Linux Server (for centos 7.X)
- IPtables-

소 속	IDC실
이 름	신용우 매니저
E-mail	tech@tongkni.co.kr

통큰아이

INDEX

1. 개요.

- 리눅스 서버에서 제공하는 기본 방화벽인 iptables를 이용해 간단한 조작법으로 서버의 포트를 관리 할 수 있는 서비스입니다.

- 네트워크 구간에서의 방화벽 장비나 서버에서 별도의 보안 솔루션을 통해 보안성을 강화시킬 수 있지만 여기서는 리눅스에 내장된 기본 보안 기능인 iptables를 이용하여 보안을 강화하고자 합니다.

- iptables는 서버로 수신 및 송신하는 포트나 IP를 허용 또는 차단 할 수 있습니다.

- 아래는 방화벽을 구성하는 절차입니다.
  1 iptables에 허용할 포트 및 IP 정책을 추가.
  2 허용된 정책 외에 나머지 포트는 차단.
  3 iptables 서비스 재 시작.

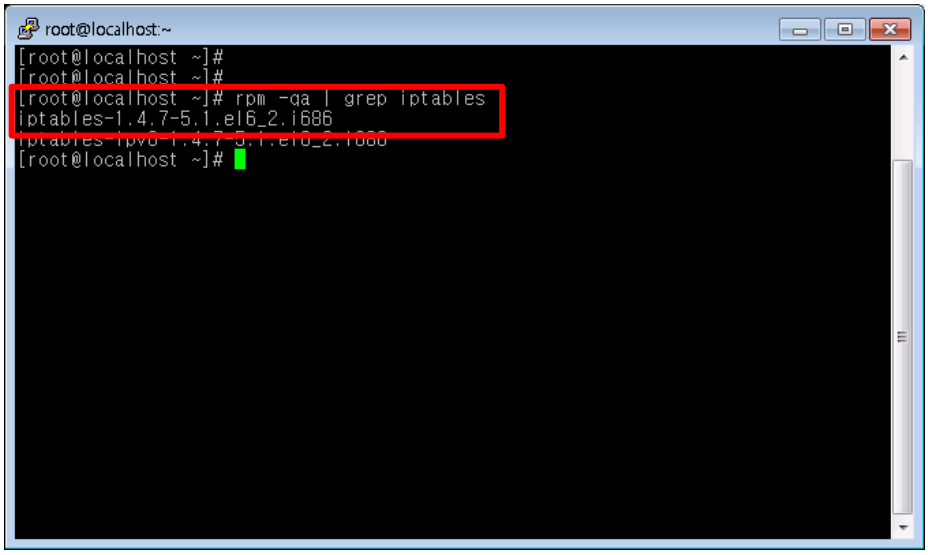
- iptables를 사용할 경우 순서가 매우 중요하며, 허용할 포트 정책을 먼저 추가한 후 남은 모든 포트를 차단하는 것이 좋습니다..

※ **주의 : SSH 접속 포트인 22번 포트를 허용하지 않은 채 남은 포트를 차단하도록 설정하면 외부PC에서 서버로의 원격접속이 불가능해집니다.**
또한 웹 서비스 등의 어떠한 서비스가 이미 운영되고 있는 서버의 경우에도 반드시 해당 서비스들의 포트를 허용하는 예외를 추가한 후에 방화벽을 설정하시기 바랍니다.

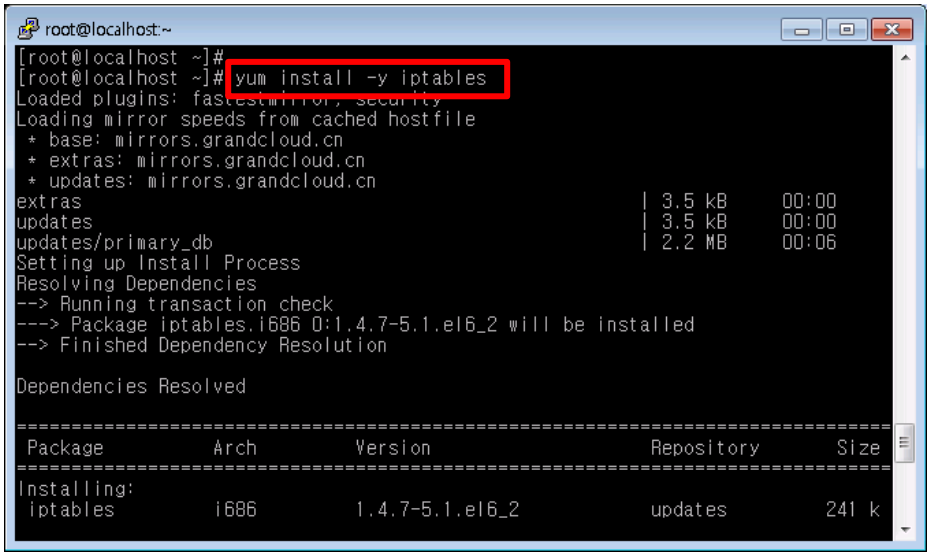
- 본 매뉴얼은 보안을 위한 방화벽 설정 방법에 대해 작성되었습니다.

