iptables – restore script

Правила iptables применяются сразу же после выполнения.

К примеру, если в терминале ввести:

```
$ iptables -A INPUT -p TCP --dport 22 -j DROP
```

то соединение по ssh сразу будет потеряно.

Создадим скрипт, который будет очищать все правила iptables:

```
# vim /etc/restore_iptables.sh

#!/bin/sh
IPT="/sbin/iptables"
# Удаляем все правила
$IPT -F
$IPT -X
# Разрешаем все подключения
$IPT -P INPUT ACCEPT
$IPT -P FORWARD ACCEPT
$IPT -P OUTPUT ACCEPT
```

Также нужно сделать скрипт исполняемым:

```
# chmod +x /etc/restore_iptables.sh
```

В случае потери доступа к удаленному хосту в результате неправильной настройки iptables, мы восстановим рабочую конфигурацию из файла /etc/restore_iptables.sh, сбросив новые настройки к заведомо рабочим. Для этого добавим в cron периодический запуск /etc/restore_iptables.sh

```
crontab -e

# Сбрасывать iptables к рабочим настройкам каждые 5 минут

*/5 * * * * /etc/restore_iptables.sh
```

http://www.natalink.ru/articles/nastroyka_iptables_na_udalennom_hoste