

## HOW TO CONFIGURE CISCO FIREWALL – PART I

### Cisco

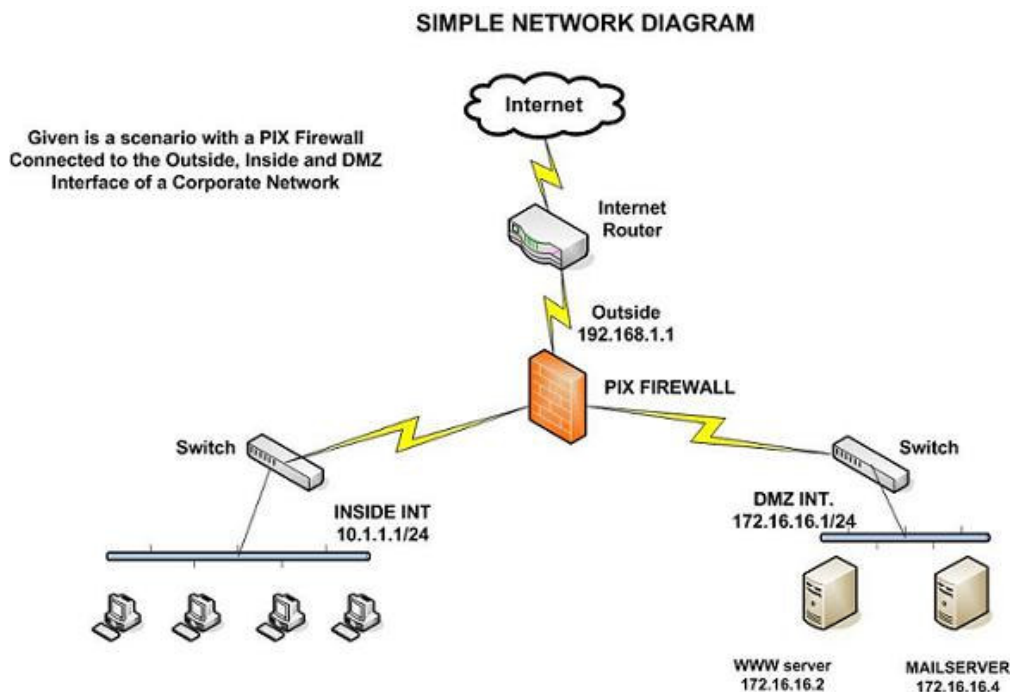
#### Abstract:

Please find below a step by step process to configure the PIX Firewall from scratch. A simple scenario is given here where you have a corporate network with a PIX Firewall connected to the Internet through the Outside Interface, Internal Network through the Inside interface and DMZ through the DMZ Network. This paper would assist you in a simple step by step, near complete configuration for a PIX Firewall running a midsized corporate network

Note: An effort has been made to keep this paper as simple as possible for the newbies. Much theory is not covered as you have numerous sites on the internet from where you can read that stuff.. Referral Links are given from time to time for more detailed configuration from Cisco website for Reference purpose.

The Outside Network is connected to the internet through a Internet Router. The Inside Network is connected to a switch to the Internal Clients or Inside Hosts. The DMZ network consists of two servers, the Web server and the WEB server.

#### A Simple Network Diagram



The first thing in configuration is getting connected to the pix firewall. You use the console cable to connect the cable to the console port of the pix firewall. The other end goes to the serial port of your computer. You can then use a terminal emulation software to get connected to the prompt. For Windows users, HyperTerminal is a good option.

### **The next step is booting the Firewall.**

When a non-configured PIX Firewall boots up, it prompts to preconfigure it through interactive prompts. If you press Enter to accept the default answer of yes, you are presented with a series of prompts that lead you through the basic configuration steps:

Pre-configure PIX Firewall now through  
interactive prompts [yes]? Enable Password []: abc123

Clock (UTC)  
Year [2002]:  
Month [Aug]:  
Day [2]: 12  
Time [2:45:37]: 12:22:00  
Inside IP address: 10.1.1.1  
Inside network mask: 255.255.255.0  
Host name: pixfirewall  
Domain name: secmanager.com  
IP address of host running  
PIX Device Manager: 101.1.111  
Use this configuration and write to flash? Y  
The above can also be achieved by entering the setup command in privileged mode.