2. iptables 설치하기.

1 iptables 서비스가 설치되어 있는지 확인합니다.
-> rpm -qa | grep iptables



2 만약 설치되어 있지 않은 경우 yum을 이용하여 설치합니다.
-> yum install -y iptables



3 재부팅때 iptables가 시작될수 있도록 설정합니다.
-> systemctl enable iptables.service

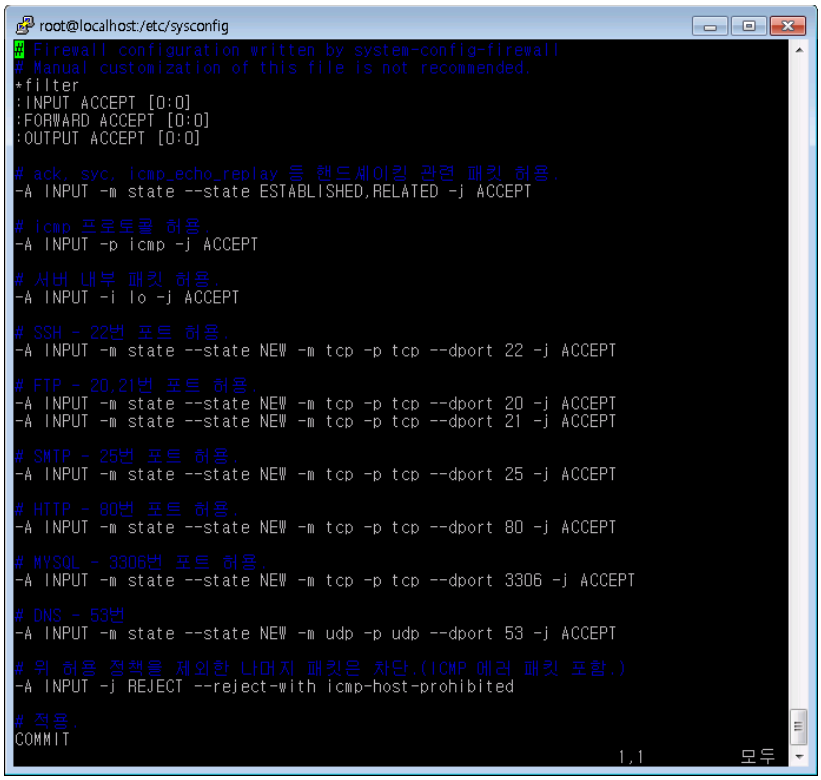
3. iptables 설정하기.

1 방화벽 구성을 보다 쉽게 하기 위해 아래 스크립트를 이용합니다. 아래 스크립트를 복사하여 붙여 넣기 하시면 됩니다.

```
service iptables stop

echo "# Firewall configuration written by system-config-firewall" > /etc/sysconfig/iptables
echo "# Manual customization of this file is not recommended. " >> /etc/sysconfig/iptables
echo "*filter" >> /etc/sysconfig/iptables
echo ":INPUT ACCEPT [0:0] " >> /etc/sysconfig/iptables
echo ":FORWARD ACCEPT [0:0] " >> /etc/sysconfig/iptables
echo ":OUTPUT ACCEPT [0:0] " >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# ack, syc, icmp_echo_replay 등 핸드셰이킹 관련 패킷 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# icmp 프로토콜 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -p icmp -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# 서버 내부 패킷 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -i lo -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# SSH - 22번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# FTP - 20,21번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT" >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# SMTP - 25번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# HTTP - 80번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# MYSQL - 3306번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# DNS - 53번" >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# 위 허용 정책을 제외한 나머지 패킷은 차단.(ICMP 에러 패킷 포함.)" >> /etc/sysconfig/iptables
echo "-A INPUT -j REJECT --reject-with icmp-host-prohibited" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# 적용. " >> /etc/sysconfig/iptables
echo "COMMIT" >> /etc/sysconfig/iptables

service iptables start
```

2 /etc/sysconfig/iptables 파일을 확인합니다. 각 정책마다 이해하기 쉽도록 주석을 작성해 놓았으며, 다른 서비스 포트 허용 정책을 추가할 경우 기존 문장을 참고하여 **마지막 차단 정책 상단에 추가**하시면 됩니다.

➔ vim /etc/sysconfig/iptables



※ iptables 정책에서는 먼저 선언 된 정책이 우선순위가 있으므로, 모든 패킷 차단 정책 하단에 허용 정책을 넣으면 적용이 되지 않으므로 항상 유의하시기 바랍니다.

