

Chapter 21

Security

Firewall

◎ FreeBSD firewalls

- > ipfw -- IP firewall and traffic shaper control program
 - ipfw(8)
- > ipf (IP Filter) - alters packet filtering lists for IP packet input and output
 - ipf(8)
- > pf -- packet filter
 - pf(4)

<http://www.freebsd.org/doc/en/books/handbook/firewalls.html>

Firewall (1)

Using ipfw

1. Add these options in kernel configuration file and recompile the kernel

```
options      IPFIREWALL
options      IPFIREWALL_VERBOSE
options      IPFIREWALL_FORWARD
options      IPFIREWALL_DEFAULT_TO_ACCEPT
```

2. Edit /etc/rc.conf to enable firewall
 - "firewall" keyword in rc.conf

```
# firewall
firewall_enable="YES"
firewall_script="/etc/firewalls/rules"
firewall_quiet="YES"
```

Firewall (2)

3. Edit ipfw command script that you specify in rc.conf
 - Ex: /etc/firewall/rules

- > ipfw command
 - # ipfw list (show current firewall rules)
 - # ipfw flush (delete all firewall rules)

 - # ipfw add {pass | deny} {udp | tcp | all} from where to where

Firewall (3)

- Example (Head part)

```
#!/bin/sh

fwcmd="/sbin/ipfw -q"
myip="140.113.17.215"
${fwcmd} -f flush

${fwcmd} add pass all from ${myip} to any

# Allow TCP through if setup succeeded
${fwcmd} add pass tcp from any to any established
${fwcmd} add deny log all from any to any frag
echo -n "Established "

# Allow icmp (ping only)
${fwcmd} add pass icmp from any to any icmptypes 0,3,8,11
```

Firewall (4)

◉ Example (service part)

```
# Allow Samba
${fwcmd} add pass tcp from 140.113.17.0/24 to ${myip} 137-139 setup
echo -n "Samba "
```

```
# Allow HTTP/HTTPS
${fwcmd} add pass tcp from any to ${myip} 80 setup
${fwcmd} add pass tcp from any to ${myip} 443 setup
echo -n "HTTP/HTTPS "
```

```
# SSH
${fwcmd} add pass tcp from any to any 22 setup
echo -n "SSH "
```

```
# open any system port that your system provide
```

Firewall (5)

- Example (Tail part)

```
# Default to deny
${fwcmd} add 65500 reset log tcp from any to any
${fwcmd} add 65501 reject udp from any to any
${fwcmd} add 65502 reject log icmp from any to any
${fwcmd} add 65534 deny log all from any to any
```

Firewall (6)

- ◉ Manual reset firewall rules
 - > Edit the script and
 - > # sh /etc/firewall/rules
- ◉ When you install new service and wondering why it can not use...
 - > # ipfw flush
 - > Delete all firewall rules to remove problems caused by firewall

Firewall (7)

- ◉ Debug your system via log file
 - > /var/log/security

```
Dec 25 11:25:36 sabsd last message repeated 2 times
Dec 25 11:45:06 sabsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:1997 140.113.17.215:5554 in via fxp0
Dec 25 11:45:07 sabsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:1997 140.113.17.215:5554 in via fxp0
Dec 25 11:45:07 sabsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:4062 140.113.17.215:1023 in via fxp0
Dec 25 11:45:08 sabsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:4062 140.113.17.215:1023 in via fxp0
Dec 25 11:45:09 sabsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:4246 140.113.17.215:9898 in via fxp0
Dec 25 12:05:44 sabsd kernel: ipfw: 65500 Reset TCP 204.100.126.30:2188 140.113.17.215:445 in via fxp0
Dec 25 12:05:45 sabsd last message repeated 2 times
```

Configuration Examples

- ◎ /usr/share/examples
- ◎ ipfw/
 - > /usr/share/examples/ipfw/change_rules.sh
- ◎ ipfilter/
- ◎ pf/

