iptables – логирование в отдельный файл

Надоело смотреть мусор от логов iptables в файле messages. Исправляем. Если rsyslog уже установлен в системе, то создаем конфигурационный файл:

```
# touch /etc/rsyslog.d/10-iptables.conf
```

Имя с цифрой 10 (10-iptables) – так как для демона важен порядок конфигурационных файлов, а в системе уже присутствует 50-default.conf, он бы первый заворачивал все логи в messages.

```
# vi /etc/rsyslog.d/10-iptables.conf
```

```
:msg, contains, "iptables denied: " -/var/log/iptables.log
& stop
:msg, contains, "Ping detected: "   -/var/log/iptables.log
& stop
```

Строка с “:msg” говорят rsyslog, что нужно искать в логе фразы “iptables denied: ” или “Ping detected: ” -/var/log/iptables.log, и когда он их находит, то переносит в файл /var/log/iptables.log.

Строка с “& stop” просто дает понять rsyslog, чтобы найденные строки, подходящие под условия, не дублировались в основной лог /var/log/messages.

```
# service rsyslog restart
```