4. 활용하기.

4.1 특정 IP에서만 SSH 접속 가능한 정책.

1 vi 편집기로 /etc/sysconfig/iptables를 열어 기존 22번 포트를 허용하는 정책을 삭제합니다.

➔ vim /etc/sysconfig/iptables

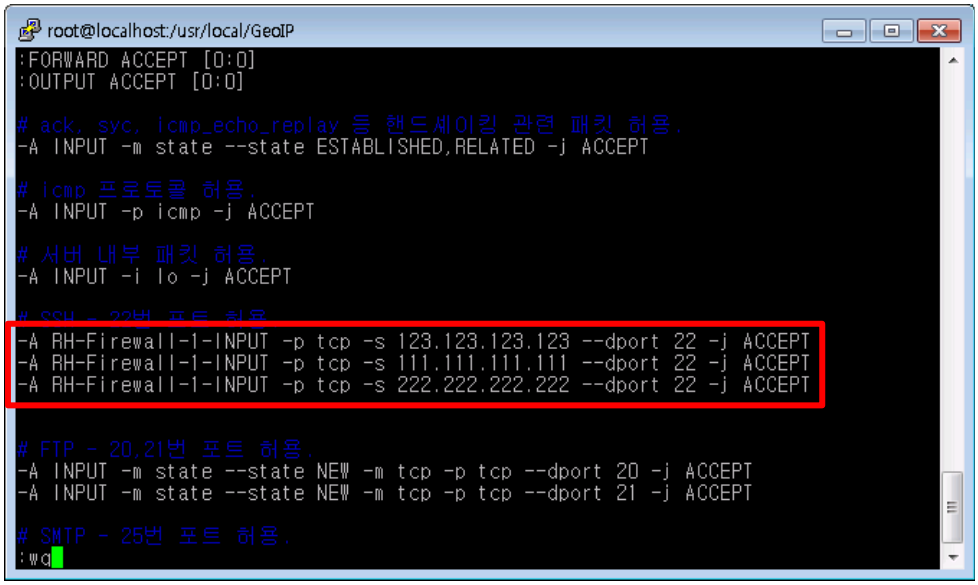
삭제 : "-A INPUT -m state –state NEW -m tcp -p tcp –dport 22 -j ACCEPT"

2 해당 줄에 아래처럼 추가합니다.

➔ -A RH-Firewall-1-INPUT -p tcp -s 123.123.123.123 –dport 22 -j ACCEPT

(123.123.123.123 ip 에서만 22번 포트(SSH)에 접근 할 수 있도록 설정.)

※ 여러 IP에서의 접속이 필요한 경우 같은 방식으로 추가합니다.



3 서비스를 재시작 합니다.

➔ service iptables restart

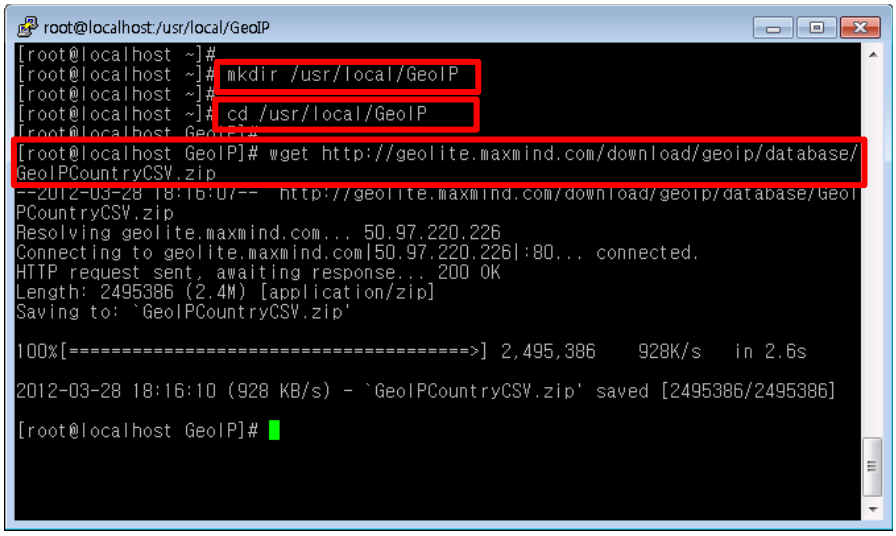
4.2 중국 또는 특정 국가의 IP 대역 차단 정책.

