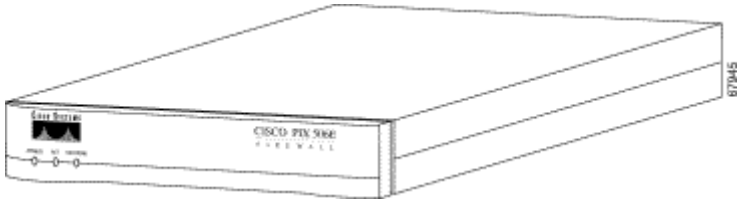
PIX Firewall의 설정

WOWHACKER (WOWCODE TEAM)
By Secret (secret@wowhacker.org)
http://www.wowhacker.org



1. PIX 방화벽에 대해서

Cisco Secure PIX Firewall 은 시스코 최고의 방화벽 제품이다. IOS 방화벽 기능 셋트는 가격이 민감한 고객 혹은 기업 네트워크 안에서 억세스를 차단하는 역할에 촛점이 맞춰져있고, PIX 는 시스코의 종합패키지로 오늘날 시장에서 주요 방화벽 제품들과 머리를 맞대고 경쟁하도록 나온제품이다. PIX 방화벽은 다음과 같은점에서 IOS방화벽과 차별화한다.

- 통합된 하드웨어/소프트웨어 : PIX 방화벽은 막중한 방화벽서비스를 위해 만들어진 하드웨어 플랫폼에서 동작하는 통합 패키지이다. 소프트웨어 패키지로만 제공되지않는다.

- 적응보안 알고리즘(ASA:Adaptive Security Algorithm) : PIX는 패킷 필터도 어플리케이션 프록시 방화벽도 아닌 고성능의 cut-through(메시지의 뒷부분이 도착하기전에 앞부분을 먼저 전달하는기술) 프록시 구조를 가진다.

- 통합된 VPN 옵션 : 삽입식 프로세서 카드로 IPSec(Internet Protocol Security) 암호화와 IKE(Internet Key Exchange)표준을 지원하는 가상 사설 네트워크를 설정할 수 있다.

네트워크 관리자들은 네트워크 보안에서의 요구에 부응하기 위해 시스코 Secure PIX 방화벽 같은 특정 목적에 맞춰진 장치쪽응로 돌아서고 있다. PIX 방화벽의 전자회로와 소프트웨어는 진보된 보안 기능과 고성능 작업량에의 요구 사이의 균형을 잘 맞추도록 되어 있다.
네트워크 기구와 방화벽이 가능한 라우터사이에서의 논쟁을 넘어서서 시스코는 경쟁사들의 유닉스 플랫폼기반의 방화벽에 대해서 실시간 내장 방식 PIX를 내놓고 있다. 시스코의 주장은 유닉스기반의 방화벽이 성능과 보안의 측면에서 그 값을 해야 한다는 것이다. 그런데 유닉스와 같은 범용 운영체제는 방화벽의 의무를 다하기에 부적절한 지연과 오버헤드만 아니라 그 자체에 해커들이 방화벽에 침입하기 위해서 이용할 수 있는 보안상의 헛점이 있다는것이다.

2. PIX 방화벽의 설정

1) 콘솔터미널의 사용

첫번째, 컴퓨터의 시리얼 포트와 PIX 방화벽의 시리얼 포트에 PIX 액세서리 킷트의 시리얼 케이블은 연결한다.
두번째, 터미널 접속용 프로그램(ex, 하이퍼터미널, Secure CRT)을 실행한다.
세번째, 새로운접속을 설정(직렬연결로 COM1 사용)
네번째, COM1에 관한 설정을 한다.
(9600 BPS, 데이터비트 8 , 패리티없음, 정지비트 1, 흐름제어는 하드웨어)
다섯번째, 방화벽으로의 시리얼연결 시작

2) 운영소프트웨어의 사용

- bh5xx.bin : 부트헬퍼 디스켓 생성 이미지
- pix60n.bin : 운영소프트웨어 이미지
- pfss6nn.exe : PIX Firewall Syslog Server(PFSS)
- rawrite : 이미지파일을 풀어 부트디스켓으로 생성
  * address 명령어는 PIX서버의 상주 IP주소
  * server 는 TFTP 서버의 IP주소
  * file 은 PIX 방화벽의 소프트웨어 이미지
  * gateway 는 게이트웨이가 필요로 할경우 사용

* ping 은 시스템의 ping 과 동일

예제)

```
Rebooting....
PIX BIOS (4.0) #47: Sat May 8 10:09:47 PDT 2001
Platform PIX-525
Flash=AT29C040A @ 0x300

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Flash boot interrupted.
0: i8255X @ PCI(bus:0 dev:13 irq:11)
1: i8255X @ PCI(bus:0 dev:14 irq:10)

Using 1: i82558 @ PCI(bus:0 dev:14 irq:10), MAC: 0090.2722.f0b1
Use ? for help.
monitor> addr 192.168.1.1

address 192.168.1.1
monitor> serv 192.168.1.2

server 192.168.1.2
monitor> file pix601.bin

file cdisk
monitor> ping 192.168.1.2

Sending 5, 100-byte 0x5b8d ICMP Echoes to 192.168.1.2, timeout is 4 seconds:
!!!!!
Success rate is 100 percent (5/5)
monitor> tftp

tftp pix601.bin@192.168.1.2.....
Received 626688 bytes

PIX admin loader (3.0) #0: Mon Aug 7 10:43:02 PDT 1999
```

Flash=AT29C040A @ 0x300

Flash version 6.0.1, Install version 6.0.1

Installing to flash

3) TFTP 다운로드 오류 코드

오류코드	설명
-1	PIX firewall 과 TFTP 서버의 timeout
2	이더넷 장치로부터 받은 패킷 길이가 유효한 TFTP 패킷 길이가 아니다.
3	받은 패킷이 서버에서의 SERVER 명령어에 의한 것이 아니다
4	IP 헤더의 길이가 유효한 TFTP 패킷 길이가 아니다.
5	받은 패킷의 IP 프로토콜 타입이 UDP가 아니다.
6	받은 패킷의 목적지 주소가 Address명령에 의한 주소와 일치하지않다.
7	대외적인 UDP 포트가 아니다
8	패킷의 UDP Checksum 계산이 틀렸다.
9	알수없는 TFTP 코드
10	TFTP 전송 오류
-10	입력한 이미지 파일을 찾을수없다. 퍼미션이나 파일의 존재유무를 확인하여라
11	시퀀스에 의해 TFTP패킷을 받았다.

