Представляю пример настройка **Fail2Ban** с **IPTABLES LOG**. Настройку ядра опускаем.
1. Добавим правило:
iptables -A INPUT -i ${WAN} -p tcp -m tcp --tcp-flags FIN,SYN,ACK SYN -j LOG --log-prefix "TCP: " Все что не попало выше в ACCEPT будет сыпаться в лог. 2. У меня стоит Metolog. Добавил правило в **metalog.conf**
IPTables :

regex = "TCP: "
logdir = "/var/log/iptables"
break = 1

Все логи с IPTAbles будут сыпаться в отдельный файл **/var/log/iptables/current** 3. Дбавляем фильтр в
Fail2ban
:
nano /etc/fail2ban/filter.d/ip_tables.conf

[Definition]
failregex = TCP: .* SRC=.*$
ignoreregex =
4. Добавляем правило в Fail2Ban: **nano /etc/fail2ban/jail.conf**
[ipt-kernel]

enabled = true
filter = ip_tales
action = iptables-allports[name=IPT, protocol=tcp]
logpath = /var/log/iptables/current
maxretry = 3

После перезапуска сервиса fail2ban и при повытке перебора паролей или достучатс до вас, сработает блокровка. Вы можете изменить правило поверки в филтре и протестировать его командой: **fail2ban-regex /var/log/iptables/current /etc/fail2ban/filter.d/ip_tables.conf**