

Contents

- 1 Iptables is not set-up by default on Debian Sarge.
- 2 Iptable command line options:
- 3 Rules of Iptables:
- 4 Control of Iptables (inactive is a blank file with no rules):
- 5 Port Forwarding & NAT - Network Address Translation - V.Basic:
- 6 My Firewall Config:
- 7 Remove / Delete an individual /single Iptable Rule
- 8 Other pieces of information to remember:
 - ◆ 8.1 Iptables Forward with NAT
- 9 Saving ALL IPTABLE Rules
- 10 fail2ban - Debian Etch/Ubuntu
 - ◆ 10.1 Problems with fail2ban and ssh attempts on ubuntu
- 11 Firewall on Centos / RH

Iptables is not set-up by default on Debian Sarge.

```
apt-get install iptables
```

The init (start/stop) script for iptables is new within sarge - using if-up and if-down. The old init script is still available to load and save iptables rules. Do the following to set-up the iptables init script (details obtained from http://www.howtoforge.com/linux_iptables_sarge):

```
gunzip /usr/share/doc/iptables/examples/oldinitdscript.gz -c > /etc/init.d/iptables
chmod +x /etc/init.d/iptables
mkdir /var/lib/iptables
chmod 700 /var/lib/iptables
```

Iptable command line options:

```
-A => Append this rule to the WhatEver Chain
-s => Source Address
-d => Destination Address
-p => Protocol
--dport => Destination Port
-j => Jump. If everything in this rule matches then 'jump' to ACCEPT
-I => ACCEPT 1 Insert at position 1 of the ACCEPT Chain
-P => Set Policy e.g. iptables -P INPUT DROP
```

Rules of Iptables:

As it is a table of rules, the first rule has precedence. If the first rule dis-allows everything then nothing else afterwards will matter.

- INDIVIDUAL REJECTS FIRST
- THEN OPEN IT UP

Iptables_Firewall

• BLOCK ALL

List iptable rules:

```
iptables -n -L (-n prevents slow reverse DNS lookup)
```

Reject all from an IP Address:

```
iptables -A INPUT -s 136.xxx.xxx.xxx -d 136.xxx.xxx.xxx -j REJECT
```

Allow in SSH:

```
iptables -A INPUT -d 136.xxx.xxx.xxx -p tcp --dport 22 -j ACCEPT
```

*If Logging - Insert Seperate Line *BEFORE* the ACCEPT / REJECT / DROP*

```
iptables -A INPUT -d 136.xxx.xxx.xxx -p tcp --dport 3306 -j LOG
```

```
iptables -A INPUT -d 136.xxx.xxx.xxx -p tcp --dport 3306 -j ACCEPT
```

Block All:

```
iptables -A INPUT -j REJECT
```

Control of Iptables (inactive is a blank file with no rules):

```
/etc/init.d/iptables save active
```

```
/etc/init.d/iptables load active | inactive
```

Port Forwarding & NAT - Network Address Translation - V.Basic:

```
iptables -t nat -A PREROUTING -p tcp -d 136.201.xxx.xxx --dport 443 -j DNAT --to 136.201.xxx.xxx:22
```

The Above will do on its Own. The above allows someone to ssh into the box on port 443 incase port 22

****NB**** Set ipForwarding in /etc/networking/options !!!!!!!!!!!

If Forwarding from another Network:

```
iptables -A FORWARD -p tcp -d 136.201.xxx.xxx --dport 22 -j ACCEPT
```

Web Port Forwarding: <http://www.hackorama.com/network/portfwd.shtml>

NB: Must allow IN Traffic and Connections the server started/ initiated

(<http://rimuhosting.com/howto/firewall.jsp>):

```
iptables -A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT
```

```
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -m state --state RELATED -j ACCEPT
```

