For this lab section, refer to Figure 26-6 on page 927 of the book.

Step 1

```
PIX1(config)# icmp permit any echo-reply inside
```

Step 2

```
PIX1(config)# access-list 100 permit ip host 192.168.1.192
any
PIX1(config)# nat (inside) 0 access-list 100
```

Step 3

```
PIX2(config)# icmp deny any echo outside
PIX2(config)# icmp deny any echo-reply outside
```

Step 4

```
PIX2(config)# service resetinbound
```

Configure the PIX with the **service resetinbound** command, available in PIX Software versions 4.2 and later. Normally, the PIX silently drops inbound connection attempts that are not permitted. When the PIX is configured with the **service resetinbound** command, the PIX sends an RST to unpermitted connection attempts. When the IDENT service receives an RST, it is notified that the IDENT service is unavailable for that client, and continues to process the original traffic that spawned the IDENT request. This significantly decreases the delay for IDENT processing.
Or, use the established command with the **permit to tcp 113** options. (Read the caution first!)

Caution: Allowing port 113 traffic may be considered a security risk. Consult your site's security policy before implementing the established command or adding static/conduit or static/access list pairs.

Step 5

```
PIX2(config)# filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0
PIX2(config)# filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0

PIX1(config)# filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0
PIX1(config)# filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

Step 6

```
logging on
logging timestamp
logging console critical
logging monitor critical
logging buffered critical
logging trap critical
logging history emergencies
logging host inside 192.168.1.7
```

Step 7

```
snmp-server host inside 192.168.1.8
snmp-server location San Jose, CA
snmp-server contact Alina B
snmp-server community nice_try
snmp-server enable traps
```

Step 8

```
ntp authentication-key 6727 md5 cisco6727
ntp authenticate
ntp trusted-key 6727
ntp server 192.168.1.7 key 6727 source inside prefer
```

Step 9

```
ip verify reverse-path interface outside
```

Step 10

```
no fixup protocol smtp 25
ip address outside 130.100.26.2 255.255.255.224
ip address inside 192.168.1.222 255.255.255.0
access-list outside_access_in permit tcp any host
130.100.26.125 eq smtp
access-group outside_access_in in interface outside
static (inside,outside) 130.100.26.125 192.168.1.125 netmask
255.255.255.255 0 0
```

Step 11

```
global (outside) 10 interface
nat (inside) 10 0.0.0.0 0.0.0.0 0 0
```

Step 12

```
auto-update timeout 35
auto-update server
https://********@192.168.1.100//www.cisco.com
 verify-certificate
tftp-server inside 192.168.1.100 pix
```

Step 13

```
ip address outside 130.100.26.2 255.255.255.224
ip address inside 192.168.1.222 255.255.255.0
dhcpd address 192.168.1.200-192.168.1.220 inside
dhcpd dns 207.67.1.10
dhcpd wins 172.16.1.10
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd domain PracticalStudies.Security.com
dhcpd enable inside
```