잠깐) PIX소프트웨어 이미지는 시스코 웹사이트의 CCO user로 가입을 해야하며, http://www.cisco.com/register/ 에서 등록할수있다.
cco 사용자이름과 비밀번호를 가지고있다면, ftp클라이언트 프로그램으로 **cco.cisco.com** 으로 접속하여 소프트웨어 이미지를 다운로드받을 수가 있다.

4) 네트워크 라우팅의 설정

- PC를 이용하여, 콘솔이나 터미널을 이용하여 PIX 방화벽에 접속
- PIX방화벽에 접속했다면, 설정모드로 접근한다. **conf term** 명령어
- PIX방화벽의 ARP 케쉬를 초기화 한다. **clear arp** 명령어
- inside 인터페이스의 설정모드로 접근한다.
- PIX방화벽의 inside 인터페이스의 기본경로를 설정
  ip route 0.0.0.0 0.0.0.0 PIX inside IP주소
- show ip route 명령으로 게이트웨이의 목록 열람
- PIX방화벽의 ARP 케쉬를 초기화 한다. clear arp 명령어
- 기본 route가 변경되었다면, **write memory** 명령어로 플레쉬 메모리에

설정하고, clear arp 명령어로 케쉬를 초기화 하고 기본게이트웨이를 라우터로부터의 사용이 가능하도록 한다.

5) PIX 방화벽 설정의 시작

PIX 방화벽설정시에 언제나 **write terminal**명령어를 자주 사용한다.
이 write memory 명령어는 설정내용을 플레쉬 메모리에 저장하는것이다.

PIX를 설정하는데 있어서 2개이상의 인터페이스를 가지고 있다면 보안레벨을 위해서 **nameif** 명령으로 보안레벨설정을 할 수가 있다.

- 터미널 에뮬레이션 프로그램 시작
- PIX방화벽의 전원을 켠다
- PIX방화벽에 접속한다.
  Pixfirewall>
- 설정모드로 들어가기위해서 enable 을 입력하고 엔터를 친다.
  Pixfirewall> **enable**
  Pixfirewall#

- 인터페이스의 설정

새롭운 인터페이스를 설정하기 위해서는 nameif 명령어를 이용하여 인터페이스에 이름을 설정할 수가 있다.
그리고 interface 명령을 사용하여 각각의 인터페이스에 대한 사용을 가능하게 할 수가 있고, 인터페이스에 대한 고정 IP주소를 지정하기 위해서는 ip address 명령어를 사용하여 설정을 할 수가있다.

* nameif 명령어

nameif 명령어에 대한 설정은 nameif 명령어로 설정을 하고, show nameif 명령어로 설정한 내용을 열람할 수가 있다.

기본포멧은 다음과 같다.
(Nameif 하드웨어ID 인터페이스 보안레벨)

여기서 하드웨어ID부분은 ehternet0 또는 e0 으로 설정하여 사용할 수가 있고 인터페이스는 사용하는 인터페이스이름 그리고 보안레벨은 위에서 말한 보안레벨설정에 관한부분이며 security0 부터 security100 까지 설정이 가능하다.

그리고, 낮은 보안레벨의 인터페이스에서 높은레벨의 인터페이스로 접근하기위해서는 nat 명령어를 이용하여 구성을 할 수가 있다.

설정의예)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 perimeter security50

* ip address 명령어
ip 주소를 설정하기위해서 네트워크에 연결한 PIX방화벽의 각각의 인터페이스에 ip address 명령어를 사용하여 ip주소를 할당하여 설정할 수가 있다.

기본 포멧은 다음과 같다.
ip address inside ip주소 넷마스크
ip address outside ip주소 넷마스크

설정의 예)
ip address inside 192.168.1.1 255.255.255.0

설정내용의 열람은 다른 명령어들처럼 명령어 앞에 show를 이용한 show ip 명령어로 입력된 ip 명령에 대한 내용을 열람할 수가 있다.

* interface 명령어
PIX방화벽이 이더넷 인터페이스를 가지고 있다면, 기본적으로 모든 인터페이스들에 interface 명령어를 제공하는데, 만약 PIX방화벽이 기가비트 이더넷을 가지고있거나 FDDI 또는 토큰링 인터페이스를 사용할때는 이들에 대한 별도의 참고문헌을 이용하면 된다.

interface명령어에 대한 기본 포멧은 다음과 같다.
Interface 하드웨어ID 하드웨어속도 [shutdown]

설정의 예)
interface ethernet0 auto shutdown
interface ethernet1 10baset

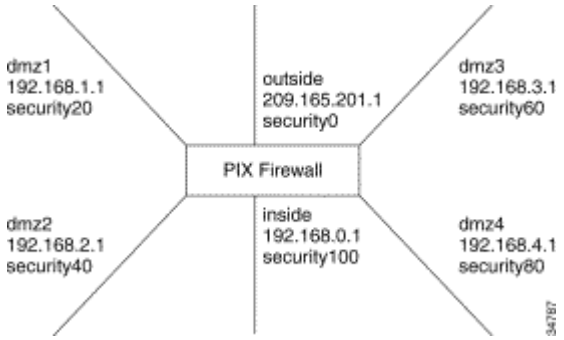
- 사용자들의 접속설정

이것은 nat 이나 global 이라는 명령어를 이용하여, 사용자들이 낮은 보안레벨의 인터페이스에서 높은레벨의 인터페이스등의 네트워크에접속가능하도록 설정을 하는것이며, 이미 설정되어있는 명령어를 열람하려면 show nat 또는 show global 명령어로 열람할수있고, 잘못설정하여 해당명령어를 삭제하려면 명령어 앞에 no를 붙혀서 명령문을 실행하면 해당명령어에 대한 삭제가 이루어진다. 이것은 터미널엥서 복사하고 붙혀넣기 방법을 이용하면 매우 쉽게 할 수가이었다. 그리고 show nat 이나 show global명령어를 이용해서 잘못입력된 명령어에 대한 삭제가 이루어졌는지여부를 다시한번 확인을 한다.

