

第8章 使用并升级Cisco PIX防火墙软件映像

本章包含下列主题：

- ❖ 使用命令接口
- ❖ 配置、维护并测试PIX防火墙
- ❖ 升级PIX OS
- ❖ 进行口令恢复操作

PIX 命令行接口

PIX 提供了四种管理访问模式：

- ❖ 非特权模式——当一开始访问PIX防火墙时，就是处于这种模式中。这种模式经常被称为用户可执行模式。显示的提示符是>。
- ❖ 特权模式——这种模式显示的提示符是#，在这种模式中，我们可以改变当前设置。在特权模式中，我们也可以使用任何非特权命令。一旦我们访问特权模式，就可以访问配置模式。

维护并测试PIX防火墙

- ❖ 在使用PIX防火墙的时候，有许多通用的维护配置命令。为了从非特权模式进入到特权模式，然后再进入配置模式，需要输入下列命令序列：

```
pixfirewall> enable
```

```
password: *****
```

```
pixfirewall# config t
```

```
pixfirewall(conf)#
```

下列命令用于配置、维护和测试PIX防火墙：

- ❖ enable——如果用户知道口令，enable命令就可以让他进入特权模式。输入enable命令之后，PIX防火墙将要求用户输入特权模式的口令。要想退出特权模式并返回前一种模式，可以使用disable、exit或quit命令。设置口令的命令是enable password password。在PIX防火墙的配置文件中，口令时被加密保存的。
- ❖ configure terminal——如果我们想交互式地改变PIX防火墙的配置，应采用命令configure terminal。任何添加的配置参数都将被归并到当前运行的配置当中。当对PIX防火墙进行配置修改时，修改会立刻生效，并被保存到RAM里正在运行的配置当中。

❖ enable password——这条配置命令的参数将设置允许我们访问特权模式的口令。在我们输入enable命令之后，就被要求输入这个口令。系统没有为enable password命令分配缺省的口令。当第一次访问特权模式时（在产生第一个enable口令之前），要求我们输入一个口令。因为还没有设置口令，所以只要输入一个回车就可以访问特权模式。口令区分大小写的，而且可以具有最多16个字母数字型的字符。我们可以使用任何字符，但是问号、空格和冒号除外。如果改变了一个口令，最好采用一种符合该节点安全策略的方式，对口令进行存储（例如，写入到日志中，并存储到一个安全的区域）。因为enable password是被加密的（缺省），一旦它被产生或改变，在配置文件中都不能以明文的形式看到它。命令show enable显示的是口令的加密形式。在设置enable password时，我们也可以选择输入口令的加密形式。具体做法是，在输入password后，输入可选项encrypted。

- ❖ passwd——命令passwd可以让用户为访问PIX防火墙的Telnet设置口令。缺省的口令值是“cisco”。口令值是一个区分大小写的、最长16个字符的、字母数字型的字符串。可以使用除了问号或空格以外的任何字符。需要着重指出的是，如果美哟设置Telnet口令，一个加密的字符串仍然出现在配置中。命令clear passwd将把Telnet口令重置为cisco。在使用passwd命令来设置口令时，用户也可以选择输入口令的加密形式。具体做法是在输入口令后，输入可选项encrypted。
- ❖ Show configure——这条命令在终端上显示存储在Flash存储器中的配置文件（有时被称为“启动配置（start configuration）”）。因为Flash是非易失性的，所以如果PIX发生掉电或重新启动，存储在那里的配置不会被丢失。启动配置是在系统启动期间，PIX防火墙将装载到RAM中的配置。

- ❖ write terminal——这条命令在终端上显示当前运行的配置（有时被称为“当前配置（current terminal）”）。这个配置是被存储在RAM中的。
- ❖ write net——将当前运行的配置文件存储到TFTP服务器上。将所有配置文件进行离线备份存储是一个好的习惯。当指定TFTP服务器的IP地址和文件路径时，运行的配置就被存储在那个指定的位置。
- ❖ write erase——这条命令清除位于Flash存储器中的配置文件。
- ❖ write floppy——这条命令将运行配置存储到磁盘上。

- ❖ write memory——对PIX做出的任何改动都会立即生效。改动将被写入到位于RAM中的运行配置中。如果想把一个改动保存在PIX防火墙上，就应该用命令write memory将它存储在Flash存储器中。使用这条命令将会用RAM中的配置替换Flash中现存的配置。RAM中的配置保持不变。此命令不会干扰防火墙的数据包处理工作。在此命令执行期间，我们不可以对配置进行任何改动。
- ❖ write standby——将位于活跃的故障切换PIX防火墙上RAM中存储的配置，写到备用PIX防火墙上的RAM中。当活跃的PIX防火墙启动时，它自动将配置写到备用PIX防火墙上。使用这个命令将强制把活跃的PIX防火墙的配置写到备用PIX防火墙。不支持故障切换的PIX防火墙型号不支持使用这条命令。