1 GEOIP는 전 세계 IP 할당 목록 리스트 제공하는 서비스입니다. 이를 이용하여 각 국가의 IP대역을 쉽게 iptables에 적용할 수 있습니다. 우선 GEOIP 의 DB파일을 다운 받습니다.

➔ mkdir /usr/local/GeoIP

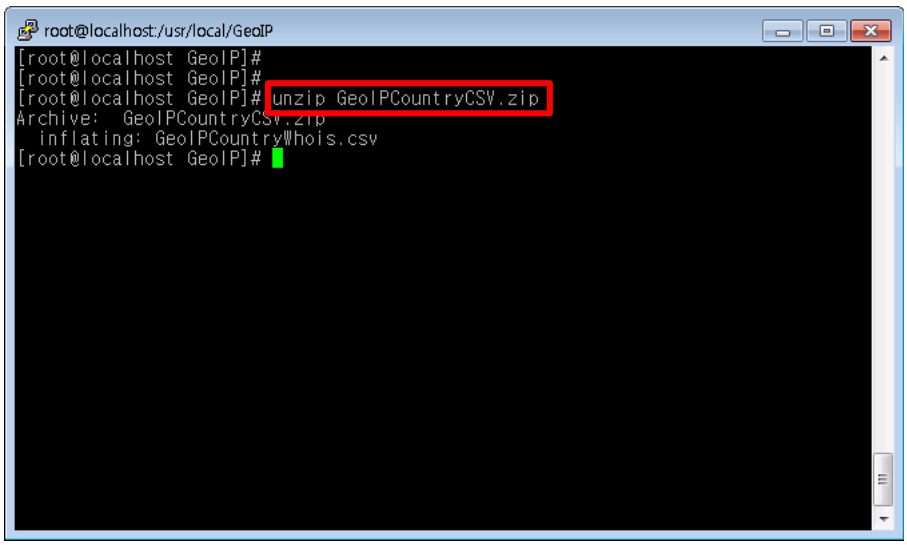
➔ cd /usr/local/GeoIP

➔ wget http://geolite.maxmind.com/download/geoip/database/GeoIPCountryCSV.zip



2 unzip으로 파일의 압축을 풉니다. (unzip이 없을 경우 “yum install -y unzip” 으로 설치)

➔ unzip GeoIPCountryCSV.zip



3 vi 편집기로 ban.sh 스크립트 파일을 생성하여 아래 스크립트를 붙여넣습니다.

➔ vim ban.sh

➔ 아래 스크립트를 삽입 후 chmod 700 ban.sh

※ 만약 다른 국가의 IP대역을 적용하려는 경우 아래 스크립트 중 “China”부분을 다른 국가로 변경하시면 됩니다.

```
#!/bin/sh
DATA=/usr/local/GeoIP/GeoIPCountryWhois.csv
echo "# Block IP Address : China " > /etc/sysconfig/iptables_china
for IPRANGE in `egrep "China" $DATA | cut -d, -f1,2 | sed -e 's/"//g' | sed -e 's/,/-/g'`
do
   #echo  $IPRANGE
   echo "-A INPUT -p all -m iprange –src-range $IPRANGE -j DROP" >> /etc/sysconfig/iptables_china
done
```

```
root@localhost:~
#!/bin/sh
DATA=/usr/local/GeoIP/GeoIPCountryWhois.csv
echo "# Block IP Address : China " >> /etc/sysconfig/iptables
for IPRANGE in `egrep "China" $DATA | cut -d, -f1,2 | sed -e 's/"//g' | sed -e '
s/,/-/g'`
do
    #echo  $IPRANGE
    echo "-A INPUT -p all -m iprange --src-range $IPRANGE -j DROP" >> /etc/sysco
nfig/iptables
done

~
~
~
~
~
~
~
~
~
~
~
:wq!
```

4 ban.sh를 실행하면 /etc/sysconfig/iptables_china 에 중국 IP대역을 차단하는 정책이 저장됩니다. 정상적으로 저장 되었는지 확인합니다.

➔ cat /etc/sysconfig/iptables_china

```
root@localhost:/etc/sysconfig
[root@localhost sysconfig]#
[root@localhost sysconfig]# cat /etc/sysconfig/iptables_china
# Block IP Address : China
-A INPUT -p all -m iprange --src-range 1.0.1.0-1.0.3.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.0.8.0-1.0.15.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.0.32.0-1.0.63.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.1.0.0-1.1.0.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.1.2.0-1.1.63.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.2.0.0-1.2.2.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.2.4.0-1.2.127.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.3.0.0-1.3.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.4.1.0-1.4.127.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.8.0.0-1.8.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.10.0.0-1.10.9.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.10.11.0-1.10.127.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.12.0.0-1.15.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.24.0.0-1.31.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.45.0.0-1.45.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.48.0.0-1.51.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.56.0.0-1.63.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.68.0.0-1.71.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.80.0.0-1.95.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.116.0.0-1.119.255.255 -j DROP
-A INPUT -p all -m iprange --src-range 1.180.0.0-1.185.255.255 -j DROP
```