참고로 NAT를 사용하지않으려면 nat 0 명령어를 사용하면된다.

첫번재, 우선 show nameif 명령어를 사용하여 인터페이스들의 보안레벨 및 구성을 열람한다.

두번째, 그리고 네트웍구성을 간단하게 스케치 해본다.



(참고 그림)

세번재, nat 명령어로 낮은레벨의 원하는 사용자가 높은레벨로 접근허용할수 있도록 구성한다.

* inside 사용자가 낮은레벨의 인터페이스로 접속

nat (inside) 1 0 0 명령어

* dmz4사용자가 낮은레벨의 인터페이스나 dmz3,dmz2 ,dmz1 또는 outside 로 접속

nat (dmz4) 1 0 0 명령어

* dmz3사용자가 낮은레벨의 인터페이스나 dmz4,dmz2,dmz1 또는 outside 로 접속

nat (dmz3) 1 0 0 명령어
* dmz2 사용자가 낮은레벨의 인터페이스나 dmz1 과 outside로 접속
nat (dmz2) 1 0 0 명령어
* dmz1 사용자가 outside로 접속
nat (dmz1) 1 0 0

여기서 , 0 0 은 모든 호스트를 정의한다고 말하는것이다.

다른 예제로 오직 192.168.2.42 에서만 dmz2 인터페이스에 접속할수있게 하려면,
nat (dmz2) 1 192.168.2.42 255.255.255.255
라 한다.

여기서 1은 NAT ID 이며, 위에서 말했듯이 NAT ID 가 0 이면 사용하지않음을 이야기하는것이다.

nat명령어와 유사하게 사용할수있는 것은 global 명령어가 있는데, 이것은 nat과 유사하나, 광대역적인 주소를 사용할수 있다는 점이 다르고, 총 65535개의 호스트부터 , 단 한 개의 호스트가지 사용이 가능므로 nat 명령어보다는 더 효율적인 설정이 가능하다.

설정의 샘플을 보면, 다음과 같다.
global (outside) 1 209.165.201.5 netmask 255.255.255.254
global (outside) 1 200.165.201.10-209.165.201.20 netmask 255.255.255.254

이것은 global명령어로 outside의 사용자가 inside나 dmz1, dmz2등에 대해서 접속이 가능하게 하는것이며, IP에 대한 지정 및 IP대역에 대한 지정을 global명령어로 설정을 한것이다.

또한가지의 예를 들자면, 10.1.0.0/16의 호스트들은 192.168.1.1로 맵핑되고 10.1.1.1/16의 호스트들은 209.165.200.235로 맵핑이 되는것이다.

예)
nat (inside) 1 10.1.0.0 255.255.0.0
nat (inside) 2 10.1.1.1 255.255.0.0
global (outside) 1 192.168.1.1

global (outside) 2 209.165.200.235

- 기본라우터의 설정
route명령어로 outside route의 기본 라우터를 설정할 수가 있고, 다른 명령어들처럼 show route 명령어로 설정내용을 열람할수도 있고, no route로 route설정을 삭제할수도 있다.
만약 outside 라우터의 주소가 209.165.201.2라면 다음과 같이 하면 될것이다.
route outside 0 0 209.165.201.2 1

이 명령어는 기본라우터가 외부에 있다는 것을 말해주는것이며, 여기서 0 0은 IP주소의 0.0.0.0 과 netmask의 0.0.0.0 을 말하는것이고, 끝에 1은 라우터가 PIX방화벽으로부터 있는 홉의 숫자이다.

- PIX방화벽과 네트워크 라우팅의 설정
PIX방화벽이 인트라넷에 존재할 때, 10.3.1.0의 내부 네트워크를 가지고 있으며 10.42.1.0의 외부네트워크를 구성했다고 가정할 때 10.3.1.0의 네트워크로 192.168.1.0이 접근이 가능하도록 원한다고 한다. 이때 10.3.1.0 네트워크로 이사용자들의 접근이 가능하게 하기위해서는 static 명령어를 사용하여 다음과 같이 먼저 설정을 한다.
static (inside, outside) 10.42.1.0 10.3.1.0

그리고, PIX방화벽은 라우터가 아니기 때문에, 근거리통신망으로 트래픽을 관리하기위해 route명령어들의 구성이 필요하다.
route inside 10.3.1.0 255.255.255.0 라우터까지의 홉수

또, 외부 네트워크의 트래픽 라우터도 설정하기위해, 그 네트워크에 대한 route명령어를 사용하여 네트워크에 대한 접근을 할수있도록한다.
route outside 192.168.1.0 255.255.255.0 라우터까지의 홉수

- PING 서비스의 사용제한
access-list 명령어를 사용하여 호스트로부터의 ping 서비스를 제어할수가 있다. Ping 서비스는 ICMP 응답메세지를 전송하는 방법으로 사용하는것이기 때문에 즉, icmp에 대한 제어가 필요하다.

여기서 한가지 참고할 것은 일반적인 DoS공격에서 icmp패킷을 대량으로 전송하여 시스템에 부하를 주어 서비스에 대한 거부를 만들어줄수있는 공격들에 대한 간단한 방어법으로 icmp패킷을 차단하는 방법도 한가지의 방법이다.

