

Lab Exercise – Configure the PIX Firewall and a Cisco Router

Scenario

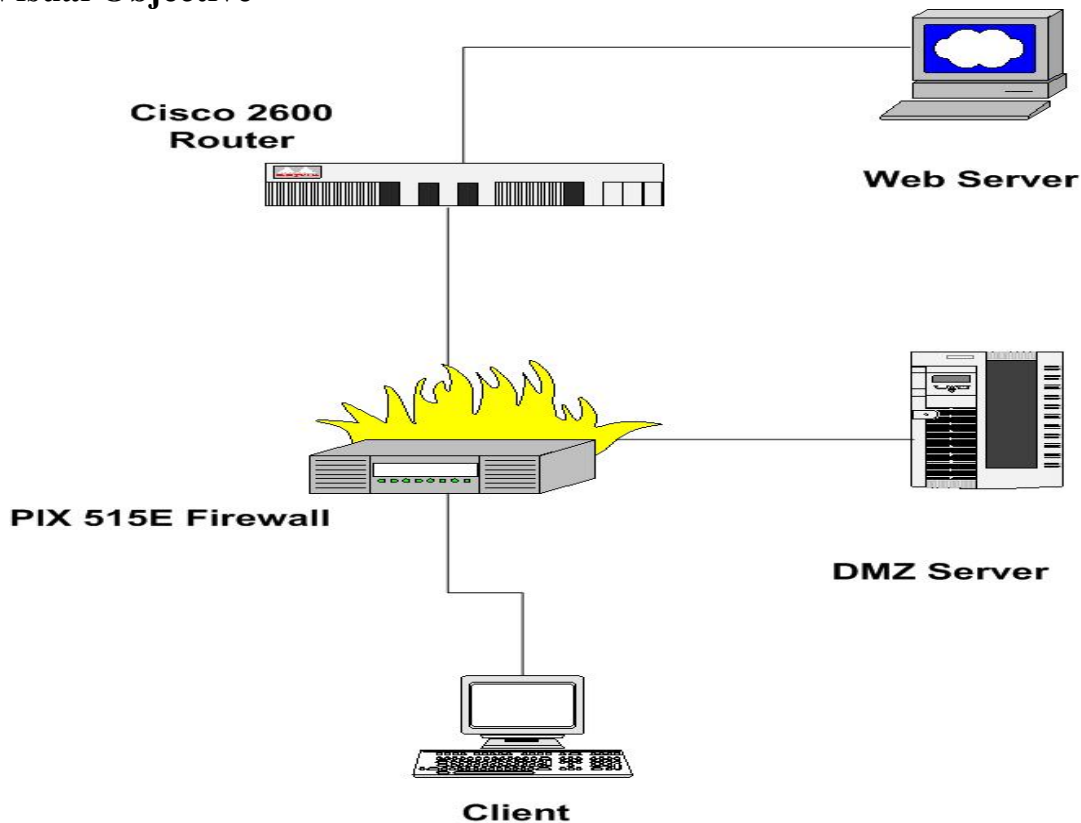
Having worked at Isis Network Consulting for two years now as an entry-level analyst, it has been your hope to move up the corporate ladder and take on new responsibilities. Your supervisor is still uncertain of your potential, but has presented you with a challenge. You along with your teammates will be assigned to setup and configure the network for a small tech firm looking to expand. As always, there will be specific objectives to meet as well as follow-up questions that need to be answered to prove your abilities. This is your moment to shine, don't let your boss down!

