hosts.allow, hosts.deny

Эта пара файлов в **/etc** является общепринятым местом для хранения правил о том, кому вы хотите позволить подключаться к службам вашей машины.

Если фаервол можно рассматривать как сокрытие двери, то эти файлы управляют тем, кому её позволено открывать.

При помощи этой пары файлов, использованная совместно, можно задать умолчания:

- всем разрешено, кроме исключённых (список запретов);
- всем запрещено, кроме допущенных (список приглашений).

По умолчанию в Slackware оба указанных файла пусты, то есть, дверь открыта всем.

Этот документ покажет, как изменить умолчание с “открыто” на более безопасное “закрыто”.

Содержание

1. Убедимся, что ключ у нас
2. Запрем дверь
3. Подготовим список гостей
    1. Добавим другой хост
    2. Добавим группу хостов
    3. Добавим другие службы
    4. Поговорим с собой
4. Примечания
5. См. также

Убедимся, что ключ у нас

Если вы подключаетесь к машине по ssh, вам захочется быть уверенным, что последующие подключения будут разрешены. Если вы сидите за машиной 192.168.0.10, отредактируйте **/etc/hosts.allow**, добавив

```
sshd:   192.168.0.10
```

Если вы используете DNS, вы также можете сослаться на машину по имени, например,

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

Запрем дверь

Для этого просто отредактируем **/etc/hosts.deny**, добавив строку

```
All:    All
```

Уже установленные соединения останутся, новые подключения через ssh будут разрешены только с 192.168.0.10.

Подготовим список гостей

Добавим другой хост

Ранее мы разрешили подключения к серверу sshd только с 192.168.0.10, если мы хотим позволить подключения другому хосту, то это несложно

```
sshd:   192.168.0.10 192.168.0.11
```

или

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

Вы можете просто поставить между ними пробел или добавить запятую для ясности.

Добавим группу хостов

Возможно выдать разрешение на подключение блоку адресов, сократив адрес или используя сетевую маску.

```
sshd:   192.168.0.
```

```
sshd:   192.168.0.0/255.255.255.0
```

Оба варианта равнозначны.

Вы можете позволить подключаться всем из домена по имени, например,

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

Добавим другие службы

Как правило, используется имя службы **КУДА** подключаются, например, в hosts.allow указывают sshd, in.telnetd, vstfpd, proftpd, но нет правил без исключений… NFS, для NFS мы указываем в правилах **ОТКУДА** каким службам мы разрешаем подключаться.

Если, например, защищаемая машина является сервером NFS, и вы собираетесь монтировать её на 192.168.0.10, мы укажем в **/etc/hosts.allow**

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

Аналогично и наоборот, чтобы там смонтировать экспорт NFS, мы укажем адрес nfsd, который

хотим смонтировать

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

Поговорим с собой

Иногда это неплохая идея, например, процесс rndc для перезагрузки bind может быть на той же машине, что и named, в этом случае мы захотим разрешить подключения с той машины, на которой мы находимся.

```
rndc:   127.0.0.1
```

Ещё раз, обратите внимание, указано имя процесса с которым мы будем общаться, а не имя слушающего процесса.

Примечания

Описанное здесь не охватывает всех вариантов грамматики указанных двух файлов и не защитит все службы, открывающие порты, но, надеюсь, даст вам почувствовать, что возможно сделать.

См. также

man (5) hosts_access

howtos, security, slackware allversions, translator bormant

From:
https://docs.slackware.com/ - **SlackDocs**

Permanent link:
https://docs.slackware.com/ru:howtos:security:inetd

Last update: **2012/11/11 15:46 (UTC)**