

Cyber Security Lab 4

Due

March 14

Goal

Perform basic configuration of PIX firewall.

Requirements

YoYoDyne has retained you to design a configuration for a border PIX firewall.

The firewall has three interfaces (inside, outside, and DMZ) 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.

Inside to outside traffic allowed:

- HTTP, HTTPS, ssh, FTP, ping request to anywhere
- Block Java on HTTP traffic

Inside to DMZ traffic allowed:

- SMTP, Ssh, HTTP, HTTPS, telnet, ping request to DMZ server

Outside to DMZ allowed:

- SMTP, HTTP and HTTPS to DMZ server

Outside and DMZ to inside allowed:

- Ping reply

Inbound traffic (outside to DMZ or inside and DMZ to inside) will require static address translation mappings.

All applications proxies for the allowed traffic should be configured (via the fixup (or inspect) command). Other application proxies should be turned off.

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

Things you will need to know

PIX Versions

PIX Fw4 and Fw5 are have more memory and are running the new PIX 7.0 image. The other PIX firewalls are running PIX 6.3. The commands are different between the two images, so if you start working on PIX 7.0, you will probably not want to switch to a PIX 6.3 device (and visa versa).

Commands of interest

Copies of all four guides in the lab.

PIX 6.3 Firewall and VPN Configuration Guide,

http://cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080172852.html

PIX 6.3 Command Reference Guide,

http://cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_book09186a008017284e.html

Cisco Security Appliance Command Line Configuration Guide, Version 7.0,

http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_book09186a0080450278.html

Cisco Security Appliance Command Reference, Version 7.0,

http://www.cisco.com/en/US/products/ps6120/products_command_reference_chapter09186a00805fdeb7.html

The base configurations enable administrative access from the inside via Telnet, SSH, and SSL (PDM). When you are prompted for authentication, enter no user name and use either “class-test” or “cisco” as the password.

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 -l -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, fixup (or inspect in PIX 7.0), filter java, ip verify reverse-path. “end” or “exit” will take you out of “config term” mode.