* ping 사용의 설정
access-list 명령어를 사용하여 ICMP 억세스를 허가한다.
access-list acl_out permit icmp any any

acl_out은 access-list명령어이며, 사용자가원하는 아무이름으로든 설정이가능하며, 이것또한 show access-list 명령어로 열람이 가능하다.
그다음으로 ICMP패킷을 전달하기 위해서 PING이 가능하기를 원한 각 인터페이스에 access-group 명령어를 꼭! 설정해야한다.
즉, access-list 명령어와 access-group명령어를 연관시켜야 한다는것이다.
access-group acl_out in interface outside

그리고, 다음 명령문들로 하여금 내부 인터페이스에 까지 PING이 가능하도록 할수도있다.
access-list acl_dmz1 permit icmp any any
access-group acl_dmz1 in interface dmz1

access-list acl_dmz2 permit icmp any any
access-group acl_dmz2 in interface dmz2

access-list acl_dmz3 permit icmp any any
access-group acl_dmz3 in interface dmz3

access-list acl_dmz4 permit icmp any any
access-group acl_dmz4 in interface dmz4

그리고, access-list 명령을 내린 것을 삭제하기 위해서는 no를 앞에 붙혀서 다음과 같은 명령어를 사용하여 제거 할수있다.
no access-list acl_in permit icmp any any
no access-list acl_out permit icmp any any
no access-list acl_dmz1 permit icmp any any
no access-list acl_dmz2 permit icmp any any

no access-list acl_dmz3 permit icmp any any
no access-list acl_dmz4 permit icmp any any

access-list 명령은 conduit 명령으로 대신할수있는데, 이방법이 사실상 더 편리하다.

내부에서 외부의 어디라도 ping서비스를 가능하도록하려면
conduit permit icmp any any

conduit 명령의 삭제는
no conduit permit icmp any any

다른것과 마찬가지로 no를 앞에 입력하면된다.

또한 conduit 명령으로 설정된내용을 열람하기 위해서는 다른것과 마찬가지로 show conduit 명령문으로 열람이 가능하다.

* PING 인터페이스의 설정으로 PING 허가 또는 거부
이것은 icmp 명령어로 직접 허가 또는 거부를 할 수가 있는 방법이며,
기본적은 포멧은 다음과 같다.

icmp permit | deny [host] src_addr [src_mask] [type] int_name
no icmp permit | deny [host] src_addr [src_mask] [type] int_name
clear icmp
show icmp

여기서
permit : 허가
deny : 거부
int_name : 인터페이스 이름
을 말한다.

- 플레쉬 메모리의 복구 또는 재부팅
write memory 명령어로 저장 되었된 플레쉬 메모리로의 복구나 방화벽의 시스템 재부팅은 reload 명령어로 하면 된다.

- Telnet 콘솔 접속의 설정
이것은 보다많은 설정 접속을 하기위해서 접속의 편리함과 많은 사용자들로부터의 접속 서비스를 허가시키기 위해서 telnet 포트로의 telnet 접속기능을 사용하여 콘솔로 접속할 수 있는 기능이다.

예) 내부의 192.168.1.2 로부터의 PIX telnet 콘솔접속설정
telnet 192.168.1.2 255.255.255.255 inside

또, 외부의 209.165.200.255 IP로부터의 PIX telnet 콘솔접속은 다음과 같다.
telnet 209.165.200.255 255.255.255.254 outside

참고로, telnet session 의 timeout에 대한 설정은 다음명령어로 설정하면 된다.
telnet timeout 15

telnet 콘솔 접속의 보안을 위해서는 인증서버와 함께 **aaa authentication telnet console** 명령어를 사용하여 보호를 할 수가있다.
이때 콘솔에 접속할때의 사용자이름은 **pix** 이며, 비밀번호는 enable passwd 명령어로 설정할수가있다.

TELNET 콘솔 접속 테스트)
telnet 192.168.0.1
PIX passwd :

기본적인 비밀번호로 CISCO를 입력하거나 비밀번호가 없으면 그냥 엔터를 치면 접속이 가능하고, 혹은 미리정의된 비밀번호를 입력하면된다.

* 외부인터페이스로부터의 텔넷 접속 보안
외부 인터페이스로부터의 텔넷접속 암호화를 위해서 다음 예제처럼 설정을 할 수가있는데, 외부인터페이스의 주소는 168.20.1.5 이고, VPN클라이언트의 IP주소가 10.1.2.0 라고 할 때,
access-list 80 permit ip host 168.20.1.5 10.1.2.0 255.255.255.0
telnet 10.1.2.0 255.255.255.0 outside

위와 같이 설정하고, VPN 클라이언트와 PIX방화벽의 보안정책 설정을 똑같

이 설정하면 된다.

- Inbound 서버 억세스 설정
PIX방화벽은 외부로 부터의 모든 내부 접속을 기본적으로 차단하는데, 이것은 static, access-list, 그리고 access-group 명령어들을 이용하여, 접속을 허가할 수가 있는것이다.

* static
static 은 보안등급이 낮은 인터페이스의 사용자들이 보안등급이 높은 인터페이스의 서버에 접근하기 위하여 사용하는 IP Address를 제공것이며, 기본 포멧은 다음과 같다.
static (high_interface,low_interface) low_address high_address **netmask** netmask

위 기본 포멧의 괄호안에는 2개의 인터페이스를 지정하여야 한다. 항상 보안등급이 높은 high_interface를 앞쪽으로 지정하여야한다. 등급이 낮은 인터페이스는 그 뒤에 위치하여야한다.

예를들어 외부 인터페이스와 특정서버(예, dmz3)가 있을 때, dmz3가 외부인터페이스보다 더 우선적으로 보안등급이 높아야하므로, (dmz3, outside)를 사용해야한다.

뒤에 있는 2개의 파라미터는 IP주소에 대해서 지정한다. High_address의 접근을 위해서 low_address 서버주소를 지정하여야 하며, high_address는 서버의 실제 IP주소를 말하는것이다.

예)
static (dmz3,outside) 209.165.201.3 192.168.3.3 netmask 255.255.255.255

* access-list
access_list 는 사용권한들을 정의 하는것이며, 어떠한 포트에 접근을 허락하는지, 어떠한 IP들을 접근가능하게 하는지에 대한 정의하는 것이다.
이 access-list의 기본포멧은 다음과 같다.
access-list ID action protocol source_address port destination_address port

(파라미터설명)
id : 리스트명령문들의 그룹을 식별하기위한 것

action : 허가 또는 거부에 대한 정의 (허가: permit, 거부: deny)

protocol : 관련 프로토콜 (일반적으로거의 tcp 이다.)

source_address : 상대의 호스트로부터 접근을 허락하기위해 상대의 IP주소를 입력한다. 모든 호스트에 대한 부분은 any 이다. 이때 네트워크 주소를 지정한다면, 네트웍 넷마스크도 지정해준다.
네트워크주소지정의 예)
192.168.1.0 255.255.255.0

Destination_address : static 명령어를 사용하여 지정한 호스트의 주소를 말하며, 이 파라미터 또한 모든 호스트에 대한부분은 any 이며, 호스트 지정시 네트웍 넷마스크도 지정해준다.