Objectives

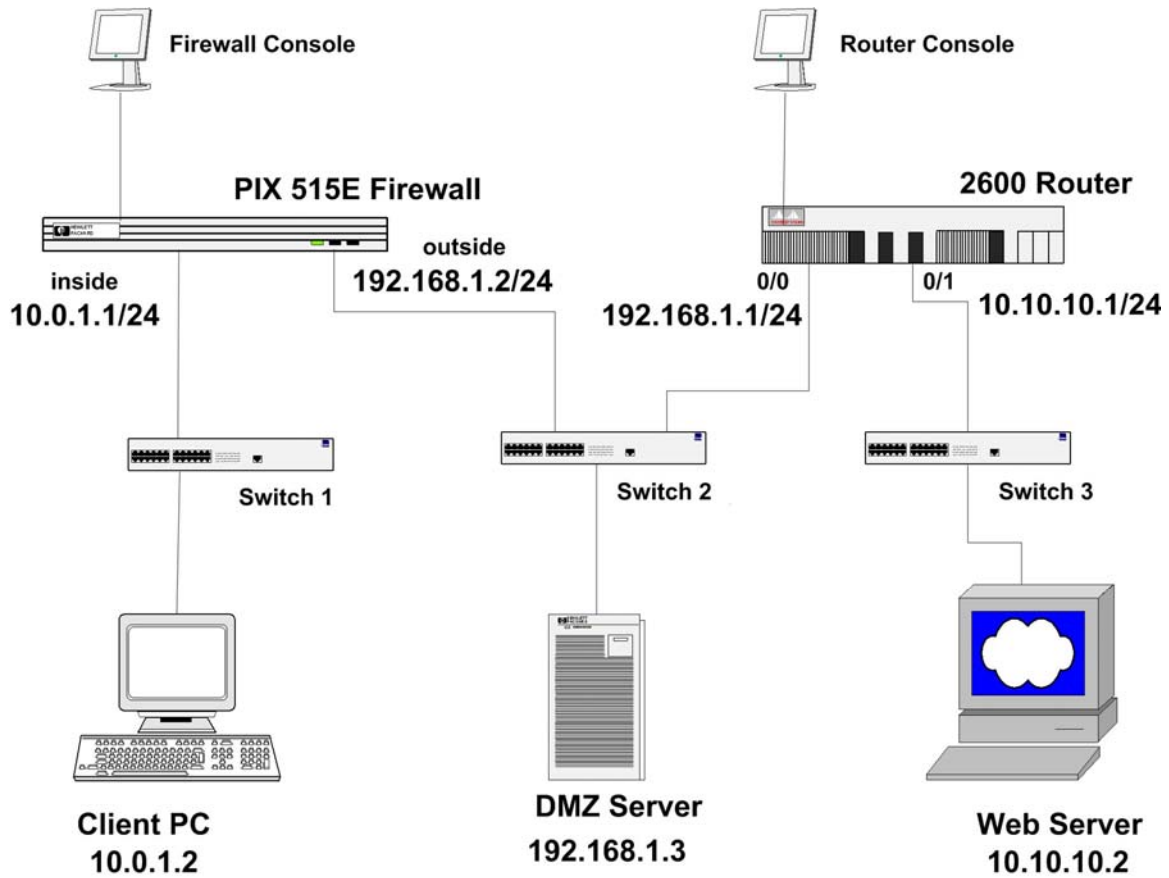
In this lab exercise you will complete the following three tasks:

- Task 1:
 - Setup the physical network with your group
- Task 2:
 - Configure basic PIX Firewall features to protect Internet access to an enterprise network
 - Configure a 2600 Router to prevent access to the DMZ Server from the outside Enterprise Network
 - Test and verify the basic PIX Firewall and the Cisco Router operation and configuration
- Task 3:
 - Disable Pinging to an Interface
 - Configure an Outbound ACL / Test and Verify the Outbound ACL

Visual Objective



Lab Setup Diagram



Lab Setup Diagram

	<i>contents</i>	<i>comments</i>
PIX/Router Password	cisco	OR no password
PIX outside interface e0	192.168.1.2	netmask: 255.255.255.0
PIX inside interface e1	10.0.1.1	netmask: 255.255.255.0
Router outside interface	192.168.1.1	netmask: 255.255.255.0
Router inside interface	10.10.10.1	netmask: 255.255.255.0
Console prompt	pix> OR pix# OR pix(config)#	pix> initial mode pix# enable mode pix(config)# configuration mode
Ctrl+Z	backward to previous mode	
PIX/Router console window	hyper-terminal	

Task 1 – Physical Network Setup

For the following task it is you and your group's duty to physically connect the network that will be used for the lab. Use the Lab Setup Diagram above to assist in the process.

