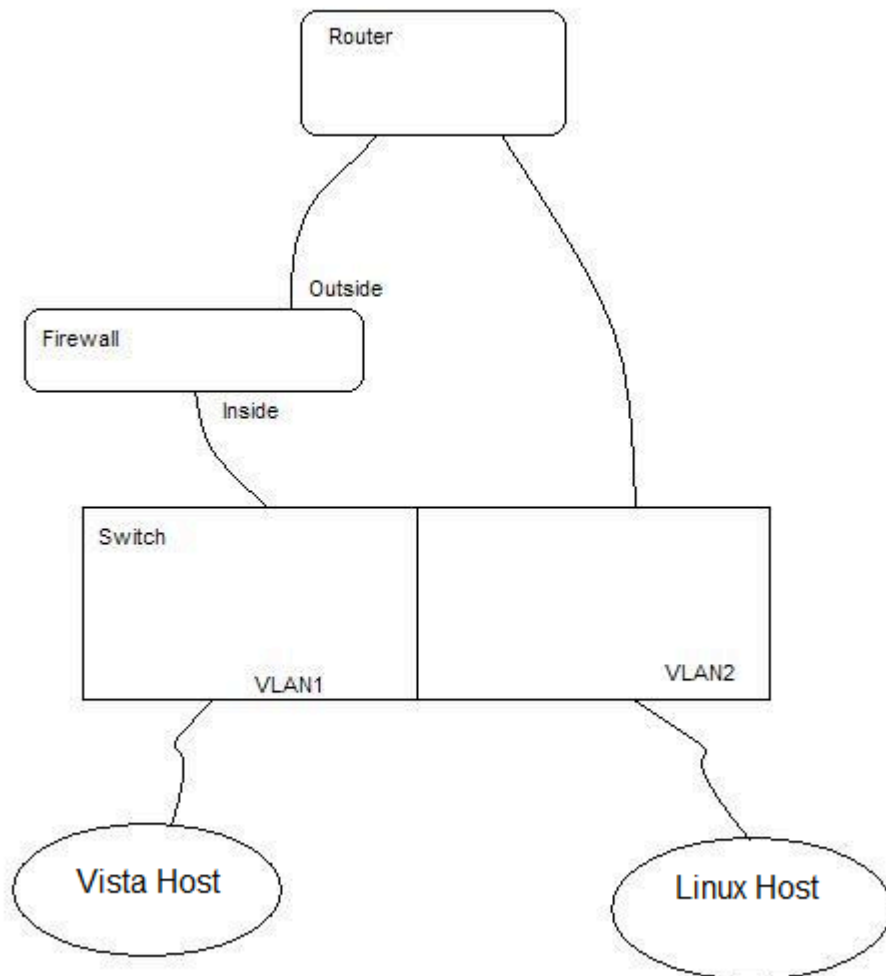


Firewalls

1 Topology

Setup the Switch, Router1, Firewall, and hosts as shown in Figure 1.

The work-area host system will be on the Inside network, simulating the inside, protected company network. The Router and Linux Host will simulate the outside, or untrusted Internet connection.



1.1 Addressing

Setup the inside addresses for the Vista Host and Inside firewall on your specified 10.10X.0.0/24 subnet, using VLAN1. Pick addresses for the Outside network and Router interface from the 10.10X.1.0/24 subnet, and 10.10X.2.0/24 subnet for the VLAN2 interfaces. ***(If you use different Subnets for your interfaces, the Examples will have to all be modified to reflect those changes!)***

Vista:10.10X.0.3

Firewall Inside (Ethernet 1):10.10X.0.20

Firewall Outside (Ethernet 0):10.10X.1.20

Router Ethernet:10.10X.1.1

Router FastEthernet:10.10X.2.1

Linux:10.10X.2.2

Recall for the Linux Host: Open a local terminal and run the following command to change the Linux Host's IP address to 10.10X.2.2 and changed the default router.

```
misy@localhost ~ $ sudo /sbin/ifconfig eth0 10.10X.2.2 netmask 255.255.255.0  
misy@localhost ~ $ sudo /sbin/route add default gw 10.10X.2.1
```

and remove the default gateway for internet/wireless access if it is configured

```
misy@localhost ~ $ sudo /sbin/route del default gw netlab1
```

Remember to adhere to the network addressing policy posted at your lab station. The password you use for the sudo command is the same as the account password (Please be sure to reset the server back onto VLAN1 when you're finished, by physically plugging it's cable into a VLAN1 port, and re-running the above ifconfig command with the 10.10X.0.2 address).