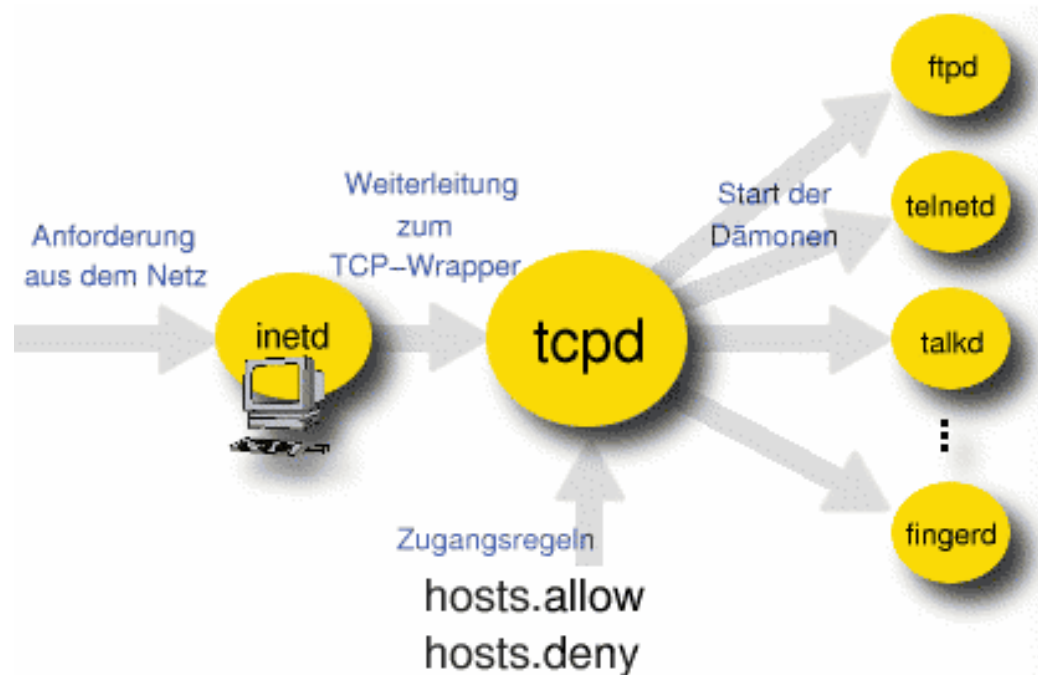
/etc/hosts.equiv and ~/.rhosts

- ◉ Trusted remote host and user name DB
 - > Allow user to login (via rlogin) and copy files (rcp) between machines without passwords
 - > Format:
 - Simple: hostname [username]
 - Complex: [+][hostname | @netgroup]
[[+][username | @netgroup]]
 - > Example
 - bar.com foo (trust user "foo" from host "bar.com")
 - +@adm_cs_cc (trust all from amd_cs_cc group)
 - +@adm_cs_cc -@chwong
- ◉ Do not use this unless you know what you are doing exactly

/etc/hosts.allow (1)

- TCP Wrapper

- > Provide support for every server daemon under its control



/etc/hosts.allow (2)

- > To see what daemons are controlled by inetd, see /etc/inetd.conf

#ftp	stream	tcp	nowait	root	/usr/libexec/ftpd	ftpd -l
#ftp	stream	tcp6	nowait	root	/usr/libexec/ftpd	ftpd -l
#telnet	stream	tcp	nowait	root	/usr/libexec/telnetd	telnetd
#telnet	stream	tcp6	nowait	root	/usr/libexec/telnetd	telnetd
shell	stream	tcp	nowait	root	/usr/libexec/rshd	rshd
#shell	stream	tcp6	nowait	root	/usr/libexec/rshd	rshd
login	stream	tcp	nowait	root	/usr/libexec/rlogind	rlogind
#login	stream	tcp6	nowait	root	/usr/libexec/rlogind	rlogind

- > TCP wrapper should not be considered a replacement of a good firewall. Instead, it should be used in conjunction with a firewall or other security tools

/etc/hosts.allow (3)

- To use TCP wrapper
 1. inetd daemon must start up with "-Ww" option (default)
Or edit /etc/rc.conf

```
inetd_enable="YES"  
inetd_flags="-wW"
```

- > Edit /etc/hosts.allow
 - Format:
daemon : address : action
 - daemon is the daemon name which inetd started
 - address can be hostname, IPv4 addr, IPv6 addr
 - action can be "allow" or "deny"
 - Keyword "ALL" can be used in daemon and address fields to means everything

/etc/hosts.allow (4)

- > First rule match semantic
 - Meaning that the configuration file is scanned in ascending order for a matching rule
 - When a match is found, the rule is applied and the search process will stop

◎ Example:

```
ALL: localhost, loghost @adm_cc_cs : allow
sshd : @sun_cc_cs, @bsd_cc_cs, @linux_cc_cs : allow
identd : ALL : allow
rpcbind : 140.113.209. 140.113.235. 140.113.23. .cs.nctu.edu.tw : allow
rpc.rstatd rpc.rusersd : 140.113.209. 140.113.235. 140.113.23. : allow
rpc.lockd rpc.statd : 140.113.209. 140.113.235. 140.113.23. : allow
mountd : 140.113.209. 140.113.235. 140.113.23. : allow
rpc.rusersd : @all_cc_cs 140.113.17.203: allow
ALL : ALL : deny
```

/etc/hosts.allow (5)

- Advance configuration
 - > External commands (twist option)
 - twist will be called to execute a shell command or script

```
# The rest of the daemons are protected.  
telnet : ALL \  
        : severity auth.info \  
        : twist /bin/echo "You are not welcome to use %d from %h."
```

- > External commands (spawn option)
 - spawn is like twist, but it will not send a reply back to the client

```
# We do not allow connections from example.com:  
ALL : .example.com \  
      : spawn (/bin/echo %a from %h attempted to access %d >> \  
      /var/log/connections.log) \  
      : deny
```


/etc/hosts.allow (6)

- > Wildcard (PARANOID option)
 - Match any connection that is made from an IP address that differs from its hostname

```
# Block possibly spoofed requests to sendmail:  
sendmail : PARANOID : deny
```

hosts_access(5)
hosts_options(5)

FreeBSD security function

- ◎ FreeBSD Security Information
 - > <http://security.freebsd.org/>
 - > <http://www.freebsd.org/security/advisories.html>
- ◎ Security Notifications List
 - > freebsd-security-notifications@freebsd.org
- ◎ See supplicant:
 - > “The FreeBSD Security Officer function”
 - <http://people.freebsd.org/~simon/presentations/>