- ❖ `configure memory`——将运行配置与Flash存储器中的配置运行合并。此命令不是替代Flash存储器中的配置，而是将运行配置和Flash配置之间的不同之处添加到Flash存储器配置中。
- ❖ `show history`——显示以前输入的命令行。可以用上下箭头逐个检查以前输入的命令。
- ❖ `show interface`——让用户可以查看关于接口的信息。在想要建立网络连接时，这是需要被首先输入的命令之一。

在输入show interface命令后所显示信息的解释如下：

- line protocol up（线路协议可用）——说明已将一条工作电缆插入到了网络接口中（第一层连通性）。
- line protocol down（线路协议不可用）——说明被插入到网络接口中的电缆不正确，或者没有将电缆插入到接口中。
- MAC address（MAC地址）——在输出中显示MAC地址。MAC出现在显示“地址是(address is)”之后。
- IP address（IP地址）——显示分配的IP地址。
- subnet mask（子网掩码）——显示子网掩码。
- MTU（最大传输单元）——数据包可以通过网络被传送的最大尺寸，以字节为单位。
- lost carrier——在传送期间，载波信号丢失的次数。

- ❖ show memory——该命令显示PIX防火墙的最大物理存储器和当前可用存储器的汇总信息。
- ❖ show version——该命令让用户可以看到当前运行在PIX防火墙上的操作系统版本。该命令的输出还显示了自从上次重新启动以来，PIX防火墙已经运行了的时间。该命令的输出还显示了：硬件类型、板上的存储器、处理器类型、Flash存储器类型、BIOS Flash信息、接口板、许可证特性、序列号码、激活密钥。
- ❖ show xlate——该命令显示了翻译槽位信息。这些信息是为通过PIX防火墙建立的会话进行地址翻译所分配的IP地址。
- ❖ ping——用于确定PIX防火墙是否具有到达一个指定目标的连通性，或者在网络上的一台主机是否可用（对PIX防火墙是可见的）。
- ❖ telnet——让我们指定哪些主机可以通过Telnet方式访问PIX防火墙的控制台。

在PIX防火墙上安装一个新的OS

根据PIX防火墙的型号和操作系统的版本，在PIX防火墙上安装一个新的操作系统步骤将会稍有不同。

❖ 升级到PIX防火墙的一个不同版本

如果PIX防火墙正在运行PIX防火墙软件版本5.1.1，或更新的版本，我们可以使用copy tftp flash命令从TFTP服务器下载软件映像。我们下载的映像将在下一次重新加载时，将被用于PIX防火墙。

在开始升级之前，PIX OS文件必须位于TFTP服务器之上。

采取下列步骤进行升级：

步骤1：执行copy tftp flash命令，并在被提示时，输入适当的信息。

步骤2：输入TFTP服务器的IP地址。

步骤3：输入源文件名称（PIX OS.bin文件）。

步骤4：输入yes以继续。

例：升级PIX OS

copy tftp flash

Address or name of remote host [127.0.0.1]?10.1.1.1

Source file name [cdisk]?pix531.bin

copying tftp://10.1.1.1/pix531.bin to flash

[yes||]?yes

[illegible]

Received 2138112 bytes.

Erasing current image.

Writing 2048056 bytes of image.

[illegible]

Image installed.

pixfirewall#

❖ 使用监视模式升级到一个不同的PIX OS

当使用监视模式升级所有当前的PIX防火墙型号时，可以采取下列步骤。准备加载到PIX防火墙上的PIX OS文件必须位于TFTP服务器上。

步骤1：中断启动进程，以进入到监视模式。为了完成这个步骤，为PIX重新加电，或者执行reload命令，然后按Escape键或发送一个“Break”字符。一旦进入到监视模式，我们就可以用问号（？）来得到命令帮助。