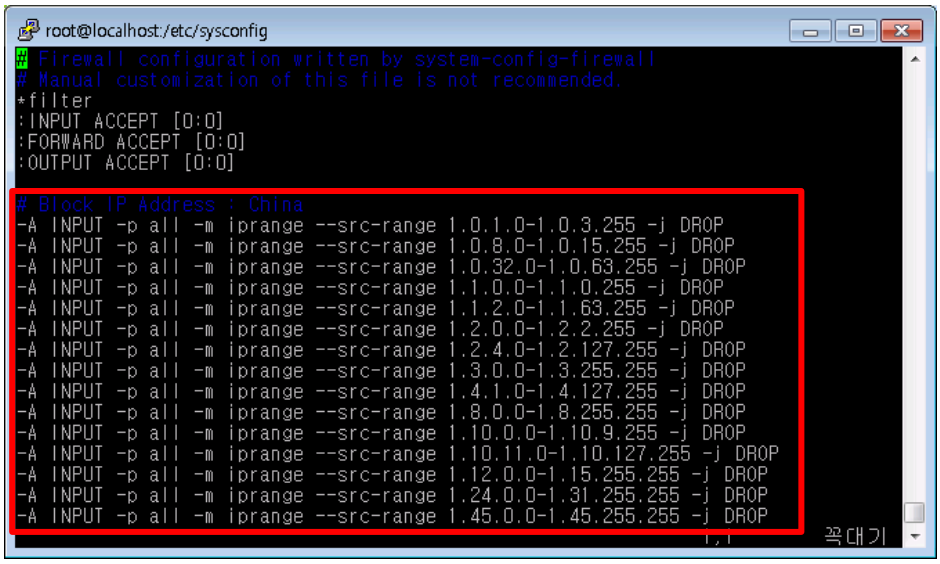
5 IP 차단 정책은 챕터3에서 설정했던 port 허용 정책보다 앞 단에 위치하여 우선순위가 높아야 합니다. 예를들어 방화벽에서 ssh 접속 허용 정책이 먼저 적용되고 중국 IP 차단 정책이 뒤에 적용된다

면, 중국 IP에서 ssh 접속을 시도하더라도 ssh 접속 허용정책에 먼저 매치되어 뒤의 IP 차단 정책을 무시하고 접속을 허용하게 됩니다. 따라서 IP 차단 정책을 먼저 적용해야 하므로 챕터 3의 스크립트를 응용하여 다음의 스크립트를 새로 생성합니다.
(빨간색으로 표시된 부분이 새로 추가된 부분입니다. 다른 국가도 추가할 경우 ③~④의 순서대로 작업 후 아래 스크립트의 해당 위치에 추가합니다.)
(챕터 3의 스크립트 중 변경사항이 있다면 아래 스크립트도 적절히 수정하시기 바랍니다.)

```
service iptables stop

echo "# Firewall configuration written by system-config-firewall" > /etc/sysconfig/iptables
echo "# Manual customization of this file is not recommended. " >> /etc/sysconfig/iptables
echo "*filter" >> /etc/sysconfig/iptables
echo ":INPUT ACCEPT [0:0] " >> /etc/sysconfig/iptables
echo ":FORWARD ACCEPT [0:0] " >> /etc/sysconfig/iptables
echo ":OUTPUT ACCEPT [0:0] " >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
cat /etc/sysconfig/iptables_china >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# ack, syc, icmp_echo_replay 등 핸드셰이킹 관련 패킷 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# icmp 프로토콜 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -p icmp -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# 서버 내부 패킷 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -i lo -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# SSH - 22번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# FTP - 20,21번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT" >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# SMTP - 25번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# HTTP - 80번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# MYSQL - 3306번 포트 허용. " >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# DNS - 53번" >> /etc/sysconfig/iptables
echo "-A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# 위 허용 정책을 제외한 나머지 패킷은 차단.(ICMP 에러 패킷 포함.)" >> /etc/sysconfig/iptables
echo "-A INPUT -j REJECT --reject-with icmp-host-prohibited" >> /etc/sysconfig/iptables

echo >> /etc/sysconfig/iptables
echo "# 적용. " >> /etc/sysconfig/iptables
echo "COMMIT" >> /etc/sysconfig/iptables

service iptables start
```

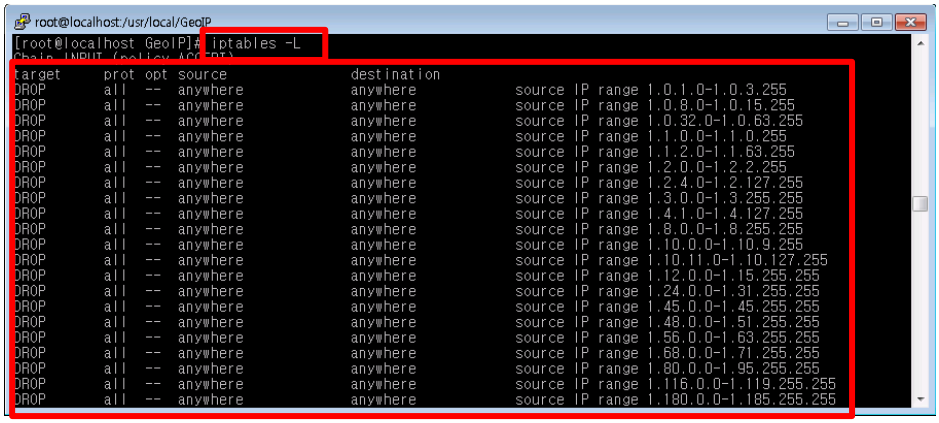
6 vi편집기로 /etc/sysconfig/iptables 파일을 열어 정책에 규칙이 적용된 것을 확인합니다.

