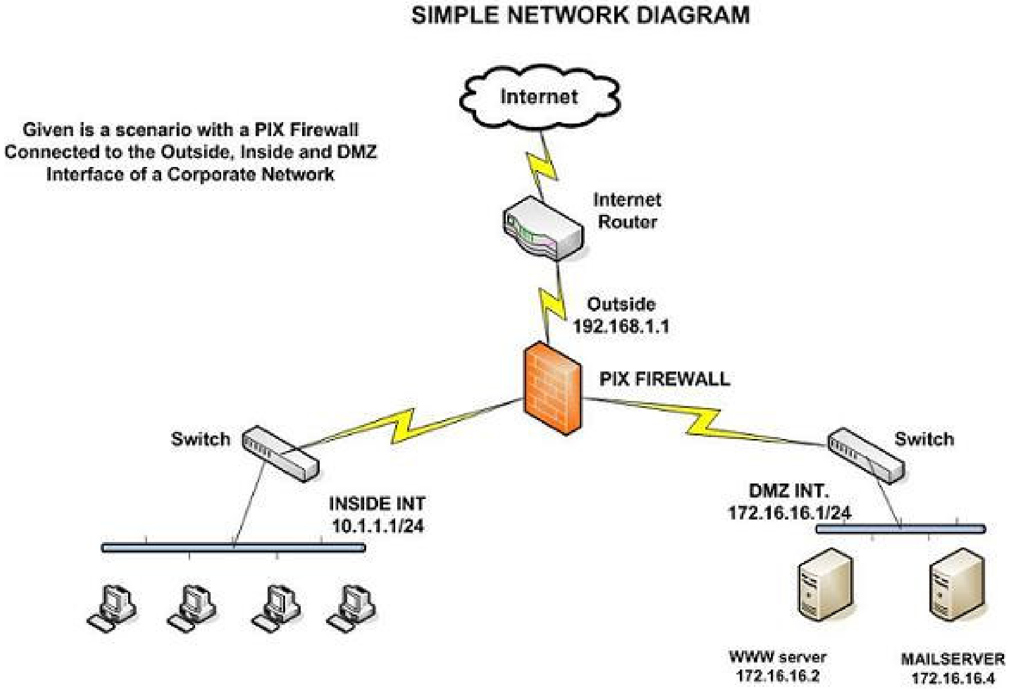
How to configure Firewall PIX

Parte II

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 Simple Network Diagram:



Network Address Translation:

Let us take a simple scenario to explain this section. Let us say that all the computers in the inside network want internet access. NAT also allows you to keep your internal IP hidden from the outside network. To achieve this you need to implement address translation. You do this using the “nat” and “global” commands.

The NAT command:

```
Pixfirewall (config) # nat (inside) 1 0.0.0.0 0.0.0.0
```

In this example, the nat (inside) 1 10.1.1.0 255.255.255.0 command means that all outbound connections from a host within the specified network, 10.1.1.0, can pass through the PIX Firewall (with address translation).

Global command:

```
Pixfirewall (config) #global (outside) 1 192.168.1.10-192.168.1.50
```

This means that use the IP address from 192.168.1.10 to 192.168.1.50 for NATing the traffic coming from the inside interface.

There is also another simple way for allowing internet /outside access to the inside network using PAT or port address translation. What this would do is hide all the internal networks behind the outside interface of the PIX firewall and transmit traffic using Port Address Translation. One limitation to this approach is that at a time it can process only less than 64000 client computers. But in most cases, this is more than enough.

PAT using Global:

```
Pixfirewall (config) # global (outside) 1 interface
```

Now, let us configure the two servers in the dmz network, the webserver and the mailserver. The wish list is to allow traffic from anywhere to reach the webserver on http, https and ftp and traffic from anywhere to reach the mail server on the smtp port.

To do this we need to setup statics and access-lists.

Setting up Static's:

```
Pixfirewall (config) #static (dmz,outside) 192.168.1.2 172.16.16.2
netmask 255.255.255.255 0 0
```

```
Pixfirewall (config) # static (dmz,outside) 192.168.1.4 172.16.16.4
netmask 255.255.255.255 0 0
```

Having configured the statics, now let us move on to configure the object-groups that would be used in configuring the access-list

Configuring object-groups:

```
Pixfirewall (config) #object-group service webservices tcp
Pixfirewall (config-service) # port-object eq http
Pixfirewall (config-service) # port-object eq https
Pixfirewall (config-service) # port-object eq ftp
Pixfirewall (config-service) # exit

Pixfirewall (config) #
```

Now let us configure the access-lists to allow access to the dmz networks from outside and also to the other interfaces:

Configuring Access-list:

```
Pixfirewall (config) # access-list external permit tcp any host
192.168.1.2 object-group webservices
```

```
Pixfirewall (config) # access-list external permit tcp any host
192.168.1.4 eq smtp.
```

```
Pixfirewall (config) #access-list external deny ip any any
```

(This is a any any drop rule. Place this at the end of the access-lists. This acl won't allow any other traffic that is not explicitly allowed to get into the firewall. This is often helpful in checking the number of hits on this acl from outside for troubleshooting or analysis purposes.)

```
Pixfirewall (config) #access-list internal permit ip 172.16.16.0
255.255.255.0 10.1.1.0 255.255.255.0
```

```
Pixfirewall (config) # access-list internal deny ip any any
```

```
Pixfirewall (config) # access-list dmz permit ip 10.1.1.0 255.255.255.0
172.16.16.0 255.255.255.0
```

```
Pixfirewall (config) #access-list dmz deny ip any any
```

Now map these access-lists to access-groups for these access-lists to work properly:

Configuring Access Groups:

```
Pixfirewall (config) #access-group external in interface outside
Pixfirewall (config) # access-group internal in interface inside
Pixfirewall (config) #access-group dmz in interface ethernet2
```

With this we have configured the PIX firewall for a normal office setup.

These commands will be helpful in checking the configuration of the pix firewall and also in troubleshooting, analysis and fine tuning.

Useful Commands:

```
show config
```

```
show blocks
show checksum

show conn

show cpu usage

show history

show memory

show processes

show routing

show running-config

show startup-config

show tech-support

show tcpstat

show traffic

show uauth/clear uauth

show version

show xlate/clear xlate
```

Note: There is a lot that you can do with the PIX firewall. This document is just a simple guide for a easy setup. It covers most popular setups. In case you need any further information please refer to Cisco website at http://www.cisco.com

Further reference:

Cisco PIX Firewall Command Reference, version 6.3
Getting Started document for more detailed information from the Cisco Website