Some areas to note:

- The DMZ server uses the 0/0 ports in the pix firewall and router while the client and web servers use 0/1 ports
- The firewall and router consoles are connected to their respective counterparts via serial cables
- For practicality reasons the client pc and the consoles may be the same machine to reduce equipment

Once completed, before continuing to task 2, have an instructor or a TA check over the connections for correctness.

Task 2 – Configure the PIX Firewall and a Cisco Router

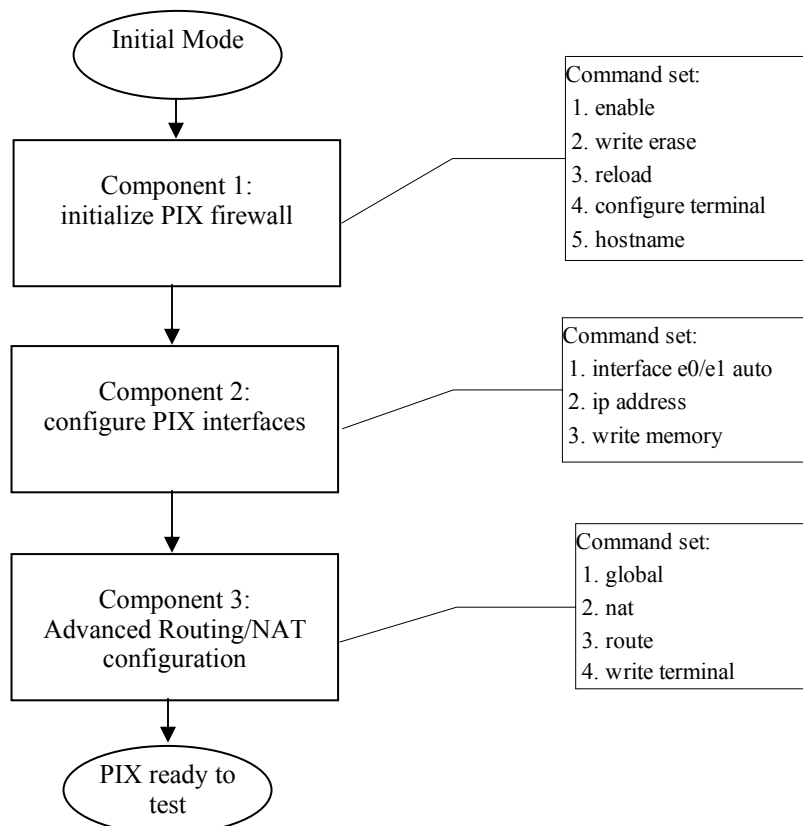
This task mainly consists of three sub-tasks. First of all, you need to configure basic PIX Firewall features to protect Internet access to an enterprise network. Second, you need to configure a Cisco 2600 Router to prevent access to the DMZ Server from the outside Enterprise Network. And last, you must test and verify the basic PIX Firewall and the Cisco Router operation and configuration, and adjust the configuration if you find something wrong.

Note: Cisco products are pretty consistent on their configuration interface, not only console/terminal interface but also graphic user interface (GUI). Through this entire lab exercises, we hope you

Task 2.1: Configure the PIX Firewall Interfaces

In this subtask, you will first learn several basic commands to get yourself familiar with Cisco network equipments. At this step, you are able to know how to initialize PIX firewall and switch between several working modes. Second, you will learn how to enable up the network interfaces (inside/outside) of PIX firewall and assign each an IP address. To let

Task overview



Command description

	<i>command</i>	<i>command usage</i>	<i>comments</i>
Initialize PIX	enable	Pix>enable	Switch pix to enable mode (pix#)
	write	Pix# write erase	Erase previous configuration to default
	reload	Pix# reload	Reload basic manufacture setup routine.
	configure	Pix# configure term	Switch pix to configurable status.
	hostname	Pix# hostname <i>name</i>	Change the hostname to <i>name</i>

	<i>command</i>	<i>command usage</i>	<i>comments</i>
Configure PIX interfaces	interface	Pix(config)# interface e0 auto	Enable ethernet0/1 interfaces for sensing 10/100 auto communication. No IP address at this moment.
	ip address	Pix(config)# ip address outside[inside] 192.x.x.x. 255.x.x.x	Assign IP address to the outside and the inside network interface.
	show	Pix(config)# show [interface ip address history ]	Show command is often used to verify current configuration, in order to find errors at early age.

