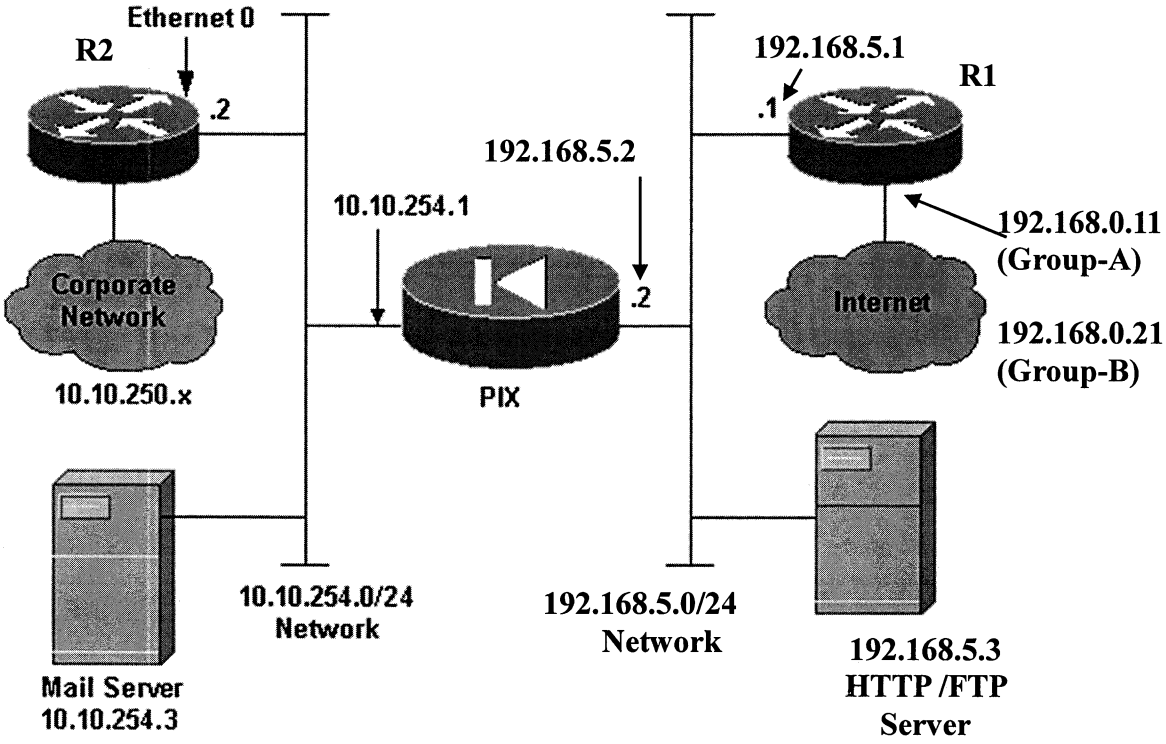
Lab 6: CISCO PIX FIREWALL 501 with 2 CISCO 2600 ROUTER Configuration

Objective: Students will configure two CISCO PIX Firewall and 4 CISCI Routers.

SCENARIO:



NOTE: RTRA is 'R1' or 'R3' depending on your Team and RTRB is 'R2' or 'R4'

