Firewall Configuration Lab

Goal

Perform basic configuration of PIX firewall.

Due

Submit your final report on compass by midnight Friday, March 5. You can work in teams of two or three. Only one report needs to be submitted for the group.

Requirements

CosaNostra Pizza has hired your group 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 CosaNostra Pizza should be able to web surf, ssh, and ping anywhere in the outside. They should also be able to pull mail via POP from 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 and access the ftp server on the DMZ machine. You should spend some time filtering out addresses that should not come from the "outside world". You should investigate Internet Storm Center reports to find currently hostile machines to block (say at least the top 10 attackers http://isc.sans.org/reports.html). Also look at the bogon list (unallocated address ranges) maintained by Team Cymru (http://www.cymru.com/Documents/bogon-list.html). Also remember that the only private network your outside interface should see is 192.168.100.0/24.

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 machine as the Boss's machine in your configuration.

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

All application 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.

Set the domain name of the device to “cosanostra.com”. Set the banner to warn that any unauthorized access is illegal.

Things you will need to know

PIX Interaction

All the clients and all the FW inside interfaces are on a common vlan. To communicate with a particular FW, the client machine will need to have an address statically set within the network associated with that firewall's inside interface. For example to communicate with FW1-1 (address 192.168.11.1 and network 255.255.255.0), you could set your client's address to 192.168.11.100 with a default gateway of 192.168.11.1 and DNS address of 130.126.2.131.

The PIX are configured to allow telnet connections from the inside network. The telnet password is “cisco”.

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 licenses on the PIX images installed only allow communication 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>
```

Some of the admin contexts do not have RSA certificates set. If the ssh fails with a message about a bad or missing certificate, telnet in and run the following command:

```
crypto key generate rsa modulus 512
```

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 theory this should work on Linux, but I have only been successful in getting ASDM running on windows, so use the windows VM to give it a try.

The ASDM requres JRE 5 (or 1.5). I have a copy downloaded in the lab, which we can pass around. Once the JRE is installed, point your browser to the https URL if your firewall's inside address, e.g., https://192.168.11.1 for fw1-1. It will prompt for a user name and password. Leave the user name blank and the password is class-test.

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

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 (called security contexts in the PIX documentation). One context is the admin context and is named admin. 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 non-admin 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. The admin config is stored on the firewall persistent storage. You can use the "copy" command to get a copy of the admin's running configuration to the ftp server.

If you really mess up the configuration, you could update the configuration file on the ftp server and reload the virtual firewall to revert to that version. You can also edit the configuration file directly and use "copy startup-config running-config" or "reload" 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 routeable 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.

In theory, that one routeable address should be sufficient for all address translation, but it may be easier to set of the different types of address translation with different external

addresses. You may assume that you own the outside interface address plus 100, too. For example, FW1-1 owns 192.168.100.11 and 192.168.100.111. Both addresses may be used for the address translation configuration.

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.

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

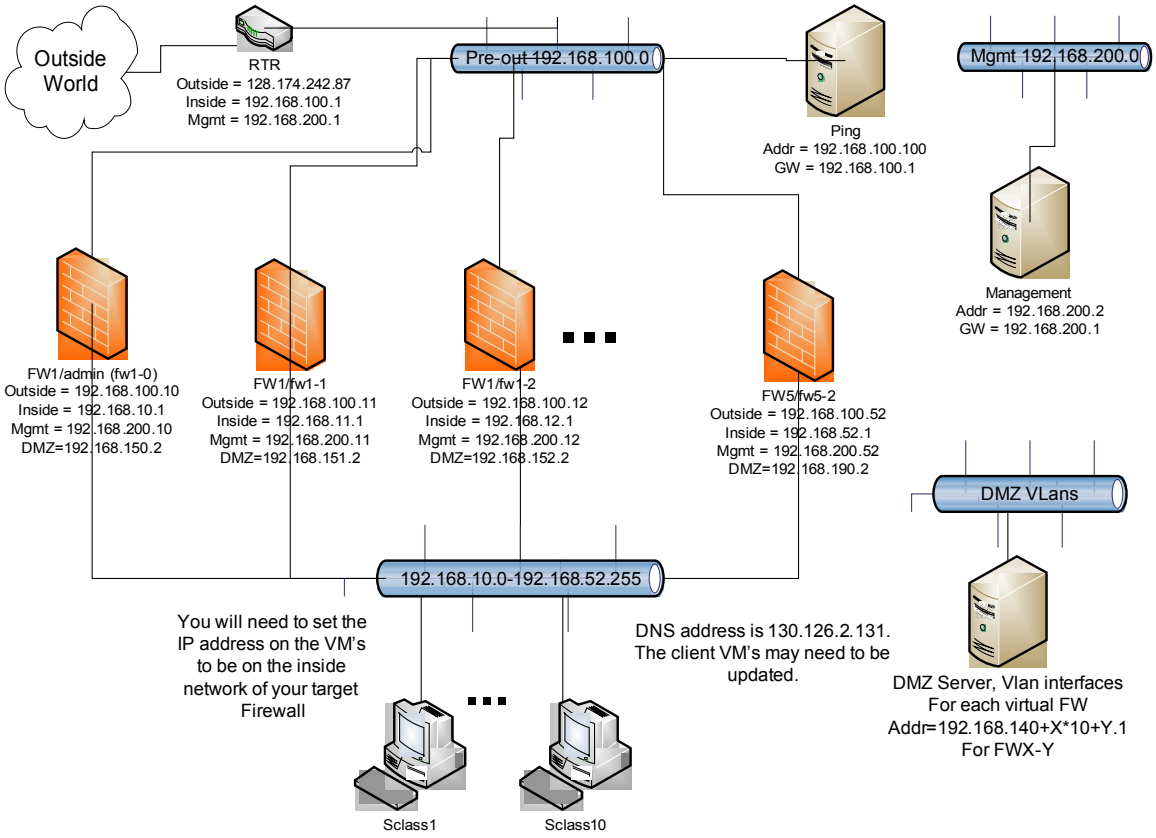
1. The firewall configuration file
2. A brief description of what you did to configure and test the firewall, including a precise enumeration of your interpretation of the specifications.
3. An example syslog entry from blocked traffic.
4. List three aspects of this configuration that you would not do in real life.
5. How would you augment the firewall architecture (by rearranging the firewall, adding other mechanisms, etc), to improve CosaNostra's perimeter security?

Testing Traffic

The ping box is situated outside all the firewalls. It can be used to test your inbound firweall rules. To try and access the inside and DMZ networks from the outside, you can SSH to ping. From there you can wget and ftp to try and access your target machines.

There is an apache web server and ftp server running on the DMZ machine. It has minimal content. Feel free to add test content as needed.

Complete Lab Configuration



Single Firewall Perspective