The pix Firewall has four modes of Operation as given below:

- Unprivileged mode: This mode provides a restricted, limited, view of PIX Firewall settings. Example : pixfirewall>
- Privileged mode: This mode enables you change the current firewall settings. Example: pixfirewall#
- Configuration mode: This mode enables you to change the system configurations of the firewall. Example pixfirewall(config)#
- Monitor mode: This mode is used to update the image over the network, perform password recovery or backup the configuration onto the TFTP server

In case you don't want to use the setup command for the configuration, you can use the console connection and configure as follows:

## **Privileged mode**

The first step is to enter the privileged mode:

```
Pixfirewall> en  
Password: (Enter or Cisco, for more information refer to the configuration manuals  
that came with the firewall)  
Pixfirewall#
```

## **Changing password**

The next step is to change the enable password on the firewall:

```
Pixfirewall# enable password abc123
```

The next step is to enter the configuration mode for changing the system configurations. To enter the config mode, enter the following command:

```
Pixfirewall# configure terminal (or popularly conf t)  
Pixfirewall (config) #
```

## **Give a Hostname to the firewall.**

You might want to give a hostname to the firewall. You can use the hostname command to do this.

```
Pixfirewall (config) #hostname CorpFW1  
CorpFW1(config)#
```

To save the information, use the write memory command or simply `wr mem`.

```
CorpFW1(config)# write memory
```

For purposes of this document, we continue to give the firewall the name "Pixfirewall". So let us change the name back to Pixfirewall

```
CorpFW1(config)# hostname Pixfirewall  
Pixfirewall (config) # wr mem
```

## **Setup the console timeout:**

Next, you might want to setup the console timeout for security reasons. The default timeout is 0, which means unlimited.

Pixfirewall (config) # console timeout 5

This means you have setup a console timeout of 5 minutes ( the value can be set from 0-60 minutes) which means after a idle time of 5 minutes, the session will be closed.

### **Setup a banner to your Pix firewall.**

You can do this with the banner command:

Pixfirewall (config) # banner exec Unauthorized access will be prosecuted.

There are also two other commands available:

banner login  
banner motd

To remove banner you use the no banner or clear banner commands.

### **Naming an Interface:**

The first two interfaces would have the default names of inside and outside. While inside interface has a security level of 100, the outside interface has a default security level of 0.

Let us configure the Ethernet 2 interface as the dmz.

Pixfirewall (config) # nameif ethernet2 dmz sec60

In this example, we are assigning a security\_level of 60 to the DMZ network.

### **Configure the Interface:**

Now let us turn the interface on and configure the speeds for these interfaces:

Pixfirewall (config) # interface ethernet0 100full  
Pixfirewall (config) #interface ethernet1 100full  
Pixfirewall (config) #interface ethernet2 100full

### **Assign IP Address to the Interface:**

Pixfirewall (config) # ip address outside 192.168.1.1 255.255.255.0  
Pixfirewall (config) # ip address inside 10.1.1.1 255.255.255.0  
Pixfirewall (config) #ip address dmz 172.16.16.1 255.255.255.0

You can use the "show ip" command to view the ip address information and "clear ip" command to remove all assigned IP addresses from all interfaces.

### **Route Commands:**

Now let us setup the routing information on the pix firewall.

This is the default route, where we are configuring the next hop of the default route to the IP address of the Internet Router which is 192.168.1.100

```
Pixfirewall (config) # route outside 0.0.0.0 0.0.0.0 192.168.1.100 1
```

```
Pixfirewall (config) # route inside 10.0.0.0 255.0.0.0 10.1.1.1 1
```

```
Pixfirewall (config) # route dmz 172.16.17.0 255.255.255.0 172.16.16.1 1
```

So using these route commands you are telling the PIX router that route the traffic for 10.0.0.0/8 network to inside, 172.16.17.0/24 network to dmz. The default route is set for outside, which means for all other networks, route the traffic through the outside interface.