Port : 포트는 말그대로 해당 서비스의 포트번호

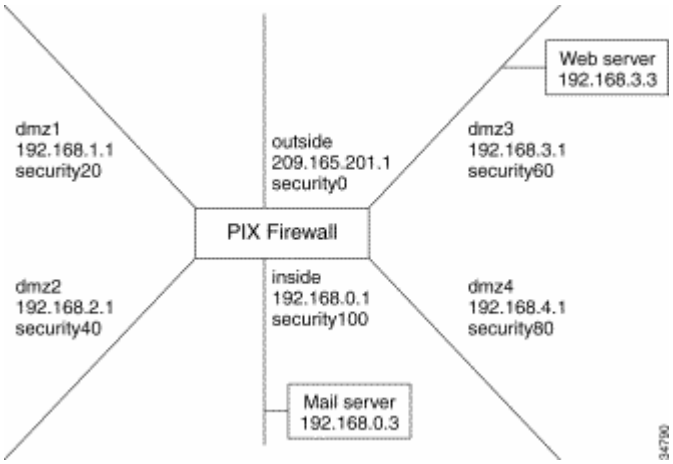
예제)
209.165.201.3 에서 192.168.3.3 으로의 inbound 접속을 허가하고,
access-list 에는 80번 포트인 웹서비스의 허가를 하는 룰을 설정.

static (dmz3,outside) 209.165.201.3 192.168.3.3 netmask 255.255.255.255
access-list acl_out permit tcp any host 209.165.201.3 eq www

* access_group
이 명령어는 서로 연관있는 명령을 그룹화 하는것이며, 명령어의 포멧은 다음과 같다.
access_group ID in interface low_interface

위의 기본포멧에서 ID는 access_list 명령어에서 사용된 ID값과 동일하다.
static (dmz3,outside) 209.165.201.3 192.168.3.3 netmask 255.255.255.255
access-list acl_out permit tcp any host 209.165.201.3 eq www
access-group acl_out in interface outside

설정의 예)



(네트웍 구조 스케치)

외부에서 내부의 메일서버로 접속가능하게 하는 명령

static (inside,outside) 209.165.201.4 192.168.0.3 netmask 255.255.255.255

access-list acl_out permit tcp any host 209.165.201.4 eq smtp

access-group acl_out in interface outside

두개의 access-list 명령어 사용하여, PPTP 전송 프로토콜과 GRE 프로토콜의 설정

static (dmz2,outside) 209.165.201.5 192.168.1.5 netmask 255.255.255.255

access-list acl_out permit tcp any host 209.165.201.5 eq 1723

access-list acl_out permit gre any host 209.165.201.5

access-group acl_out in interface outside

dmz1의 사용자가 메일서버의 inside 인터페이스로 접근

static (inside,dmz1) 192.168.1.4 192.168.0.3 netmask 255.255.255.255

access-list acl_dmz1 permit tcp any host 192.168.1.4 eq smtp

access-group acl_dmz1 in interface dmz1

dmz2의 사용자가 메일서버로 접근

static (inside,dmz2) 192.168.2.4 192.168.0.3 netmask 255.255.255.255

access-list acl_dmz2 permit tcp any host 192.168.2.4 eq smtp

access-group acl_dmz2 in interface dmz2

dmz3의 사용자가 메일서버로 접근

static (inside,dmz3) 192.168.3.4 192.168.0.3 netmask 255.255.255.255

access-list acl_dmz3 permit tcp any host 192.168.3.4 eq smtp

access-group acl_dmz3 in interface dmz3

dmz4의 사용자가 메일서버로 접근

static (inside,dmz4) 192.168.4.4 192.168.0.3 netmask 255.255.255.255

access-list acl_dmz4 permit tcp any host 192.168.4.4 eq smtp

access-group acl_dmz4 in interface dmz4

외부의 사용자가 dmz3의 웹서버에 접근

static (dmz3,outside) 209.165.201.3 192.168.3.3 netmask 255.255.255.255

access-list acl_out permit tcp any host 209.165.201.3 eq www

access-group acl_out in interface outside

dmz1의 사용자가 웹서버로 접근

static (dmz3,dmz1) 192.168.1.3 192.168.3.3 netmask 255.255.255.255

access-list acl_dmz1 permit tcp any host 192.168.1.3 eq www

access-group acl_dmz1 in interface dmz1

dmz2의 사용자가 웹서버로 접근

static (dmz3,dmz2) 192.168.2.3 192.168.3.3 netmask 255.255.255.255

access-list acl_dmz2 permit tcp any host 192.168.2.3 eq www

access-group acl_dmz2 in interface dmz2

dmz4의 사용자가 웹서버로 접근, nat 그리고 global 명령어를 사용하여 dmz4의 사용자들이 높은 보안 레벨의 인터페이스인 dmz3로 접속.

nat (dmz4) 1 192.168.4.0 255.255.255.0

global (dmz3) 1 192.168.3.10-192.168.3.100 netmask 255.255.255.0

inside 사용자들의 접근

nat (inside) 1 192.168.0.0 255.255.255.0

- 아웃바운드 억세스 설정
이 설정은 사용자들로 부터 아웃바운드 의 억세스 허가 또는 거부에 대한 설정을 말하며, 기본포멧은 다음과 같다.

access-list ID action protocol source_address src_port destination_address dest_port

파라미터의 설명은 다음과 같다.
id : 리스트명령문들의 그룹을 식별하기위한 것

action : 허가 또는 거부에 대한 정의 (허가: permit, 거부: deny)

protocol : 관련 프로토콜 (일반적으로거의 tcp 이다.)

source_address : 상대의 호스트로부터 접근을 허락하기위해 상대의 IP주소를 입력한다. 모든 호스트에 대한 부분은 any 이다. 이때 네트워크 주소를 지정한다면, 네트웍 넷마스크도 지정해준다.
네트워크 주소지정의 예)

10.1.2.0 255.255.255.0

만약 같은 계열의 IOS 소프트웨어를 사용한다면, 0.0.0.255 값을 사용한다.