	<i>command</i>	<i>command usage</i>	<i>comments</i>
Advanced PIX configuration	global	Pix(config)# global (outside) 1 192.x.x.20- 192.x.x.250 netmask 255.x.x.0	Global command builds up a global IP address pool to translate inside IP address into outside IP address, in order to let inner hosts access outside world.
	nat	Pix(config)# nat (inside) 1 0 0	Enable the IP address translation. In this lab, nat command allows inside hosts for outbound access.
	route	Pix(config)# route outside 0 0 192.x.x.1	Set up the route table to direct traffic to other network.
	write	Pix(config)# write memory	Record the current configuration to the flash memory in PIX.

Configure PIX step by step

- **Step 1:**

```
Pix>enable
Password: cisco
Pix#
```

→

```
Pix# write erase
Pix# reload
```

→

```
Pix>enable
Pix# configure term
Pix(config)# hostname pix
```

→ **Finish**

Note: After reload, pix firewall will go into basic manufacture setup routine. We do not want to use that routine. Thus, when you encounter the message “Preconfigure PIX firewall now through interactive prompts [yes]?”, **enter NO.**

- **Step 2:**

```
Pix(config)# interface e0 auto
Pix(config)# interface e1 auto
Pix(config)# show interface
```

→

```
Pix(config)# ip address outside 192.168.1.2 255.255.255.0
Pix(config)# ip address inside 10.0.1.1 255.255.255.0
Pix(config)# show ip address
```

→

```
Pix(config)# write memory
```

→ **Finish**

Note:

1. By default the interfaces are disabled. You must enable all interfaces you intend to use.
2. Use show command often to verify each important configuration operation.

a) show interface. (you should see)

```
interface ethernet0 "outside" is up, line protocol is up
hardware is i82559 ethernet, address is 0011.2040.2498 MTU 1500
bytes, BW 100000 Kbit full duplex
.....
interface ethernet1 "inside" is up, line protocol is up
```

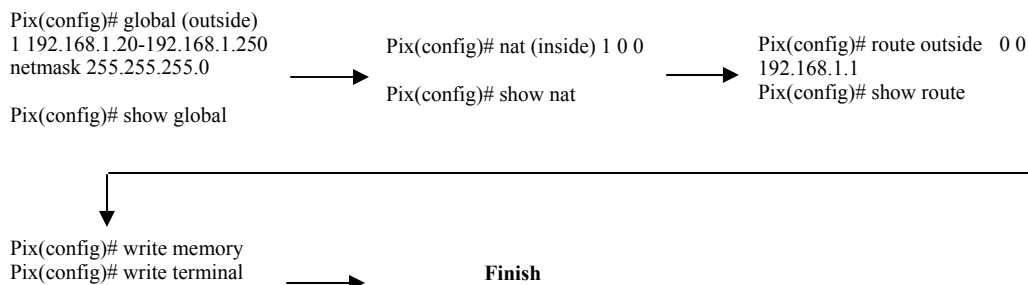
b) show ip address. (you should see)

```
System IP Addresses:
ip address outside 192.168.1.2 255.255.255.0
ip address inside 10.0.1.1 255.255.255.0
Current IP Addresses:
ip address outside 192.168.1.2 255.255.255.0
ip address inside 10.0.1.1 255.255.255.0
```

3. after write to memory, you should be able to see following message:

```
Building configuration...
Cryptochecksum: f0d9d025 7cfe9d97 c879550f cb74e78d
[OK]
```

• **Step 3:**



Note: The nat ID in command **global** and **nat** must match, in this case, it is **1**. This allows multiple nat ip pools within one PIX firewall.

After entering command show nat, you should see “1 0.0.0.0 0.0.0.0”.