➔ vim /etc/sysconfig/iptables



7 iptables -L 명령어를 이용하여 INPUT 정책에 규칙이 적용된 것을 확인합니다.

➔ iptables -L



8 위 적용된 정책을 삭제하려면 /etc/syscofig/iptables에서 추가된 내용을 삭제한 후 iptables 서비스를 재시작 하면 됩니다.

➔ vim /etc/sysconfig/iptables

➔ service iptables restart

4.3 특정 공격에 대한 방어 정책.

- 아래 특정 공격에 대한 방어정책을 서버환경에 맞게 수정하고 /etc/sysconfig/iptables의 적절한 위치에 삽입하시기 바랍니다. 예를 들어 80번 포트에 대한 syn packet을 방어하려는 경우, 80번 포트 허용 정책인 "INPUT -m state –state NEW -m tcp -p tcp –dport 80 -j ACCEPT" 윗단에 방어 정책을 적용해야 먼저 걸러낸 후 80번 포트를 허용하게 됩니다.

- 한 IP에서 30개 이상의 syn packet이 80번 포트로 들어오면 공격으로 판단하여 차단합니다.
  ➔ -A INPUT -p tcp –syn –dport 80 -m connlimit –connlimit-above 30 -j DROP

- ICMP Flooding 공격 방어 : 목적지의 가용성 확인을 위한 ping 메시지 확인을 담당하는 ICMP 패킷을 모두 차단합니다. 챕터 3의 스크립트 중 -A INPUT -p icmp -j ACCEPT 정책을 아래와 같이 수정하시기 바랍니다.
  ➔ -A INPUT -p icmp -j DROP

- Brute-force attack 방어 (SSH) : 같은 IP에서 60초동안 10번의 SSH 접속 로그인 실패 시 60초간 접속을 차단합니다. 22번 SSH 포트로 오는 모든 "새로운 연결"은 SSH_BLACK 이름으로 정의 후 감시하며 접속 IP 정보를 로그로 기록하고 10번 이상 시도한 접속을 60초동 차단합니다. 로그는 /var/log/messages 에 남습니다.
  (**Brute-force attack** : 패스워드 사전 파일을 이용하여 미리 지정한 아이디를 지속적으로 대입하여 취약한 패스워드로 설정된 ID를 찾는 공격)
  ➔ -A INPUT -p tcp –dport 22 -m state –state NEW -m recent –set –name SSH_BLACK
  -A INPUT -p tcp –dport 22 -m state –state NEW -m recent –update –seconds 60 –hitcount 10 –rttl –name SSH_BLACK -j LOG –log-prefix SSH_BLACK:
  -A INPUT -p tcp –dport 22 -m state –state NEW -m recent –update –seconds 60 –hitcount 10 –rttl –name SSH_BLACK -j DROP

- Brute-force attack 방어 (FTP) : 같은 IP에서 60초동안 10번의 FTP 접속 로그인 실패 시 60초간 접속을 차단합니다. 21번 FTP 포트로 오는 모든 "새로운 연결"은 FTP_BLACK 이름으로 정의 후 감시하며 접속 IP 정보를 로그로 기록하고 10번 이상 시도한 접속을 60초동안 차단합니다. 로그는 /var/log/messages 에 남습니다.
  ➔ -A INPUT -p tcp –dport 21 -m state –state NEW -m recent –set –name FTP_BLACK
  -A INPUT -p tcp –dport 21 -m state –state NEW -m recent –update –seconds 60 –hitcount 10 –rttl –name FTP_BLACK -j LOG –log-prefix FTP_BLACK:
  -A INPUT -p tcp –dport 21 -m state –state NEW -m recent –update –seconds 60 –hitcount 10 –rttl –name FTP_BLACK -j DROP

(참고) iptables 옵션 참고 사이트.
http://www.cyworld.com/LinuxerChoi/10518923

(참고) iptables 예제 참고 사이트.
http://blog.naver.com/junix?Redirect=Log&logNo=80132536243

(참고) Well-Known 포트 번호 리스트.
참고하셔서 서비스에 필요한 포트번호가 있다면 방화벽 허용정책에 추가하시기 바랍니다.