Destination_address : static 명령어를 사용하여 지정한 호스트의 주소를 말하며, 이 파라미터 또한 모든 호스트에 대한부분은 any 이며, 호스트 지정시 네트웍 넷마스크도 지정해준다.

Port : 포트는 말그대로 해당 서비스의 포트번호

이 아웃바운드에 대한 설정은 inbound대한 설정을 참고로 하여 설정하면된다. 왜냐하면 inbound와 outbound의 설정방법이 동일하기때문이다.
.
설정의 예)
내부네트웍 사용자들의 외부 특정사이트의 접근을 차단 즉, 특정사이트에 대해서만 outbound 를 차단

access-list acl_in deny tcp any host 209.165.201.29 eq www

access-group acl_in in interface inside

dmz2의 192.168.2.0에서 dmz1인 192.168.1.0의 다른 어떠한 서버로의 접근을 차단

access-list acl_dmz2 deny tcp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0

access-group acl_dmz2 in interface dmz2

- 필터링 기능의 설정

* 자바필터링

이것은 웹서비스중에 java 언어에 대한 필터링으로 java로 보통 자바에플릿에 대한 필터링으로 주로 사용된다. java애플릿으로 인한 내부자료의 유출등 보안상문제가 많아 많이 설정을 하는 추세이지만, 웹서핑시에 사용자는 많은 불편함이 있을수가있다.

설정의 예로 모든 웹서비스에 대한 java 필터링을 하는 샘플설정이다.

filter java 80 0 0 0 0

* url 필터링

url필터링은 특정 ip나 특정 서버등에 대한 필터링작업으로 통제를 할 수 있는 필터링이다. 응용설정으로 특정웹사이트에 대한 접근 통제를 할 수가이었다.

설정의 예로 10.0.2.54가 기본이 되는 웹연결을 제외한 모든 아웃바운드연결을 필터링하는 샘플설정이다.

url-server (perimeter) host 10.0.1.1

filter url http 0 0 0 0

filter url except 10.0.2.54 255.255.255.255 0 0

- syslog의 사용 설정

*syslog 메시지 레벨

레벨번호	이름	메시지 타입
0	**Emergencies**	쓸모없는 메시지
1	**alerts**	직접작업 요청 메시지
2	**Critical**	경계 상태 메시지
3	**Errors**	오류 메시지
4	**Warnings**	경고 메시지

5	**Notification**	평균 상태 메시지
6	**Informational**	정보 메시지
7	**Debugging**	디버깅, FTP명령어, WWWurl 디버그

Syslog는 syslog 서버에서 %(퍼센트) 기호화 시스템 로그 메시지를 전송받는다.

%PIX-level-message_number: message_text

(syslog의 사용)

로그기록의 시작 : logging moniter

디스플레이 메시지 : terminal moniter

syslog 기록/열람 종료 : terminal no monitor , no logging monitor

Syslog 서버로의 로그메세지 전송:

로그서버는 dmz1의 192.168.1.5 서버 이라고 한다.

이때, logging host 명령어를 사용하여 다음과같이 명령한다.

logging host dmz1 192.168.1.5

또한, 로그 레벨도 설정을 한다.

logging trap debugging

메시지 전송의 시작 및 종료는 다음과 같다.

메시지 전송의 시작: logging on

메시지 전송의 종료: no logging

syslog 서버로의 메시지 전송 종료는 no logging message 명령어를 사용하면 된다.

메시지 전송 차단 및 허가 의 예제)

%PIX-6-305002: Translation built for gaddr IP_addr to IP_addr

같은 메시지의 경우, 메시지 차단은 다음과 같이 한다.

no logging message 305002

다시 메시지 전송을 원한다면 다음처럼 명령한다.
logging message 305002

또, disable 된 메시지들을 열람하려면,
show logging disabled
no logging message 305002
이라고 하면 된다.

* PIX 방화벽 Syslog 서버(PFSS) 의 사용
PIX방화벽 Syslog 서버는 윈도우 NT시스템에서 syslog 메시지를 열람할수 있는데, 윈도우 NT 시스템을 사용한다면 PFSS를 이용하여 TCP이벤트 메시지나 Time Stamp 메시지 그리고 PIX방화벽의 가동상태나 정지상태등의 유무의 정보등을 열람할 수가 있다.
이 PFSS는 Cisco Connection Online(CCO)에서 구할 수가 있다.

(PFSS의 설정)
PIX방화벽의 syslog에서 tcp 옵션에 관한 설정 이며, 여기서 오직 하나의 tcp나 udp 만을 사용할수가있다.

logging host interface address tcp/port

로그 레벨의 설정을 다음과 같다.
logging trap debugging

그리고, 로그 메시지 전송의 시작은 logging on 명령을 사용하고, 전송의 종료는 no logging on 명령 사용을 하면되고, 만약 syslog 서버로 부터의 메시지전송을 중단하고싶다면, no logging message *syslog_id* 명령어를 사용하고, 여기서 *syslog_id* 는 syslog 메시지 ID 이다.

PFSS에서 time stamped 메시지들을 원한다면, Clock set 명령어를 사용하여 PIX 방화벽의 시간를 설정하고 나서, logging timestamp 명령어를 이용하여 time stamping 을 시작하도록 한다.
설정의 예제는 다음과같다

예제)
2000년 April 1 , 오후 2시 25분으로 시계설정을 하고, 타임스템핑 시작
clock set 14:25:00 apr 1 2000
logging timestamp

타임스템핑의 종료는 no logging timestamp 명령어를 사용한다.
참고로, IPSec 디지털 인증기능을 사용한다면, 시계설정을 GMT(Greenwich Mean Time)로 설정한다.

* 유닉스 시스템의 Syslog 설정
이것은 PIX 방화벽에서의 syslog 메시지를 유닉스 계열의 시스템에서 전송받기 위한설정이다.

설정의 예)
PIX방화벽에서 logging host 명령어를 이용하여 syslog 메시지를 전송받을 유닉스계열의 호스트 IP를 지정하도록 한다.

