have a connection with the PIX, and that characters are going from the terminal to the PIX, and from the PIX to the terminal.

Note: Because you are locked out, you will see only a password prompt.

4. Insert the PIX Password Lockout Utility disk into the floppy drive of the PIX.
5. Push the Reset button on the front of the PIX. The PIX will reboot from the floppy and print the message below:

```
Erasing Flash Password. Please eject diskette and reboot.
```

6. Eject the disk and press the Reset button. You will now be able to log in without a password. When you are prompted for a password, press ENTER.
7. The default Telnet password after this process is "cisco." There is no default enable password. Go into configuration mode and issue the **passwd your_password** command to change your Telnet password and the **enable password your_enable_password** command to create an enable password, and then save your configuration.

PIX Without a Floppy Drive

To recover your password, follow the steps below:

Note: Sample output from the password recovery procedure is available below.

1. Install a serial terminal or a PC with terminal emulation software on the PIX console port.
2. Verify that you have a connection with the PIX, and that characters are going from the terminal to the PIX, and from the PIX to the terminal.

Note: Because you are locked out, you will see only a password prompt.

3. Immediately after you power on the PIX Firewall and the startup messages appear, send a BREAK character or press the ESC key. The `monitor>` prompt is displayed. If needed, type ? (question

mark) to list the available commands.

4. Use the **interface** command to specify which interface the ping traffic should use. For floppiless PIXes with only two interfaces, the **monitor** command defaults to the inside interface.
5. Use the **address** command to specify the IP address of the PIX Firewall's interface.
6. Use the **server** command to specify the IP address of the remote TFTP server containing the PIX password recovery file.
7. Use the **file** command to specify the filename of the PIX password recovery file. For example, the 5.1 release uses a file named **np51.bin**.
8. If needed, enter the **gateway** command to specify the IP address of a router gateway through which the server is accessible.
9. If needed, use the **ping** command to verify accessibility. If this command fails, fix access to the server before continuing.
10. Use the **tftp** command to start the download.
11. As the password recovery file loads, the following message is displayed:

```
Do you wish to erase the passwords? [yn] y
Passwords have been erased.
```

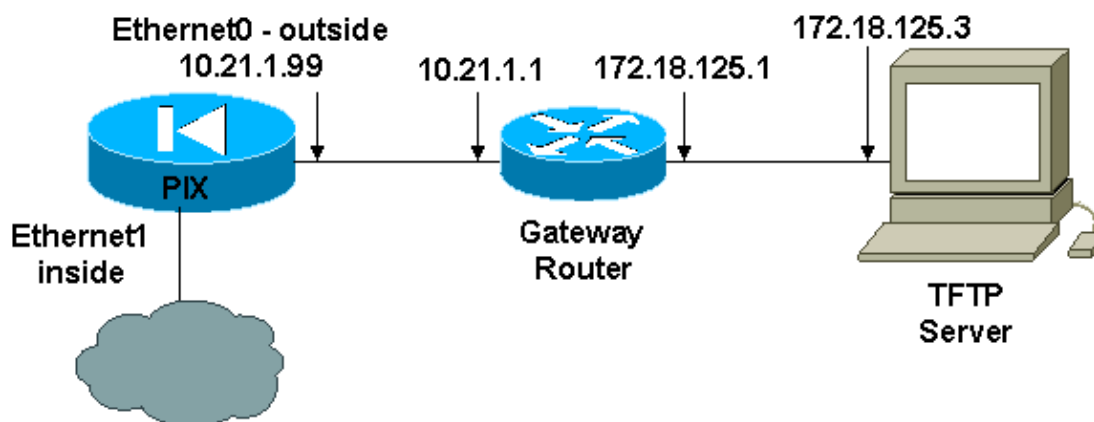
Note: If there are Telnet or console **aaa authentication** commands in version 6.2, the system will also prompt to remove these.

12. The default Telnet password after this process is "cisco." There is no default enable password. Go into configuration mode and issue the **passwd *your_password*** command to change your Telnet password and the **enable password *your_enable_password*** command to create an enable password, and then save your configuration.

Sample Output

The following example of floppiless PIX password recovery with the TFTP server on the outside interface is taken from a lab environment.

Network Diagram



```
monitor> interface 0
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7 )

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10), MAC: 0050.54ff.82b9
monitor> address 10.21.1.99
address 10.21.1.99
monitor> server 172.18.125.3
server 172.18.125.3
```

```
monitor> file np52.bin
file np52.bin
monitor> gateway 10.21.1.1
gateway 10.21.1.1
monitor> ping 172.18.125.3
Sending 5, 100-byte 0xf8d3 ICMP Echoes to 172.18.125.3, timeout is 4 seconds:
!!!!
Success rate is 100 percent (5/5)
monitor> tftp
tftp np52.bin@172.18.125.3 via 10.21.1.1.....
Received 73728 bytes

Cisco Secure PIX Firewall password tool (3.0) #0: Tue Aug 22 23:22:19 PDT 2000
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xd8000

Do you wish to erase the passwords? [yn] y
Passwords have been erased.

Rebooting....
```

Related Information

- [PIX Support Page](#)
 - [Documentation for PIX Firewall](#)
 - [PIX Command References](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support – Cisco Systems](#)
-

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.