

Cyber Security Lab 1

Due

February 7

Goal

Perform basic configuration of PIX firewall.

Requirements

Bob Co. has hired you and your partner to design a configuration for a border PIX firewall.

The firewall has four interfaces (inside, outside, DMZ, and mgmt) and is designed to separate internal corporate machines from DMZ servers and from the outside world. It needs to be configured to enforce the following constraints.

The employees of Bob Co should be able to web surf, ssh, and ping anywhere in the outside. They should also be able to pull mail via POP via a mail server running on the DMZ machine. They also need to ssh to the DMZ machine for maintenance and browse the web server. The web traffic accessed from the inside should not have any java or activeX content.

People from the outside world should be able to surf the DMZ web server. Appropriately authenticated mail servers should communicate via SMTP with the DMZ machine. In addition, the boss wants to be able to SSH in from his home computer to his work computer. You can use the Ping box (192.168.100.100) as the bosses computer.

The DMZ machine is not yet configured. There will be one DMZ virtual machine with a unique address for each firewall. The details will be posted on the class web site and in the newsgroup when they become available (by Thursday).

No traffic is allowed from Control to the other interfaces or to Control from the other interfaces. The control network should be an isolated network dedicated to managing and monitoring the network security devices. However, in our scenario, the control network is also connected to the outside router to enable you to upload your final configs.

All applications proxies for the allowed traffic should be configured via the inspect command. All other application proxies should be turned off. All protocols necessary for a good user experience should be allowed.

Configure antispoof checks on the outside interface (via the ip verify reverse-path command).

Set the domain name of the device to "bob.com". Set the banner to warn that any unauthorized access is illegal.

Things you will need to know

PIX Versions

All PIX are loaded with image 7.2.1. All PIX are loaded with ASDM 5.2.1. ASDM is a GUI management java application. In the past I have gotten that to run under windows. Unfortunately, I do not have the windows environment set up yet. When that is ready, I will post to the class newsgroup.

The PIX images installed only communicate with ssh version 1 and DES. From linux, the following command will allow you to connect via ssh:

```
ssh -1 -l pix -c des <ip address of the firewall>
```

This will get you to the first prompt. To actually do anything interesting, you will want to execute the “enable” command to enter privileged mode. It will prompt you for another password which should be “class-test”.

At this point, the prompt should end with “#”. You can run “show config” to see the configuration loaded in non-volatile RAM (basically the config that would be loaded when the firewall reboots) or “show running-config” to show the config currently executing in memory (if you just logged on, these should be the same). “show interface” shows the current addresses and state of the interfaces. “show xlate” shows the current state of the translation (or session) table.

At any point “?” will show you the commands that can be executed at this point. You can also enter a command followed by the “?”, e.g., “show ?”, to see all the options of the command.

Execute “config term” to enter configuration mode from the terminal. “?” will show many more possible configuration commands. Configuration commands that you will need for this lab include: access-list, access-group, static, inspect, filter java, ip verify reverse-path. “end” or “exit” will take you out of “config term” mode.

To make your edits persistent, use the command “write memory” or “write mem”. This will push the edits to the startup config storage.

The PIX 7.2 documentation is voluminous, so I cannot print copies for you. Online references are below.

Cisco Security Appliance Command Line Configuration Guide, Version 7.2,
http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/conf_gd.html

Cisco Security Appliance Command Reference, Version 7.2,
http://www.cisco.com/en/US/docs/security/asa/asa72/command/reference/cmd_ref.html

Configuration commands that you will need for this lab include: access-list, access-group, static, inspect, filter activex, , ip verify reverse-path, domain, banner. “end” or “exit” will take you out of “config term” mode.

Device Assignment and Storing Configs

We are using virtual firewalls this semester in attempt to make sharing hardware cleaner. Each of the five physical firewalls has three virtual firewalls (or security contexts). One context is the admin context and we will not be using that one. The other two contexts have the naming scheme fwX-Y, where X is the physical firewall number (1-5) and Y is the context number (1 or 2). Each context has its persistent configuration stored on the management machine (192.168.200.2). It is accessed via ftp using Alice's account. The configurations are stored at /home/alice/configs/fwX-Y.cfg. Original versions of those configurations are stored at /home/alice/configs/orig.

We will likely have multiple teams sharing a context in some cases. When getting ready to start work on their context, the team should copy their version of the configuration into /home/alice/configs/fwX-Y.cfg (perhaps backing up the previous version to fwX-Y.cfg.bak). Then they should reload the context.

You can also edit the configuration file directly and use “copy startup-config running-config” to bring the changes into the system. Editing directly is useful for removing commands (e.g., access-lists where you must list each entry you one to remove prefixed by “no”).

Address Translation Requirements

PIX uses security levels associated with the interfaces to determine what traffic should be allowed and should not be allowed. Traffic originating from a high security interface (e.g. Inside) to a lower security interface (e.g. Outside) is *outbound* traffic. Traffic originating from a low security interface to a higher security interface is *inbound* traffic.