포트	프로토콜	응용 프로그램	프로토콜 시스템	서비스이름
7	TCP	Echo	단순 TCP/IP 서비스	
7	UDP	Echo	단순 TCP/IP 서비스	
9	TCP	Discard	단순 TCP/IP 서비스	
9	UDP	Discard	단순 TCP/IP 서비스	

13 TCP Daytime 단순 TCP/IP 서비스
13 UDP Daytime 단순 TCP/IP 서비스
17 TCP Quotd 단순 TCP/IP 서비스
17 UDP Quotd 단순 TCP/IP 서비스
19 TCP Chargen 단순 TCP/IP 서비스
19 UDP Chargen 단순 TCP/IP 서비스
20 TCP FTP 기본 데이터 FTP 게시 서비스
21 TCP FTP 제어 FTP 게시 서비스
21 TCP FTP 제어 응용 프로그램 계층 게이트웨이 서비스
23 TCP 텔넷 텔넷
25 TCP SMTP Simple Mail Transfer Protocol
25 TCP SMTP Exchange Server
42 TCP WINS 복제 Windows Internet Name Service
42 UDP WINS 복제 Windows Internet Name Service
53 TCP DNS DNS 서버
53 UDP DNS DNS 서버
53 TCP DNS 인터넷 연결 방화벽/인터넷 연결 공유
53 UDP DNS 인터넷 연결 방화벽/인터넷 연결 공유
67 UDP DHCP 서버 DHCP 서버
67 UDP DHCP 서버 인터넷 연결 방화벽/인터넷 연결 공유
69 UDP TFTP Trivial FTP 데몬 서비스
80 TCP HTTP Windows Media 서비스
80 TCP HTTP World Wide Web 게시 서비스
80 TCP HTTP SharePoint Portal Server
88 TCP Kerberos Kerberos 키 배포 센터
88 UDP Kerberos Kerberos 키 배포 센터
102 TCP X.400 Microsoft Exchange MTA 스택
110 TCP POP3 Microsoft POP3 서비스
110 TCP POP3 Exchange Server
119 TCP NNTP Network News Transfer Protocol
123 UDP NTP Windows 시간
123 UDP SNTP Windows 시간
135 TCP RPC 메시지 대기열
135 TCP RPC 원격 프로시저 호출
135 TCP RPC Exchange Server
135 TCP RPC 인증서 서비스
135 TCP RPC 클러스터 서비스
135 TCP RPC 분산 파일 시스템
135 TCP RPC 분산 링크 추적
135 TCP RPC Distributed Transaction Coordinator
135 TCP RPC 분산 파일 복제 서비스
135 TCP RPC 팩스 서비스
135 TCP RPC Microsoft Exchange Server
135 TCP RPC 파일 복제 서비스
135 TCP RPC 그룹 정책
135 TCP RPC 로컬 보안 기관
135 TCP RPC 원격 저장소 알림
135 TCP RPC 원격 저장소 서버
135 TCP RPC Systems Management Server 2.0
135 TCP RPC 터미널 서비스 라이선스
135 TCP RPC 터미널 서비스 세션 디렉터리
137 UDP NetBIOS 이름 확인 컴퓨터 브라우저
137 UDP NetBIOS 이름 확인 서버
137 UDP NetBIOS 이름 확인 Windows Internet Name Service
137 UDP NetBIOS 이름 확인 Net Logon
137 UDP NetBIOS 이름 확인 Systems Management Server 2.0
138 UDP NetBIOS 데이터그램 서비스 컴퓨터 브라우저
138 UDP NetBIOS 데이터그램 서비스 메신저
138 UDP NetBIOS 데이터그램 서비스 서버
138 UDP NetBIOS 데이터그램 서비스 Net Logon
138 UDP NetBIOS 데이터그램 서비스 분산 파일 시스템
138 UDP NetBIOS 데이터그램 서비스 Systems Management Server 2.0
138 UDP NetBIOS 데이터그램 서비스 라이선스 로깅 서비스
139 TCP NetBIOS 세션 서비스 컴퓨터 브라우저
139 TCP NetBIOS 세션 서비스 팩스 서비스