步骤2：指定用于TFTP传输的PIX防火墙接口。在监视提示符下输入下列命令：

```
monitor> interface num
```

步骤3：指定PIX防火墙接口的IP地址：

```
monitor> address ip_address
```

步骤4：指定缺省网关（如果需要的话）：

```
monitor> gateway ip_address
```

步骤5：验证到TFTP服务器的连通性：

```
monitor> ping server_address
```

步骤6：指定TFTP服务器：

```
monitor> server ip_address
```

步骤7：给出映像文件名称：

```
monitor> file name
```

步骤8：开始TFTP进程：

```
monitor> tftp
```

步骤9：在映像下载完毕后，我们被提示要安装新的映像。输入y来将映像安装到Flash中。

步骤10：当提示输入一个新的激活密钥时，输入y来输入一个新的基于特性的激活密钥，或者输入n来保留我们现有的基于连接的激活密钥。

❖ 升级到PIX防火墙的一个不同版本

如果PIX防火墙正在运行PIX防火墙软件版本5.1.1,或更新的版本，我们可以使用copy tftp flash命令从TFTP服务器下载软件映像。我们下载的映像将在下一次重新加载（重新启动）时，被用于PIX防火墙。

在开始升级之前，PIX OS文件必须位于TFTP服务器之上。

采取下列步骤进行升级：

- ❖ 步骤1：执行copy tftp flash命令，并在被提示时，输入适当的信息。
- ❖ 步骤2：输入TFTP服务器的IP地址。
- ❖ 步骤3：输入源文件名称（PIX OS.bin文件）。
- ❖ 步骤4：输入yes以继续。

口令恢复

口令恢复需要将一个特殊的文件传送到PIX，这个文件在不改动配置的情况下，可以使已配置的口令无效。根据我们拥有的PIX防火墙的不同型号，存在两种不同的方法进行口令恢复。

对于PIX防火墙型号：PIX Classic、PIX 10000、510和520，使用软盘方法。PIX防火墙型号506、515、525和535都使用监视模式来传送文件。

❖ 对于PIX Classic等的软盘口令恢复

步骤1：根据我们正在运行的PIX防火墙软件版本，从Cisco连接在线下载np`xx`.bin文件（这里的`xx`是在PIX防火墙上运行的OS版本号）。

步骤2：将rawrite.exe文件下载到我们先前下载的口令版本的相同目录中。

步骤3：在我们得到这两个文件之后，打开一个MS-DOS窗口，如下所示，执行rawrite.exe文件，并根据提示输入适当的信息：

c:>\ rawrite

RaWrite 1.2 – Write disk file to a floppy diskette

Enter the source file name:npxx.bin

(where XX=version number)

Enter the destination drive:a:

please insert a formatted diskette into drive A:and press -ENTER-:

<ENTER>

Number of sectors per track for this disk is 18

Writing image to drive A:.Press^C to abort.

Track:78 Head:1 Sector:16

Done.

C:\>

步骤4：用我们刚刚创建的磁盘重新启动我们的PIX防火墙。在遇到提示的时候，输入y，来清除口令：

```
Do you wish to erase the passwords?[yn]y
```

```
Passwords have been erased
```

系统自动恢复口令，并开始重新启动（在清除Flash口令之后，必须取出口令恢复磁盘）。Telnet口令被恢复成cisco。

❖ 对于PIX 506等的TFTP口令恢复

步骤1：根据我们正在运行的PIX防火墙软件版本，从
www.cisco.com 下载所需的文件：

www.cisco.com/warp/public/110/34.shtml

步骤2：将我们刚刚下载的二进制文件移动到我们的
TFTP服务器上的TFTP主文件夹。

步骤3：重新启动我们的PIX防火墙，并通过中断启动
进程，进入到监视模式。要想这么做，我们必须按
住Escape键，或发送一个Break字符。

步骤4：指定用于TFTP传输的PIX防火墙接口。为了使用内部接口（以太网1），在监视提示符处输入下列命令：

```
monitor> interface 1
```

步骤5：为了指定PIX防火墙接口的IP地址，例如，10.10.10.1，在监视提示符处输入下列命令：

```
monitor> address 10.10.10.1
```

步骤6：指定缺省网关（通常不需要这样做）。要想这么做，我们必须在监视提示符处输入下列命令：

```
monitor> gateway ip_address
```

步骤7：为了将TFTP服务器的IP地址指定为10.10.10.100，在监视提示符处输入下列命令：

```
monitor> server 10.10.10.100
```

步骤8：通过在监视提示符处输入下列命令，验证到TFTP服务器的连通性：

```
monitor> ping 10.10.10.100
```

步骤9：为了指定口令恢复文件的文件名（例如，在下面实例中的版本5.3(1)），在监视提示符处输入下列命令：

```
monitor> file np53.bin
```

步骤10：开始TFTP进程。要想这么做，我们必须在监视提示符处输入下列命令：

```
monitor> tftp
```

步骤11：在遇到提示的时候，输入y，来清除口令。

```
Do you wish to erase the passwords?[yn]y
```

```
Passwords have been erased
```

系统将自动清除口令，并开始重新启动。