Any inbound traffic must be targeting a statically mapped address. This statically mapped address may map the address to itself (e.g. DMZ to inside traffic). Traffic coming from the outside must be targeting a routeable address.

In the lab configuration, our firewalls are protected by a router, which has the routeable address. The router will perform address translation from the 192.168.100.0/24 to real routable addresses. Therefore, for the sake of our lab, assume that the network 192.168.100.0/24 is routeable. Each device has one routeable address associated with its outside interface. Similarly, all traffic leaving the outside interface must have a routeable source address.

To enable outbound traffic, you will need to set up an address pool using the **global** command, and set up a hiding rule using the **nat** command. You can use the outside interface address as the global pool value.

Getting the address translation right is a key part to configuring any border security device and a PIX device in particular.

Lab Configuration

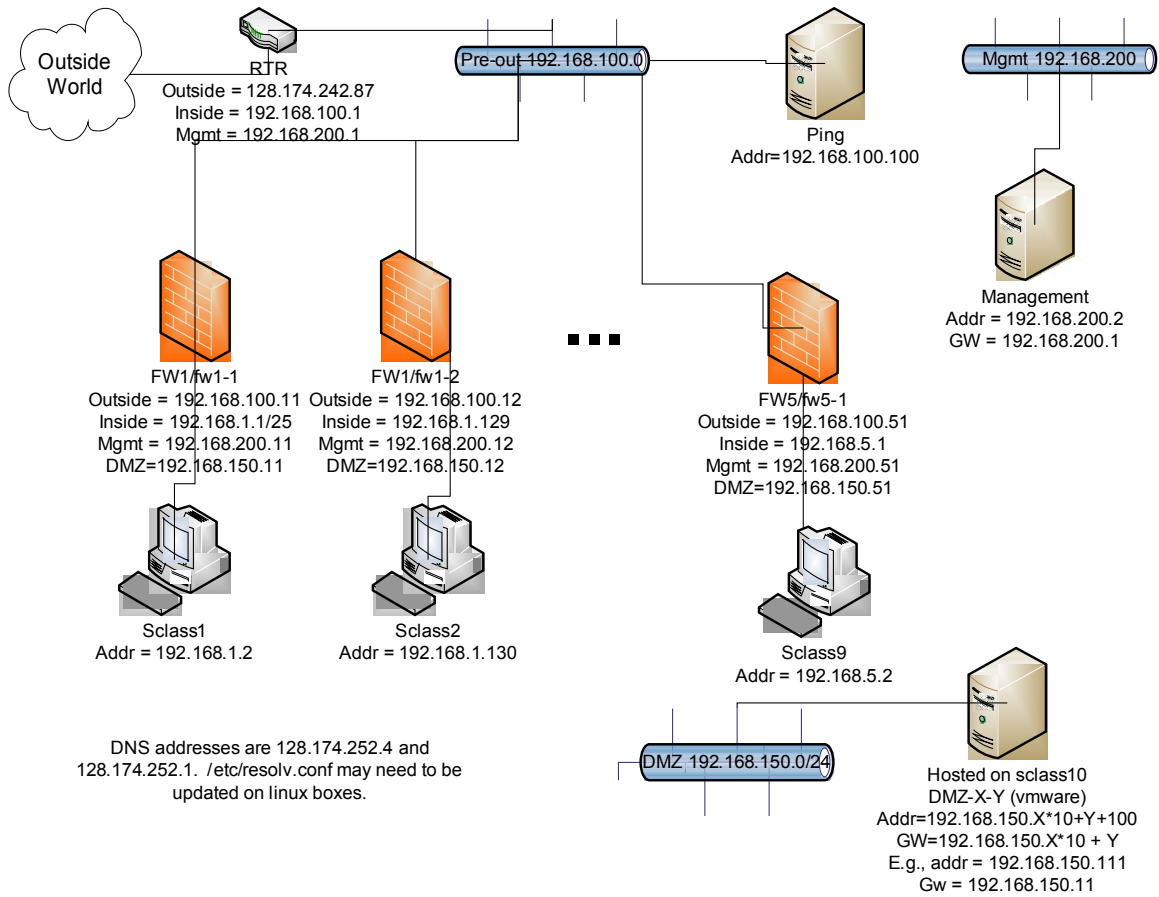


Figure 1: Lab configuration and addressing

Testing Traffic

To try and access the inside and DMZ networks from the outside, you can SSH to ping. From there you can wget to try and access your target machines.

There will be an apache web server running in each of the DMZ Virtual machines. It will have minimal content. Feel free to add test content as needed.

Your tasks

You will need to perform the following tasks.

1. Configure the firewall based on the requirements specified. Verify that the traffic is passing as you expect.
2. Work with logging to get evidence that traffic is being blocked as expected. Look at the “logging” command.

Hand-in Items

1. The firewall configuration file
2. A brief description of what you did to configure and test the firewall, including a more precise enumeration of your interpretation of the specifications.
3. An example syslog entry from blocked traffic.
4. List three aspects of this configuration that you would not do in real life.
5. Once the border firewall is deployed, is Bob Co? safe from malware exploits? Why or why not?