PIX Firewall

```
!---NOTE:  If you ever feel you need to set the configuration back to factory !
!---default, issue 'write erase' command.  After the configuration in flash is
!---deleted, issue a 'reload' command.  However, do note that you can simply
!---over write existing configurations by running updated configuration
!---commands.  From default, tere is no 'en' password.  Hit ENTER to escalate.
!NOTE: For each section, PIX, RTRA and RTRB, you will need to telnet through
!your terminal server using the hostname of the machine before executing these
!steps

!--- Once in enable mode, go to configuration mode with command 'config t'

en

config t

!--- X below is according to your team, A or B
hostname PIX501-X

banner motd cAUTHORIZED USE ONLY!c
```

```
!--- Example setting an Enable mode password:

 PIX501-X(config)#enable password cisco (use a more secure password)

!--- This password overrides the enable password and is encrypted inside the
!---config file

PIX501-X(config)#enable secret peter (should be different from enable mode
password)


service password-encryption

!--- Sets the outside address of the PIX Firewall:

ip address outside 192.168.5.2

!--- Sets the inside address of the PIX Firewall:

ip address inside 10.10.254.1

!--- Sets the global pool for hosts inside the firewall:

global (outside) 1 192.168.5.12-192.168.5.254

!--- Allows hosts in the 10.0.0.0 network to be
!--- translated through the PIX:

nat (inside) 1 10.0.0.0

!--- Configures a static translation for an admin workstation
!--- with local address 10.14.8.50:

static (inside,outside) 192.168.5.11 10.14.8.50

!--- Allows syslog packets to pass through the PIX from RTRA.
!--- You can use conduits OR access-lists to permit traffic.
!--- This version of PIX uses conduits better
!--- To the admin workstation (syslog server):
!--- NOTE: The 'eq 514' means 'equals 514,' which permits on port 514 (syslog)



conduit permit udp host 192.168.5.11 eq 514 host 192.168.5.1


!--- Permits incoming mail connections to 192.168.5.10:

static (inside, outside) 192.168.5.10 10.10.254.3

!--- Using conduits

conduit permit TCP host 192.168.5.10 eq smtp any

!--- PIX needs static routes or the use of routing protocols
!--- to know about networks not directly connected.
!--- Add a route to network 10.14.8.x/24.
```

```
route inside 10.14.8.0 255.255.254.0 10.10.254.2

!--- Add a default route to the rest of the traffic
!--- that goes to the internet.

Route outside 0.0.0.0 0.0.0.0 192.168.5.1

!--- Enables the Mail Guard feature
!--- to accept only seven SMTP commands
!--- HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT:
!--- (This can be turned off to permit ESMTP by negating with
!--- the no fixup protocol smtp 25 command):

fixup protocol smtp 25

!--- Allows Telnet from the inside workstation at 10.14.8.50
!--- into the inside interface of the PIX:

telnet 10.14.8.50

!--- Turns on logging:

logging on

!--- Turns on the logging facility 20:

logging facility 20

!--- Turns on logging level 7:

logging history 7

!--- Turns on the logging on the inside interface:

logging host inside 10.14.8.50
```

Note: R1/R3 is the outside shield router. It must shield the PIX Firewall from directed attacks, protect the FTP/HTTP server, and act as an alarm system. If anyone breaks into RTRA, the system administrator should be notified immediately.