After entering command show route, you should see:

```
outside 0.0.0.0 0.0.0.0 192.168.1.1 1 OTHER static
inside 10.0.1.0 255.255.255.0 10.0.1.1 1 CONNECT static
```

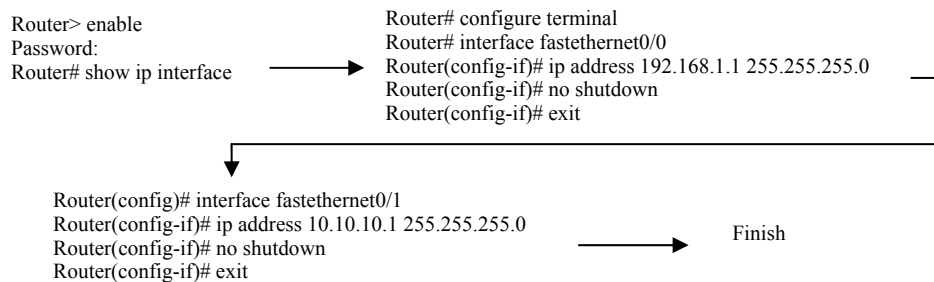
```
outside 192.168.1.0 255.255.255.0 192.168.1.2 1 CONNECT static
```

After entering command show terminal, you should see:

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

Task 2.2: Configuring the Router Port IP Connections

This is the final step which sets the external and internal router port IP numbers before a connection may be established.



Task 2.3: Verify the PIX Firewall Interfaces Configuration

To test the configuration of PIX interfaces and the operation of the global and nat statements by origination connections through PIX firewall, we need to verify using following test cases:

- a) Case1: Go to “Client PC” and open the IE web browser. Use the web browser to access the outside server at IP address 10.10.10.2 by entering <http://10.10.10.2>. If you are successful, the browser page will have a message like “**Hi This is the Outside Server!**”

Note: Observe the IP address translate table by using **show xlate**, you will see something like following:

```
1 in use, 1 most used
Global 192.168.1.20 Local 10.0.1.2
```

A Global Address chosen from the low end of the global range has been mapped to the inside client.

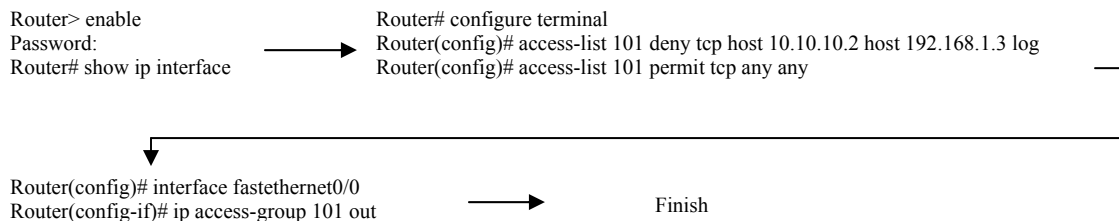
- b) Case 2: Go to the “**Web Server**” and open the web browser. Use the web browser to access the outside server at IP address 192.168.1.3 by entering <http://192.168.1.3>. If you are successful, the browser page will have a message like “**Hi This is the DMZ Server!**”.

Note: This activity is just to show the concept of a DMZ server and is not actually connected to a DMZ interface at the pix firewall or the any router.

Task 2.4: Configure the Router to prevent

Letting an outside host freely access inside server usually is not a desirable thing. In this task, we will learn how to setup access control rules for particular request using Cisco 2600 router. The interfaces are already configured on the router. We will only add an access-list and associate it with the interface **fastethernet0/0**. This will prevent access from the “**Web Server PC**” to the “**DMZ Server PC**”.

Configure ACL step by step



Verify that the IP Interface is correctly configured and the access-list has been now associated with the correct interface. Go to the “**Web Server PC**” and open the web browser. Use the web browser to access the outside server at IP address 192.168.1.3 by entering <http://192.168.1.3>. You will not be able to access the DMZ Server.

Note: Check the log buffer of the router to see the details of the connection that was denied. The log should look something like the following:

```

Log Buffer (11500 bytes):
Mar  2 03:37:11.629: %SEC-6-IPACCESSLOGP: list 101
denied tcp 10.10.10.2(0) -> 192.168.1.3(0), 3 packet
  
```

The log buffer shows that 3 tcp packets were denied because of the access list 101
This completes the lab.