다음으로 유닉스 시스템에 root(최고관리자권한)로 로그인하여 다음 명령어를 수행한다.
</var/log/pix 라는 로그저장용 디렉토리 생성>
mkdir /var/log/pix
</var/log/pix/pixfirewall 이라는 파일의 생성>
touch /var/log/pix/pixfirewall

그리고, root(슈퍼유저)로 계속 로그인 되어있는 상태에서 /etc/syslog.conf 파일을 유닉스용 에디터(예, VI 나 pico)로 편집하는데, 이때 syslog level을 선택하여 다음과 같이 입력한다.

PIX Firewall syslog messages <이부분은 주석이다>
local4.level /var/log/pix/pixfirewall <- 이전에 생성한 파일

syslog level 리스트는 다음페이지를 참고하길바란다.

<syslog.conf 의 syslog level 리스트>

Syslog level	Syslog.conf 에서 사용될 level
0 - Emergencies	**local4.emerg**
1 - Alerts	**local4.alert**
2 - Critical	**local4.crit**
3 - Errors	**local4.err**
4 - Warnings	**local4.warn**
5 - Notifications	**local4.notice**
6 - Information	**local4.info**
7 - Debugging	**local4.debug**

이제 모든설정 및 syslog.conf 설정이 마무리 되었다면, syslog 데몬을 리로드해야하는데 다음명령어로 할 수가 있다.
아래 명령어는 유닉스시스템을 조금이라도 다루어본사람은 쉽게 알수있을것이다. 이것은 syslog.pid를 열어서 syslog pid값을 구하고 그 값을 HUP 즉, hangup 을 하여, 데몬의 reload를 하는것이다.

kill -HUP 'cat /etc/syslog.pid'

* FTP와 URL 메시지의 로그기록
FTP명령어와 WWW URL들을 syslog 가 enable 이 되었있을 때, 해당 로그에 대한 기록을 할 수있는데, 이때 FTP와 URL메시지는 syslog level7에서 기록된다.
또한, inbound와 outbound 동시에 syslog 로 기록이 된다.

설정의 예)
FTP명령어와 WWWURL에 대해서 syslog의 로그를 기록할때는 fixup protocol 명령어를 이용하여 설정한다.
여기서 **fixup protocol** 명령어는 방화벽을 통한 특별한 어플리케이션들에 대한 조작을 위한것이다. 흔히 실행되는것들 (예를 들면, HTTP의 80번포트)처럼 잘알려진 포트의 어플리케이션들을 위한 특별한 처리기능을 가능하게 하거나 불가능하게 할수있다.

만약 http 80번과 ftp 21번에 대한 사용을 명시하려면 다음과 같이 명령한다.

fixup protocol http 80
fixup protocol ftp 21

위와 같이 http 80 번과 ftp 21번에 대한 사용을 명시한 상태에서의 syslog는 사용을 명시하였으므로, 해당서비스에 대한 log 를 기록하게 된다.

이때 URL 기록의 샘플을 보면 아래와 같다.

%PIX-5-304001: user 192.168.69.71 Accessed URL 10.133.219.25 : www.example.com

FTP기록도 아래를 참고하길 바란다.

%PIX-6-303002: 192.168.69.71 Retrieved 10.133.219.25: 10.1.1.42

이 로그들은 모두 PIX방화벽의 콘솔 모드에서도 로그를 열람하는 명령어인 show logging 명령어로도 열람이 가능하다.

- AAA(Authentication And Authorization) 사용자 권한의 추가

RADIUS or TACACS+ 서버 즉, 인증서버를 가지고 있을 때 사용자 인증 및 보안정책등을 설정 할 수가 있다.

위의 RADIUS와 TACACS+서버 에 대한 설명은 해당 설정파트 에서 다시 설명을 하겠다.

- AAA(Authentication And Authorization)의 설정

이것은 특정한 사용자들의 인증에 대한 허가 또는 불허가에 대한 처리를 하기위해서 이 AAA설정을 한다. 추가적으로는 특정서비스 또는 특정호스트로 사용자들을 허락하기 위해 이 방화벽구성을 사용 할 수 도있고 만약 이것을 구성 하게 된다면, 인증서버와 방화벽사이의 보안에 신경을 더 많이 써야할 것이다. PIX방화벽은 FTP, Telnet 또는 HTTP의 억세스를 위해 아웃바운드 사용자들에게 신뢰있는 프롬프트를 제공한다. 시스템에 접근할 수 있는 사람의 설정 및 어떤 서비스에 인증하는지 어떠한 서버를 허가하는지에 대한 것을 설정할수있다.

우선 참고로 TACACS에 대해서 알아보자

TACACS란?

TACACS는 유닉스 네트웍에 적용되는 다소 오래된 인증 프로토콜로서, 주어진 시스템에 대해 액세스를 허용할 것인지를 결정하기 위하여, 원격 액세스 서버가 사용자의 로그인 패스워드를 인증 서버에 전달할 수 있게 해준다. TACACS는 암호화되지 않은 프로토콜이므로, 그 이후에 나온 TACACS+와 RADIUS 프로토콜에 비해 덜 안전하다. TACACS의 다음 버전은 XTACACS (Extended TACACS)이며, 둘 모두 RFC 1492에 기술되어 있다.

이름이야 어찌되었든, TACACS+는 전적으로 새로운 프로토콜이다. 보다 최근에 만들어졌거나 갱신된 네트웍에서는, 일반적으로 TACACS+와 RADIUS기 이전의 프로토콜들을 대체하였다. TACACS+은 TCP를 사용하며, RADIUS는 UDP를 사용한다. 일부 관리자들은 TCP가 보다 안정적인 프로토콜이라는 이유를 들어, TACACS+를 사용할 것을 권고하고 있다. RADIUS가 인증과 허가를 하나의 사용자 프로필 내에 모두 가지고 있는데 반하여, TACACS+는 두개의 작업으로 나눈다.
TACACS와 XTACACS는 많은 오래된 시스템에서 아직도 운영되고 있다

설정의 예)
static 과 access-list 명령어를 이용하여 외부호스트의 내부네트웍으로 억세스를 하가하여 inbound 인증에 대한 부분을 생성한다.