1.2 Routing

The systems in the network will still require some form of routing information to be able to interconnect, whether static or dynamic routing is used. Recall that Routers and IRPs like RIP, only deal with connected networks. Setup default routing on the Vista Host and the Linux Host since they have single points of egress. Setup static routing on the firewall and the router to allow them to route to the networks on the opposite sides of the devices (Firewall route to subnet 10.10X.2.0 through Router, Router route to subnet 10.10X.0.0 through Firewall).

Router

```
Router1(config)#ip routing  
Router1(config)#ip route 10.10X.0.0 255.255.255.0 10.10X.1.20
```

Firewall

```
Firewall(config)#route outside 10.10X.2.0 255.255.255.0 10.10X.1.1
```

2 Firewall Translation

2.1 Preliminary

Connect to the Firewall over the Console connection and begin to configure the firewall in much the same way as the router and switch were configured. The configuration manual for the pix firewall is located in the User manuals folder on the desktop of the Linux host (titled PIX Configuration Guide.pdf), and sample configurations are included in Appendix A of this handout. Make sure your Firewall begins with a clear/fresh configuration by issuing the command:

write erase

Chapter 2 of the configuration manual (“Establishing Connectivity”) explains the preliminary steps for setting up the firewall: setting the interface addresses, naming the interfaces, and setting up routing, and allowing ICMP (PING) testing access-lists. Additionally, you should setup informational log reporting using the logging command.

logging on
logging buffered debugging
logging console info

and

debug icmp trace

to show ping information on the Firewall console. Most of the basic setup commands are covered in Basic Configuration Examples located in the manual (page 2-25). **IMPORTANT: Make sure the Ethernet0 and Ethernet1 interfaces of the Firewall are connected to the proper equipment in Figure 1 and named appropriately for their Inside and Outside use.**

2.2 No Translation

Using the NAT ID of zero, configure the inside interface to allow inside addresses to be used without translation.

nat (inside) 0 10.10X.0.0 255.255.255.0
access-list acl_out permit icmp any any
access-group acl_out in interface outside

Test (PING) the link from inside to outside and vice-versa.

2.3 Static Translation

Using the **static** command, you should establish a static mapping between the Vista Host’s Inside address (10.10X.0.3) and an address on the Outside subnet. If the routing has been successfully configured, you should be able to ping between the Vista Host and the Linux Host, and back from the Linux Host to the static outside address of the Host. You may have to issue the **clear xlate** command before each NAT test, to clear the translation from the previous test.

```
clear xlate
no nat (inside) 0 10.10X.0.0 255.255.255.0
static (inside, outside) 10.10X.1.3 10.10X.0.3 netmask 255.255.255.255 0 0
```

2.4 Dynamic Translation

Change the static translation NAT to a dynamic translation. Use the `global` command and a nonzero NAT ID with the `nat` command to setup a pool of addresses for the translation. Remember to add a default translation address with the `global` command in case the pool is exhausted. Test and confirm the translation.

```
clear xlate
no static (inside, outside) 10.10X.1.3 10.10X.0.3 netmask 255.255.255.255 0 0
nat (inside) 1 10.10X.0.0 255.255.255.0
global (outside) 1 10.10X.1.30-10.10X.1.40
global (outside) 1 10.10X.1.3
```

3 Additional Tasks

3.1 GUI

The Adaptive Security Device Manager (ASDM) is a JAVA based configuration tool for the PIX firewall. Connect to the firewall from the Vista station browser to the firewall on the inside interface. Follow these steps to access the ASDM interface:

1. On a FIREFOX browser running on the Vista workstation connected to the PIX Firewall unit, enter the following:
`https://pix_inside_interface_ip_address`
where `pix_inside_interface_ip_address` is the IP address of the inside interface of your PIX Firewall, entered in standard (number) format.
This launches ASDM. **Note** Ensure that you add the "s" to "https" or the web browser cannot connect. HTTPS (HTTP over SSL) provides a secure connection between your browser and the PIX Firewall that you are using ASDM to configure or monitor.
 2. Accept the security certificate. (You must accept the certificate to use ASDM.)
 3. Do not enter a username. If there is an enable password, enter it. If there is no enable password, click **OK** to continue.
 4. Accept the second certificate presented also. This certificate, issued by the VeriSign certification authority (CA), ensures that the certificate originated from Cisco Systems and enables ASDM to run as a signed applet.
 5. ASDM starts after the certificates are accepted. Follow the instructions on screen.
 6. Refer to the ASDM online Help for information on how to use ASDM.
1. Use the GUI to verify the configuration from the last successful test.
 2. Save a copy of the configuration to the TFTP server on the host.
 3. Finally, use the ASDM to display interface graphs for both the Inside and Outside interfaces of the firewall.