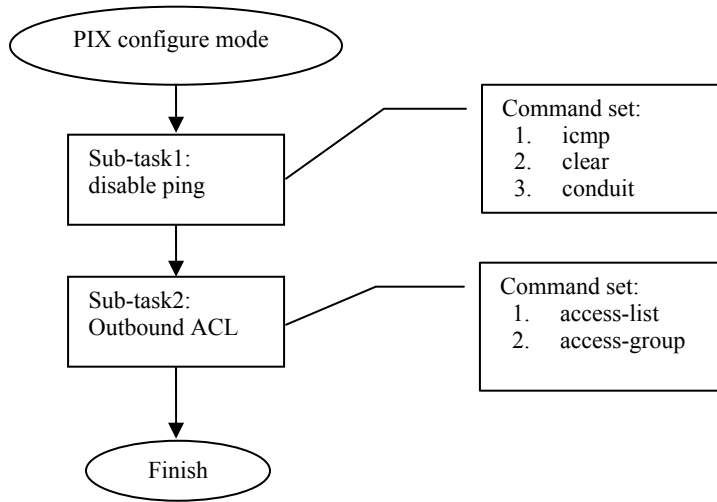
Task 3 – Configure advanced ACLs in PIX firewalls

The Access Control List (ACL) enables you to determine what traffic will be allowed or denied through the PIX Firewall. These lists are kept and may be adjusted to restrict outgoing or incoming traffic. Proper configuration of the Outbound and Inbound ACL will help maintain a safe network.

This task mainly consists of two sub-tasks:

- Disable ping to an interface
- Configure an Outbound ACL to limit traffic leaving the network

Task overview



Command description

	<i>command</i>	<i>command usage</i>	<i>comments</i>
Configure ACLs	icmp	Pix(config)# icmp [deny permit] any echo-reply inside	Deny or permit all ping requests at the inside interface
	clear	Pix(config)# clear icmp	Enable the IP address translation. In this lab, nat command allows inside hosts for outbound access.
	conduit	Pix(config)# conduit [permit deny] icmp any any echo-reply	Enable echo replies from the outside to the inside using conduit command
	access-list	Pix(config)# access- list ACLOUT permit tcp any any eq www	Create access list to allow the internal network to access Internet
	access-group	Pix(config)# access- group ACLOUT in interface inside	Add the access list to a group, and bind it to inside interface

Task 3.1: Disable Ping function to an interface

In this subtask, you will learn the process to disable ping within a network.

Ping is a feature used for network debugging. It sends out a short data burst – a single packet – and listens for a reply from the target. This can provide useful information about dropped, duplicated, or damaged packets. It also calculates the Round Trip Time (RTT), checking for the speed of the network. The ping feature is usually disabled on client PCs in companies. This is because hackers may use ping as a platform to launch Denial of Service attacks and flood the network.

Configure/Verify icmp step by step (On Client PC)

- **Step 1:**

On the command window to reach the DOS prompt (**Start->Run...-> Enter “cmd” as the program to Open**) and ping the inside interface of the PIX Firewall from the Client PC (10.0.1.2).

```
C:\> ping 10.0.1.1
```

Note: ping message will look like this:

```
Pinging 10.0.1.1 with 32 bytes of data:
Reply from 10.0.1.1: bytes=32 time<10ms TTL=255
...
Ping statistics for 10.0.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- **Step 2**

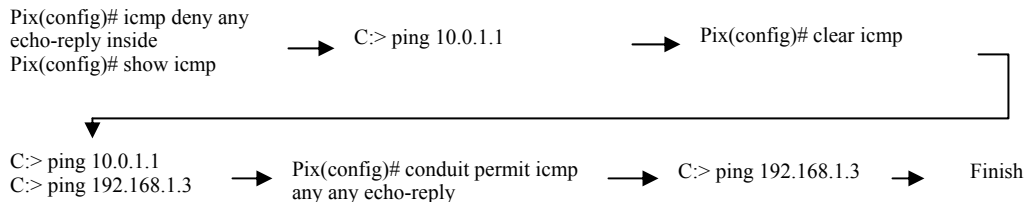
Ping outside interface of PIX firewall from Client PC (10.0.1.2). By default pinging through the PIX Firewall to a PIX Firewall interface is not allowed:

```
C:\> ping 192.168.1.3
```

Note: ping message will look like this:

```
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
```

- **Step 3:** deny all ping requests at the **inside** interface



Note: It is straightforward that whenever icmp is enabled the ping message will look like shown in step2, whenever icmp is disabled the ping message looks like:

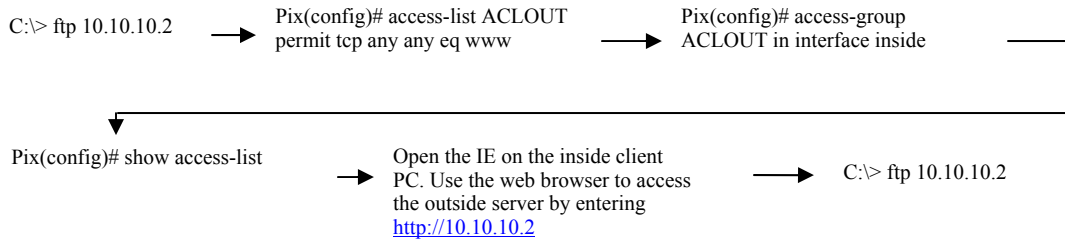
```
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
```

Task 3.2: Configure/Verify an outbound ACL

In this sub-task, you are asked to setup an outbound ACL that satisfies following requirements. On the first run TCP and IP requests will be allowed, on the second run TCP will be disabled but IP access to the web server is still allowed.

Configure/Verify ACLs step by step (On Client PC)

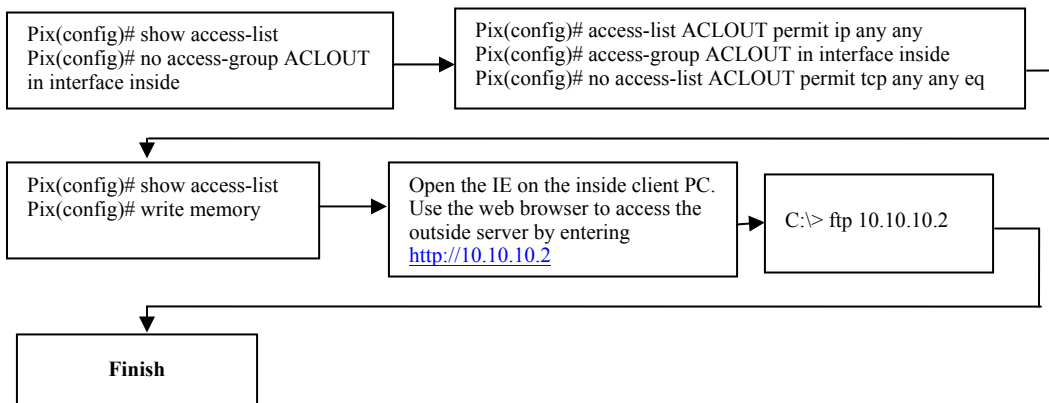
- **test 1:**



Note:

On the first run of ftp, you must be **able** to access the outside web server via FTP. After you setup the ACL, and access outside server via web browser, you can access. However, on the second run of ftp, the access will be denied due to implicit deny.

- **test 2:**



Note:

Still, you must be **able** to access the outside web server via web browser. However, you can access the outside server via FTP. Why?

Using command **show access-list**, carefully observe the response messages, for each usage, you may see something like:

