hosts.allow, hosts.deny

These two files in **/etc** are a common place for storing rules about who you want to allow to connect to the services on your machine.

While a firewall can be considered as hiding a door, these files control who is allowed to open the door.

Used in combination, these two files can be used to create either

- default open with exclusions (ban list)
- default closed with allowances (invite list)

By default Slackware ships with both these files empty, this means the door is unlocked with no-one banned.

This document will guide you through changing that default open to a more secure default closed setup.

Contents

Making sure you have a key yourself

If you are connecting to the machine by ssh you will want to make sure that subsequent connections are allowed. If the machine you are sitting in front of is 192.168.0.10, edit **/etc/hosts.allow** and add

```
sshd:   192.168.0.10
```

If you are using dns you may also refer to your machine by name, eg

```
sshd:   wibble.mynet.invalid
```

Locking the door

This is simply done by editing **/etc/hosts.deny** and adding the line

```
All:    All
```

Connections which are in use will still be usable, only new connections via ssh from 192.168.0.10 will be allowed.

Writing the guest list

Adding a second host

We have already allowed connections only to the sshd server from 192.168.0.10, if we want to allow a second host to connect, it is as simple as

```
sshd:   192.168.0.10 192.168.0.11
```

or

```
sshd:   wibble.mynet.invalid wobble.mynet.invalid
```

You may have just a space between them or add a comma for clarity.

Adding lots of hosts

It is possible to allow blocks of addresses to connect by either shortening the address or using a netmask.

```
sshd:   192.168.0.
```

```
sshd:   192.168.0.0/255.255.255.0
```

Both have the same effect.

You can allow all within a domain name to connect, eg.

```
sshd:   .mynet.invalid
```

Adding other services

In the main, the name of the service you are connecting **TO** eg sshd, in.telnetd, vstfpd, proftpd should be placed in hosts.allow, but as with all things there are exceptions… NFS, with NFS we are making rules for what services we are allowing connections **FROM**.

If for example the machine we are locking down is an nfs server, and you want to mount it on

192.168.0.10 we would put in **/etc/hosts.allow**

```
portmap:    192.168.0.10
mountd:     192.168.0.10
```

Likewise, similarly back to front, if you want it to mount an nfs export we would put in the address of the nfsd we want to mount

```
portmap:    192.168.0.10
nfsd:       192.168.0.10
```

Talking to yourself

Sometimes it's not a bad idea, for example the rndc process for reloading bind might be on the same machine running named, in this case we want to allow connections from the same machine we are on.

```
rndc:   127.0.0.1
```

Again, note it is the name of the proccess we want to talk to, not the name of the listening process.

Notes

This does not cover all the variations in grammar of these two files nor will it secure all services that open ports but should hopefully give you a taste of what can be done.

See also

man (5) hosts_access

Sources

howtos, security, slackware allversions, inetd