hosts.allow, hosts.deny

Estos dos archivos en **/etc** son un lugar común para almacenar reglas sobre a quién desea permitir conectarse con los servicios en su máquina. Si bien se puede considerar que un firewall esconde una puerta, estos archivos controlan quién tiene permiso para abrir la puerta.

Usados en combinación, estos dos archivos pueden usarse para crear

- predeterminado abierto con exclusiones (lista de prohibición)
- predeterminado cerrado con permisos (lista de invitaciones)

Por defecto, Slackware se envía con estos dos archivos vacíos, lo que significa que la puerta está desbloqueada y nadie está prohibido.

Este documento lo guiará a través de cambiar la apertura predeterminada a una configuración cerrada predeterminada más segura.

Contenidos

Asegurándose de que ud tiene una llave

Si se está conectando a la máquina por ssh querrá asegurarse de que se permiten conexiones posteriores. Si la máquina en la que está sentado es 192.168.0.10, edite **/etc/hosts.allow** y agregue

```
sshd:   192.168.0.10
```

Si está utilizando dns, también puede referirse a su máquina por su nombre, por ejemplo

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

Cerrando las puertas

TEsto se hace simplemente editando **/etc/hosts.deny** y agregando la línea

```
All:    All
```

Las conexiones en uso seguirán siendo utilizables, solo se permitirán nuevas conexiones a través de ssh desde 192.168.0.10.

Escribiendo la lista de anfitriones invitados

Añadiendo un segundo host

Ya hemos permitido conexiones solo al servidor sshd desde 192.168.0.10. Si queremos permitir que un segundo host se conecte, es tan simple como

```
sshd:   192.168.0.10 192.168.0.11
```

o

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

Puede tener solo un espacio entre ellos o agregar una coma para mayor claridad.

Añadiendo un montón de hosts

Es posible permitir que los bloques de direcciones se conecten acortando la dirección o utilizando una máscara de red.

```
sshd:   192.168.0.
```

```
sshd:   192.168.0.0/255.255.255.0
```

Ambos tienen el mismo efecto.

Puede permitir que todo dentro de un nombre de dominio se conecte, por ejemplo.

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

Añadiendo otros servicios

En general, el nombre del servicio que está conectando **TO** por ejemplo, sshd, in.telnetd, vstfpd, proftpd se debe colocar en hosts.allow, pero como con todas las cosas, hay excepciones ... NFS, con NFS estamos haciendo reglas para los servicios que estamos permitiendo conexiones **DE** .

Si, por ejemplo, la máquina que estamos bloqueando es un servidor nfs, y desea montarla en 192.168.0.10, pondríamos **/etc/hosts.allow**

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

Del mismo modo, de manera similar, si desea que se monte una exportación de nfs, pondremos la dirección de nfsd que queremos montar

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

Hablando contigo mismo!

A veces no es una mala idea, por ejemplo, el proceso rndc para volver a cargar el enlace podría estar en la misma máquina que se ejecuta con el nombre, en este caso queremos permitir conexiones desde la misma máquina en la que estamos.

```
rndc:   127.0.0.1
```

Nuevamente, tenga en cuenta que es el nombre del proceso con el que queremos hablar, no el nombre del proceso de escucha.

Notas

Esto no cubre todas las variaciones en la gramática de estos dos archivos ni asegurará todos los servicios que abren puertos, pero con suerte debería darle una idea de lo que se puede hacer.

Ver también

man (5) hosts_access

Sources

howtos, security, slackware allversions, inetd