PIX Introduction

Daniel B. Cid <daniel@underlinux.com.br>
http://www.ossec.net

What is a firewall?

A firewall is a tool used to prevent unauthorized access between two or more networks. Nowadays we have three kinds of firewall technologies:

-Access lists
-Stateful Inspection
-Proxy

*The PIX can use both of them.
*For more info about firewall technologies read the article “Firewall-intro.pdf”

What is PIX?

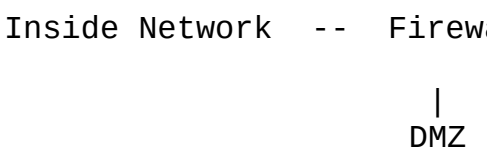
PIX is the Cisco Firewall, which uses a proprietary operating system called finesse. The four major advantages of the PIX are the embedded system (which is very "secure"), the ASA (Adaptive Security Algorithm), the cut-through proxy and the available options of redundancy.

Six models of the PIX Firewall are available:

Cisco PIX 501,506,515,520,525,535

Pre-Configuration:

Before start, we need to determine some things: All the examples here are going to use this network topology:



With these IP addresses:

Inside network 10.0.0.0/24 – Firewall inside IP: 10.0.0.1
DMZ network 172.16.1.0/24 - Firewall DMZ IP: 172.16.1.1
Outside IP: 200.1.1.1
Default route 200.1.1.2

In the DMZ we have an email server (IP 172.16.1.5) and an http server (IP 172.16.1.6).

Before Starting:

Before starting, we need to remember that on the PIX the ethernet0 is the Outside interface and the ethernet1 is the Inside interface. The Outside interface has a security level of zero and the inside of 100. All traffic from a lower level security interface to a high level security level is denied (unless allowed by an access list or conduit). Traffic from a high level security to a lower level security is always allowed (unless denied by an access-list).

Basic Configuration:

Setting the hostname (MYFW):

hostname MYFW

Naming the interfaces (the securityxx is the security level):

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 DMZ security30

Configuring the interfaces:

interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full

ip address ethernet0 200.1.1.1 255.255.255.0
ip address ethernet1 10.0.0.1 255.255.255.0
ip address ethernet2 172.16.1.1 255.255.255.0

Setting up PAT and the default route:

nat (inside) 1 10.0.0.0 255.255.255.0
nat (DMZ) 1 172.16.1.0 255.255.255.0

global (outside) 1 200.1.1.1 netmask 255.255.255.0
global (DMZ) 1 172.16.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 200.1.1.2

Redirecting smtp and www traffic to the DMZ

static (DMZ,outside) tcp 200.1.1.1 smtp 172.16.1.5 smtp netmask 255.255.255.255 0 0
static (DMZ,outside) tcp 200.1.1.1 www 172.16.1.6 www netmask 255.255.255.255 300 1000

*Where 300 is the max number of connections and the 1000 is the max number of half-open connection (embryonic).

Permiting access to the DMZ:

access-list 101 permit tcp any host 200.1.1.1 eq smtp
access-list 101 permit tcp any host 200.1.1.1 eq www
access-group 101 in interface outside

Enabling Protection against smtp attacks

fixup protocol smtp 25

*This command enables the Mail Guard, which restrict mail servers to receiving only seven commands defined in RFC 821. The commands are HELO, MAIL, RCPT, DATA, RSET, NOOP and QUIT)

Enabling Fragmentation Guard:

sysopt security fragguard

Enabling Logging

logging on (to disable, no logging)
logging host inside 10.0.0.10 (your log server)
logging trap information (the logging level)

Saving your configuration:

write memory