R1 / R3

```
!--- Get in enable mode and then configuration mode
en

config t

no service tcp-small-servers
!---Small servers are daemons useful for diagnostics.  Recommendation is to
!---disable them for sdecurity.  They are enabled by default.

!--- Prevents some attacks against the router itself.
```

```
logging trap debugging

!--- Forces the router to send a message
!--- to the syslog server for each and every
!--- event on the router. This includes packets denied
!--- access through access lists and
!--- configuration changes. This acts as an early warning system to the system
!--- administrator that someone is trying to break in, or has broken in and is
!--- trying to create a "hole" in their firewall.

logging 192.168.5.11

!--- The router logs all events to this
!--- host, which in this case is the
!--- "outside" or "translated" address of the system
!--- administrator's workstation.

enable secret xxxxxxxxxxx
service password-encryption
!
interface Ethernet 0/0
 ip address 192.168.5.1 255.255.254.0

!--- Shields the PIX Firewall and the HTTP/FTP
!--- server from attacks and guards
!--- against spoofing attacks.

!
access-list 110 deny ip 192.168.5.0 0.0.0.255 any log

!--- RTRA and the PIX Firewall.
!--- This is to prevent spoofing attacks.

access-list 110 deny ip any host 192.168.5.2 log

!--- Prevents direct attacks against the
!--- outside interface of the PIX Firewall and
!--- logs any attempts to connect to the
!--- outside interface of the PIX to the syslog server.

access-list 110 permit tcp any 192.168.5.0 0.0.0.255 established

!--- Permits packets which are part
!--- of an established TCP session.

access-list 110 permit tcp any host 192.168.5.3 eq ftp

!--- Allows FTP connections into the FTP/HTTP server.

access-list 110 permit tcp any host 192.168.5.3 eq ftp-data

!--- Allows ftp-data connections into the FTP/HTTP server.

access-list 110 permit tcp any host 192.168.5.3 eq www

!--- Allows HTTP connections into the FTP/HTTP server.

access-list 110 deny ip any host 192.168.5.3 log
```

```
!--- Disallows all other connections to
!--- the FTP/HTTP server, and logs any attempt
!--- to connect this server to the syslog server.

access-list 110 permit ip any 192.168.5.0 0.0.0.255

!--- Permits other traffic destined to the
!--- network between the PIX Firewall and RTRA.

!
line vty 0 4
 login
 password xxxxxxxxxx
 access-class 10 in

!--- Restricts Telnet access to the router
!--- to those IP addresses listed in
!--- access list 10.

!
access-list 10 permit 192.168.5.11

!--- Permits only the workstation of the administrator
!--- to Telnet into the router. This
!--- access list may need to be changed to permit
!--- access from the Internet for
!--- maintenance, but should contain as few
!--- entries as possible.

!--- de-escalate to enable mode
Exit

!--- save configuration
copy run start
```

Note: R2/R4 is the inside shielding router. It is the last line of defense in your firewall, and the entry point into your inside network.

R2 / R4

```
logging trap debugging
logging 10.14.8.50

!--- Log all activity on this router to the
!--- syslog server on the administrator's
!--- workstation, including configuration changes.

!
interface Ethernet 0/0
 ip address 10.10.254.2 255.255.254.0
 no ip proxy-arp
 ip access-group 110 in

!--- Prevents inside and outside addresses
!--- from mingling; guards against attacks
```

```
!--- launched from the PIX Firewall or the
!--- SMTP server as much as possible.

!--- de-escalate out of interface mode, and back into config mode
exit


access-list 110 permit udp host 10.10.250.5 0.0.0.255 0.0.0.0


!--- Permits syslog messages destined
!--- to the administrator's workstation.

access-list 110 deny ip host 10.10.254.1 any log

!--- Denies any other packets sourced
!--- from the PIX Firewall.

access-list 110 permit tcp host 10.10.254.3 10.0.0.0 0.255.255.255 eq smtp

!--- Permits SMTP mail connections from the
!--- mail host to internal mail servers.

access-list 110 deny ip host 10.10.254.3 10.0.0.0 0.255.255.255

!--- Denies all other traffic sourced
!--- from the mail server.

access-list 110 deny ip 10.10.250.0 0.0.0.255 any

!--- Prevents spoofing of trusted addresses
!--- on the internal network.

access-list 110 permit ip 10.10.254.0 0.0.0.255 10.10.250.0 0.255.255.255

!--- Permits all other traffic sourced from
!--- the network between the PIX Firewall and RTRB.

!
line vty 0 4
 login
 password xxxxxxxxxx
 access-class 10 in

!--- Restricts Telnet access to the router
!--- to those IP addresses listed in
!--- access list 10.

!
access-list 10 permit  10.14.8.50

!--- Permits only the workstation of the administrator
!--- to Telnet into the router. This
!--- access list may need to be changed to permit
!--- access from the Internet for
!--- maintenance, but should contain as few entries as possible.

!--- A static route or routing protocol must be utilized
!--- to make the router aware of network 10.14.8.x (which is
```

```
!--- inside the corporate network). This is because
!--- it is not a directly connected network.
```

exit

```
!--- Save configuration
```
copy run start