139 TCP NetBIOS 세션 서비스 성능 로그 및 경고
139 TCP NetBIOS 세션 서비스 인쇄 스풀러
139 TCP NetBIOS 세션 서비스 서버
139 TCP NetBIOS 세션 서비스 Net Logon
139 TCP NetBIOS 세션 서비스 원격 프로시저 호출 로케이터
139 TCP NetBIOS 세션 서비스 분산 파일 시스템
139 TCP NetBIOS 세션 서비스 Systems Management Server 2.0
139 TCP NetBIOS 세션 서비스 라이선스 로깅 서비스
143 TCP IMAP Exchange Server
161 UDP SNMP SNMP 서비스
162 UDP SNMP 트랩 아웃바운드 SNMP 트랩 서비스
389 TCP LDAP 서버 로컬 보안 기관
389 UDP LDAP 서버 로컬 보안 기관
389 TCP LDAP 서버 분산 파일 시스템
389 UDP LDAP 서버 분산 파일 시스템
443 TCP HTTPS HTTP SSL
443 TCP HTTPS World Wide Web 게시 서비스
443 TCP HTTPS SharePoint Portal Server
443 TCP RPC over HTTPS Exchange Server 2003
445 TCP SMB 팩스 서비스
445 TCP SMB 인쇄 스풀러
445 TCP SMB 서버
445 TCP SMB 원격 프로시저 호출 로케이터
445 TCP SMB 분산 파일 시스템
445 TCP SMB 라이선스 로깅 서비스
445 TCP SMB Net Logon
464 UDP Kerberos Password V5 Kerberos 키 배포 센터
464 TCP Kerberos Password V5 Kerberos 키 배포 센터
500 UDP IPsec ISAKMP 로컬 보안 기관
515 TCP LPD TCP/IP 인쇄 서버
548 TCP Macintosh용 파일 서버 Macintosh용 파일 서버
554 TCP RTSP Windows Media 서비스
563 TCP SSL을 통한 NNTP Network News Transfer Protocol
593 TCP RPC over HTTPS 끝점 매퍼 원격 프로시저 호출
593 TCP RPC over HTTPS Exchange Server
636 TCP LDAP SSL 로컬 보안 기관
636 UDP LDAP SSL 로컬 보안 기관
993 TCP SSL을 통한 IMAP Exchange Server
995 TCP SSL을 통한 POP3 Exchange Server
1067 TCP 설치 부트스트랩 서비스 설치 부트스트랩 프로토콜 서버
1068 TCP 설치 부트스트랩 서비스 설치 부트스트랩 프로토콜 클라이언트
1270 TCP MOM-Encrypted Microsoft Operations Manager 2000
1433 TCP SQL over TCP Microsoft SQL Server
1433 TCP SQL over TCP MSSQL$UDDI
1434 UDP SQL Probe Microsoft SQL Server
1434 UDP SQL Probe MSSQL$UDDI
1645 UDP 레거시 RADIUS 인터넷 인증 서비스
1646 UDP 레거시 RADIUS 인터넷 인증 서비스
1701 UDP L2TP 라우팅 및 원격 액세스
1723 TCP PPTP 라우팅 및 원격 액세스
1755 TCP MMS Windows Media 서비스
1755 UDP MMS Windows Media 서비스
1801 TCP MSMQ 메시지 대기열
1801 UDP MSMQ 메시지 대기열
1812 UDP RADIUS 인증 인터넷 인증 서비스
1813 UDP RADIUS 계정 인터넷 인증 서비스
1900 UDP SSDP SSDP 검색 서비스
2101 TCP MSMQ-DC 메시지 대기열
2103 TCP MSMQ-RPC 메시지 대기열
2105 TCP MSMQ-RPC 메시지 대기열
2107 TCP MSMQ-Mgmt 메시지 대기열
2393 TCP OLAP Services 7.0 SQL Server: 하위 수준 OLAP 클라이언트 지원
2394 TCP OLAP Services 7.0 SQL Server: 하위 수준 OLAP 클라이언트 지원
2460 UDP MS Theater Windows Media 서비스
2535 UDP MADCAP DHCP 서버

2701 TCP SMS 원격 제어(제어) SMS 원격 제어 에이전트
2701 UDP SMS 원격 제어(제어) SMS 원격 제어 에이전트
2702 TCP SMS 원격 제어(데이터) SMS 원격 제어 에이전트
2702 UDP SMS 원격 제어(데이터) SMS 원격 제어 에이전트
2703 TCP SMS 원격 채팅 SMS 원격 제어 에이전트
2703 UPD SMS 원격 채팅 SMS 원격 제어 에이전트
2704 TCP SMS 원격 파일 전송 SMS 원격 제어 에이전트
2704 UDP SMS 원격 파일 전송 SMS 원격 제어 에이전트
2725 TCP SQL Analysis Services SQL Analysis Server
2869 TCP UPNP 범용 플러그 앤 플레이 장치 호스트
2869 TCP SSDP 이벤트 알림 SSDP 검색 서비스
3268 TCP 글로벌 카탈로그 서버 로컬 보안 기관
3269 TCP 글로벌 카탈로그 서버 로컬 보안 기관
3343 UDP 클러스터 서비스 클러스터 서비스
3389 TCP 터미널 서비스 NetMeeting 원격 데스크톱 공유
3389 TCP 터미널 서비스 터미널 서비스
3527 UDP MSMQ-Ping 메시지 대기열
4011 UDP BINL 원격 설치

감사합니다.