```

    access-list ACLOUT; 3 elements
    access-list ACLOUT line 1 permit tcp any any eq www (hitcnt=1)
    access-list ACLOUT line 2 permit ip any any (hitcnt=0)
  
```

The denial prevents any ftp connections to be made through the client side.

Report to deliver:

The group report is to show what you did in the project. Please clearly state your results of this project. You are expected to hand in a report in the following formats:

- A cover page (including project title) with group name and group members
- A table of contents with page numbers
- Using double-spaced typing for convenient grading
- Hard copies only, Font size 12, Single column
- A bound or stapled document, with numbered pages

The report should have the following sections. Each section has multiple items. You need to write a report section by section that covers all required items. But you do not have to write the report item by item. Take screenshots if it is necessary.

Section I: Introduction:

You should have the following parts:

- Describe the goal and motivation of this project. In addition to what has been stated in the project instruction, please tell your own expectation in this project.
- Give an outline of this report, in which the content of each section needs to be briefly described.

Section II: Task 1

You should have the following parts:

- Briefly describe the concept of firewalls.
- Briefly describe the features that Cisco Pix firewall has and the technologies that Pix uses.
- Briefly describe the features of Cisco 2600 Router.

Section III: Task 2/Task3

You should have the following parts:

- Please describe how you construct the Network step by step in detail and in order. In order to show the detail of each step, for example, you need to describe which port of the switch you used, which interface in the router/pix you used, etc. You can take some snapshots of the screen to facilitate your description.
- After the Network is constructed, show the results you get from configuring the network. For example, what command you used, and what response you got? This may not be the same as you see in the lab document.

Section IV: Questions

You should answer the following 5 questions related to this lab (**single choice**):

1. Which of the following is **true**?
 - a. Interfaces with lower security levels can access higher security levels.
 - b. The outside interface has the highest security level
 - c. The outside interface can access the inside interface.
 - d. None of the above is true.
2. Command used to deny all ping requests at the inside interface is :
 - a. icmp deny any echo-reply inside
 - b. ping deny all echo-reply inside
 - c. All of the above.

- d. None of the above.
 3. The access-list command is used to create an access-list. What is/are the functions of the access-list?
 - a. Allow the internal network internet access.
 - b. Permit outbound IP Traffic
 - c. Permit inbound FTP access
 - d. All of the above.
 4. An access list named OUT that permits all outbound IP traffic is _____.
 - a. access-list OUT permit any any
 - b. access-list OUT permit ip 255.255.255.0 host 255.255.255.0 eq www
 - c. access-list OUT permit ip any any
 - d. None of the above.
 5. Static address mapping is used _____.
 - a. To creating a permanent mapping between a local IP address and a global IP address.
 - b. While accessing an interface of a higher security level from an interface of a lower security level.
 - c. To let in traffic from outside to inside network
 - d. All of the above.
- To answer above questions, you may need to refer to Cisco document: <http://www.cisco.com/> OR the book you can find in lab.

Section V: Experiment Log

This part should describe your activities in this project.

- Clearly state the responsibility of each group member. If possible, give a table to tell who did which task, who collected information of which device, who wrote which part of the report, who coordinated the group work activities, etc.
- Give a log of your group activity, such as what you did on which day, and how many people attend.

Grading Rubric

This project has a number of specific requirements. The requirement for each section is documented in the above project instruction “Report to deliver”. Whether you will get credits depends on the following situations:

- You will get full credits on one item, if it is correctly reported as required and well written.
- You will get half credits on one item, if it is reported as required but there is something definitely wrong.
- You will not get any credit for one item, if it is not reported.

The credits for each section are in the following. Each item in one section has equal credits.

1. Section I: Introduction (10%):

Each item has 5 credits.

2. Section II: Task 1(25%):

First two items have 10 credits each, the third item has 5 credits.

3. Section III: Task 2/Task 3 (30%):

Each item has 15credits.

4. Section IV: Questions (25%)

Each question has 5 credits.

5. Section IV: Experiment log (10%)

- If you are responsible for some parts of your group work, you get 10 credits. If you do nothing for your group work, you get 0.
- If you attend more than 90% of your group activities, you get 10 credits. If you attend between 70% and 90%, you get 7 credits. If you attend between 50% and 70%, you get 5. Otherwise, you get 0.

Note

This is a group project. Only hard copies of the report will be accepted. Be sure to include the names of all the teammates and email addresses in the report. The report should be turned in before class on the specified due date. Late grade will be deducted in case the submission is not made on time and prior permission is not obtained from the Dr Liu for submitting later than the specified due date.