Lab Configuration

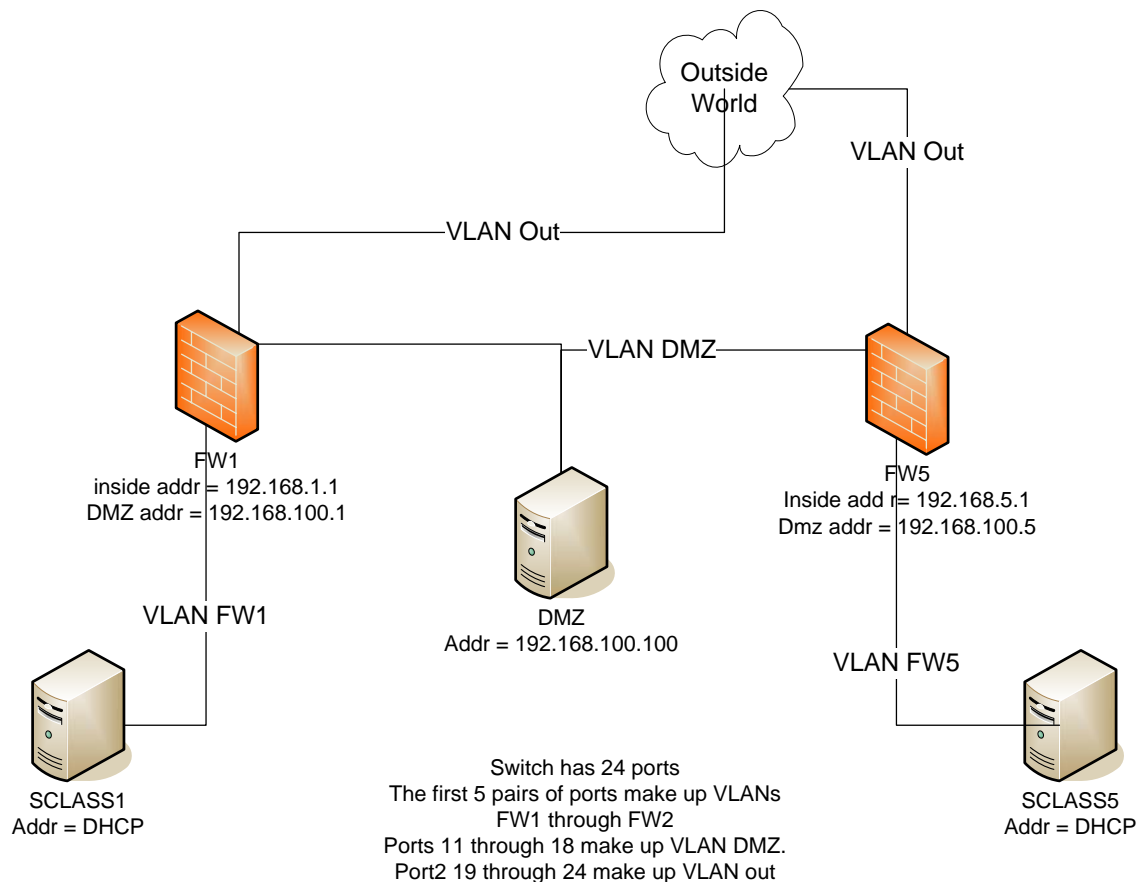


Figure 1: Lab configuration and addressing

Storing configs

There is a tftp server running on the DMZ machine (192.168.100.100). You will be able to save and reload your configurations to the DMZ server via TFTP. Use unique file names to avoid conflicts with other students.

The tftp directory on the DMZ machine is /boot. If you are writing a config, the file must exist in the directory and be world writeable. For example, if I wanted to save my config from PIX 3, I would go to the DMZ console and type

```
cd /boot/configs  
touch skh-config  
chmod 777 skh-config
```

From the PIX, I need to use the tftp-server command to indicate the address and interface of the server.

```
tftp-server dmz 192.168.100.100 configs
```

Then I can use the “write net” command to write my config to the tftp server.

```
write net :skh-config
```

When you are done with the firewall, you should issue the “reboot” command on the firewall to reload the base config in non-volatile memory.

When you are ready to work on this firewall the next time, you can use the config net command to reload your configuration. First, issue the “enable” command to get into privileged mode and the “config term” command to get into edit mode. Then you can issue:

```
config net :skh-config
```

For each firewall the tftp server has a base config in /boot/configs. fwX-base.cfg is a non-writeable copy of the base configuration for firewall X. The base config sets up the address translation and access lists to enable communication from inside to out and from inside to DMZ. Ping from inside to DMZ should also work (which required a short access list on the DMZ interface and a static address translation).

With this configuration, you should be able to ssh to the dmz machine to create and edit files in /boot/configs.

Configuring via HTTPS

The Pix Device Manager is installed on the firewalls. This is an embedded web browser interface that gives a GUI interface to the firewall configuration. Fw1-3 can be accessed from an applet via Internet Explorer by visiting <https://192.168.X.1>. Assuming you have the right version of the JRE installed (this is right on sclass2, still working on the others), another window will pop up and PDM will load up.

For Fw4 and 5, the applet is cached on the corresponding hosts and is launched via the ASDM launcher. Still working on getting the correct combination of browser and JRE loaded.

One difference with the device managers is that they write changes to non-volatile member on each page commit, so you cannot simply reload the firewall to remove your changes from the device. One way to remove your changes is to save your config to the TFTP server. Then edit the config to add “no” in front of all the access-list, address translation, and access-group commands and use “config net” to load the “no” config.

Testing Traffic

To verify that you are blocking java, try an outside site that use java, e.g., <http://java.sun.com/applets/>.

To try and access the inside from the outside, you can SSH to one of the machines from the common labs, e.g., csil-suna30.

Your tasks

You will need to perform the following tasks.

1. Configure the firewall based on the requirements specifications. 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 the firewall.
3. An example syslog entry from blocked traffic.
4. List three aspects of this configuration that you would not do in real life.