10.1.1.1 과 10.1.1.2 의 TheUauthKey 암호화
aaa-server AuthInbound protocol tacacs+

aaa-server AuthInbound (inside) host 10.1.1.1 TheUauthKey

aaa-server AuthOutbound protocol tacacs+

aaa-server AuthOutbound (inside) host 10.1.1.2 TheUauthKey

여기서 첫번재 명령어는 AuthInbound 그룹을 tacacs+ 인증을 하는것을 말하며, 두번째 명령어는 AuthInbound 서버가 inside 인터페이스에 존재하며, 10.1.1.1의 아이피를 사용하는것이며, 암호화키가 TheUauthKey 를 사용한다는 것을 말한다.
세번재 명령어는 첫번재 명령어 처럼 AuthOutbound 그룹을 tacacs+ 인증을 하는 것을 말하며 네번재 명령어 또한 두번째 명령어 처럼 AuthOutbound 서버가 inside 인터페이스에 존재하며 10.1.1.2의 아이피를 사용하며, 암호화 키는 TheUauthKey 를 사용한다는 것을 말한다.

또다른 방법의 인증방법이 존재하는데 , aaa authentication 명령어 사용으로 인하여 인증 시작을 하는것이며 기본 포멧은 다음과 같다.

aaa authentication include 인증서비스 inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask 그룹테그

설정의 예)

aaa authentication include any outbound 0 0 0 0 AuthOutbound
aaa authentication include any inbound 0 0 0 0 AuthInbound

aaa의 그룹테그는 **aaa-server**로 지정하였던과 동일하다.

aaa 허가 명령의 사용

PIX방화벽은 사용자가 접근할수 있는 어떤서비스에 대하여 결정한다음 aaa 서버로 허가를 요청하며, Outbound 와 허가를 한다.

aaa authorization의 기본포멧은 다음과 같다.

aaa authorization include | exclude author_service|[protocol/port[-port]] inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask

설정의 예)

aaa authorization include any outbound 0 0 0 0
aaa authorization include any inbound 0 0 0 0

* RADIUS(**Remote Authentication Dial-In User Service**) 인증의 설정

RADISU 인증설정에 앞서 RADIUS란 무엇인가 알아보자.

RADIUS 란?

RADIUS는 RAS가 다이얼업 모뎀을 통해 접속해온 사용자들을 인증하고, 요청된 시스템이나 서비스에 관해 그들에게 액세스 권한을 부여하기 위해, 중앙의 서버와 통신할 수 있게 해주는 클라이언트/서버 프로토콜 및 소프트웨어이다. RADIUS는 회사가 중앙의 데이터베이스 내에 사용자 프로필을 유지하고, 모든 원격지 서버가 공유할 수 있게 해준다. 그것은 더 나은 보안을 제공하며, 회사가 어느 한 곳에서 네트웍을 관리하도록 정책을 수립할 수 있게 해준다. 중앙 서비스를 가진다는 것은 또한 사용량이나 네트웍 통계 등의 추적을 쉽게 할 수 있다는 것을 의미한다. Livingston(이제는 루슨트 테크놀로지의 소유가 되었다)에 의해 만들어진 RADIUS는, Ascend와 기타 다른 네트웍 장비들에 의해 사용되는 사실상의 산업계 표준

이며, IETF 표준으로 제안되어있다.

이 인증설정은 RADIUS서버에서 지정한 사용자그룹 속성을 PIX방화벽의 RADIUS 권한 메시지에 대한 응답을 처리할 수 있는 설정이며, 먼저 access list 와 사용자그룹을 설정한다.
또한, PIX 방화벽의 사용자 인증 과정 후에 지정된 사용자 그룹을 access list와 일관성을 유지하기 위해서 TACACS+와 같은 기능을 제공하는것이기도 하다.
관리자는 먼저 PIX방화벽의 사용자그룹 접근 리스트 정의해야하는것이며 특정 조직의 제한된 사용자에 대한 거부이다.

사용의 예)

```
access-list eng permit ip any server1 255.255.255.255
access-list eng permit ip any server2 255.255.255.255
access-list eng permit ip any server3 255.255.255.255
access-list eng deny ip any any
```

참고로, Cisco Secure 기본 설정은 acl=eng에 맞춰져있으며, access list 명령어를 식별하기위해 Cisco secure설정에 이 항목을 사용해야한다. PIX 방화벽은 acl= acl_id 를 얻고 속성문자열로부터 ACL번호를 추출한다.
이것은 사용자의 uauth 엔트리에 놓이고, 사용자가 연결을 시작하려고 시도할 때, PIX방화벽은 uauth 엔트리에 접근 리스트를 확인한다.그리고 연결이 취소될 때 관련된 syslog 메시지를 생성하여 기록한다.

6) 마무리

PIX방화벽을 다중서버 또는 프로토콜 및 억세스 리스트, 쉴드 라우터등과 함께 설정하는데는 몇일이 걸릴것이며, 가능한 설정의 조합은 **무한대**이다. 그렇지만 위에서 살펴본 설정법을 본다면, 네트워크에서 가장 복잡한 장치중의 하나인 방화벽을 설정하는 일도 그렇게 복잡하지만은 않다는 것을 알았을것이다. 훨씬 더 깊이 들어갈수도 있지만, 한번에 하나의 인터페이스씩, 한번에 하나의 명령씩 하면 되는것이다. 하나씩 설정하다 보면 어느새 복합적인 기능의 방화벽 룰셋이 구성되어져 있을 것이다.

방화벽 설정에는 많은 다른 중요한 요소들이 있다. 한예로 두대의 방화벽을 운영할 수가 있는데, 이때 한대는 주게이트웨이 서버로 동작시키고, 다른 한대는 주 게이트웨이 서버에 문제가 생겼을 때 트래픽이 들어가가는 백업서버로 동작한다.(failover 명령으로 설정한다)
위의 한예처럼 PIX방화벽의 설정은 응용에 응용을 거듭나서 사용자가 상상하는 모든 것을 소화해 낼수있고, 설정의 끝은 무한대이기 때문에 끝은 존재하지않는다. 다만 스스로 창조하여 새롭게 만들어가는것만이 할일이다.