My Firewall Config:

```
#####
iptables -A INPUT -p tcp --dport 80 -j ACCEPT //apache
iptables -A INPUT -p tcp --dport 443 -j ACCEPT //apache ssl
iptables -A INPUT -p tcp --dport 53 -j ACCEPT //dns - udp for large queries
iptables -A INPUT -p udp --dport 53 -j ACCEPT //dns - udp for small queries
iptables -A INPUT -p tcp --dport 953 -j ACCEPT //dns internal
iptables -A INPUT -p tcp --dport 1080 -j ACCEPT //dante socks server
iptables -A INPUT -d 136.201.1.250 -p tcp --dport 22 -j ACCEPT //sshd
iptables -A INPUT -d 136.201.1.250 -p tcp --dport 3306 -j ACCEPT //mysql
iptables -A INPUT -d 136.201.1.250 -p tcp --dport 8000 -j ACCEPT //apache on phi
iptables -A INPUT -s 136.201.1.250 -p tcp --dport 8080 -j ACCEPT //jboss for ejc
iptables -A INPUT -d 136.201.1.250 -p tcp --dport 993 -j ACCEPT //imaps
iptables -A INPUT -s 127.0.0.1 -p tcp --dport 111 -j ACCEPT //to speed up mail via courier. Id
iptables -A INPUT -d 136.201.1.250 -p tcp --dport 139 -j ACCEPT //samba
```

Rules of Iptables:

Iptables_Firewall

```
iptables -A INPUT -s 127.0.0.1 -p tcp --dport 143 -j ACCEPT //squirrelmail
iptables -A INPUT -p tcp --dport 4949 -j ACCEPT //munin stats
iptables -A INPUT -p tcp --dport 25 -j ACCEPT //incoming mail
iptables -A INPUT -p tcp --dport 3128 -j ACCEPT //squid
iptables -A INPUT -p udp --dport 161 -j ACCEPT //snmpd
iptables -A INPUT -p icmp -j ACCEPT //Allow ICMP Ping packets.
iptables -A INPUT -p tcp -m tcp --tcp-flags ACK -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -m state --state RELATED -j ACCEPT
iptables -A INPUT -j REJECT
#####

#####PORT FORWARDING#####
iptables -t nat -A PREROUTING -p tcp -d 136.201.1.250 --dport 8000 -j DNAT --to 136.201.146.211:80
iptables -t nat -A POSTROUTING -d 136.201.146.211 -j MASQUERADE
#####
```

Remove / Delete an individual /single Iptable Rule

```
iptables -D INPUT -s 127.0.0.1 -p tcp --dport 111 -j ACCEPT
// -D = delete appropriate rule. If you dont know the exact syntax of the rule to delete do the foll
iptables -L
//count down the number of lines until you reach the rule you wish to delete
iptables -D INPUT 4
//format = iptables -D CHAIN #Rule_No
```

Other pieces of information to remember:

```
iptables -P INPUT DROP (Setting the Default Policy)
iptables -A INPUT * * * -j ACCEPT | REJECT (send back 'connection refused') | DROP (keep quiet)
```

Iptables Forward with NAT

This is already covered on this wiki here [iptables_forward](#)

Saving ALL IPTABLE Rules

It seems that the method for saving & loading iptable rules from /etc/init.d/iptables loadsave activelinactive does not save NAT rules.

The command for saving iptable rules manually is:

```
root:~# iptables-save > rules-saved
```

There is also command called iptables-restore. It is:

```
root:~# iptables-restore rules-saved
```

fail2ban - Debian Etch/Ubuntu

Fail2ban is a simple Debian etch package which uses iptables to add rules which blocks ips after various incorrect Authentication/Password attempts. To install (etch only):

```
apt-get install fail2ban
//configuration file is in /etc/fail2ban.conf
//fail and ban logs are saved in /var/log/fail2ban.log and /var/log/faillog
```

It monitors incorrect attempts in /var/log/auth.log for ssh attempts by default. The defaults are: 5 attempts before a rule is added blocking the client ip (on port 22) for 10minutes. Its a very very nice package -)

Problems with fail2ban and ssh attempts on ubuntu

fail2ban was only banning ssh attempts where the user was "unknown". It was not stopping brute force attempts at root for example. The failregex for the sshd.conf had to be changed.

```
vi /etc/fail2ban/filter.d/sshd.conf
#change the failregex line to:
failregex = (?:Failed password [-/\w+]+) .*(?: from|FROM) <HOST>
```

It could be done a lot better, but the above works. Also see:

<http://debaday.debian.net/2007/04/>

<http://debaday.debian.net/2007/04/29/fail2ban-an-enemy-of-script-kiddies/>

Firewall on Centos / RH

http://www.linuxtopia.org/online_books/centos_linux_guides/centos_linux_reference_guide/s1-iptables-init.html

Main Page Information was Got From:

<http://www.howtoforge.com/node/450>

Good Firewall explanation & Netstat:

<http://www.aboutdebian.com/firewall.htm>

<http://www.linuxguruz.com/iptables/howto/iptables-HOWTO-6.html#ss6.2>