3.2 Allowing protocols through the Adaptive Security Algorithm (ASA)

Open a Command window on the server and attempt to RSH (sudo rsh address) into the Vista Host (from the Linux Host, even though this service may not be running). Monitor the logs on the firewall. Next, use the **fixup** command to enable application inspection of these protocols through the firewall. (They may be already enabled by Default) Repeat the tests and verify that the firewall is now inspecting and allowing the connections through. (The Vista Host is not running a server for this protocol, so it should fail) Wireshark can be used to monitor traffic that enters the Firewall, and the Firewall Logs should show traffic that is blocked.

3.3 Whitehat testing

On your outside Linux host, run the NMAP (Zenmap) program against your inside host to see what, if anything, you can find out about the inside network. Try adding general access through the firewall with an ACL to permit "ip" from any source to any destination, and rerun your tests to see if you can find any additional information.

Appendix A: Configuration Examples

Configuration Examples

Example 2-1 Two Interfaces Without NAT

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
interface ethernet0 10baset
interface ethernet1 10baset
ip address outside 209.165.201.3 255.255.255.224
ip address inside 209.165.200.225 255.255.255.0
hostname pixfirewall
arp timeout 14400
no failover
names
pager lines 24
logging buffered debugging
nat (inside) 0 209.165.200.225 255.255.255.0
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
access-list acl_out permit icmp any any
access-group acl_out in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server community public
mtu outside 1500
mtu inside 1500
```

Example 2-2 Two Interfaces with NAT

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
interface ethernet0 10baset
interface ethernet1 10baset
ip address outside 209.165.201.3 255.255.255.224
ip address inside 192.168.3.0 255.255.255.0
hostname pixfirewall
arp timeout 14400
no failover
names
pager lines 24
logging buffered debugging
nat (inside) 1 0 0
global (outside) 1 209.165.201.10-209.165.201.30
global (outside) 1 209.165.201.8
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
access-list acl_out permit icmp any any
access-group acl_out in interface outside
```

```

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server community public
mtu outside 1500
mtu inside 1500

```

Example 2-4 Three Interfaces with NAT and PAT

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
interface ethernet0 10full
interface ethernet1 10full
interface ethernet2 10full
ip address outside 209.165.201.4 255.255.255.224
ip address inside 10.0.0.3 255.0.0.0
ip address dmz 192.168.0.1 255.255.255.0
hostname pixfirewall
arp timeout 14400
no failover
names
pager lines 24
logging buffered debugging
no rip inside passive
no rip outside passive
no rip inside default
no rip outside default
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
access-list acl_out permit icmp any any echo-reply
access-list acl_out permit icmp any any unreachable
access-list acl_out permit icmp any any time-exceeded
access-group acl_out in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server community public
mtu outside 1500
mtu inside 1500
mtu dmz 1500
telnet 10.0.0.100 255.255.255.255
telnet timeout 15
global (outside) 1 209.165.201.10-209.165.201.30
global (outside) 1 209.165.201.5
global (dmz) 1 192.168.0.10-192.168.0.20
nat (inside) 1 10.0.0.0 255.0.0.0
nat (dmz) 1 192.168.0.0 255.255.255.0
name 192.168.0.2 webserver
static (dmz,outside) 209.165.201.6 webserver netmask 255.255.255.255
access-list acl_out permit tcp any host 209.165.201.6 eq 80
access-group acl_out in interface outside

```

Dynamic NAT example:

```
global (outside) 1 209.165.201.10-209.165.201.20 netmask 255.255.255.224
```

```
global (outside) 1 209.165.201.5 netmask 255.255.255.224
```

The first global command statement specifies a single IP address, which the PIX Firewall interprets as a PAT. The second global command statement augments the pool of global addresses on the outside interface. The PAT creates a pool of addresses used only when the addresses in the second global command statement are in use.

Static NAT example:

The following command maps a server with an internal IP address of 10.1.1.3 to the registered IP address 209.165.201.12:

```
static (inside, outside) 209.165.201.12 10.1.1.3 netmask 255.255.255.255 0 0
```

This command simply maps the addresses; make sure you also configure access using the **access-list** and **access-group** commands

The following example illustrates the three commands required to enable access to a web server with the external IP address 209.165.201.12:

```
static (inside, outside) 209.165.201.12 10.1.1.3 netmask 255.255.255.0 0 0  
access-list acl_out permit tcp any host 209.165.201.12 eq www  
access-group acl_out in interface outside
```