

//

- Как организовать нарезку канала для определенного диапазона IP-адресов при использовании NAT или Squid?
- Какие дисциплины лучше использовать для распределения канала?
- Как ограничить скорость для VPN-клиентов?
- Есть ли удобный модуль настройки traffic shaping и iptables через Web-интерфейс?
- Возможно ли организовать синхронный канал?

Начну с последнего... Возможно! И делается только по средствам утилит [tc](#) и [iptables](#) , т.к. не в

[CBQ.init](#)

и не в

[HTB.init](#)

такой возможности не имеется (во всяком случае я ее не нашел). Теперь по порядку.

Отмечу, что

[изучаемые](#)

усердно

TrEK

'ом политики являются ничем иным, как скриптами, генерирующими набор правил для [tc](#)

и написаны лишь для того, чтобы упростить работу с данной утилитой. Соответственно, при использовании NAT'а, логичнее всего использовать эти скрипты в связке с

[Internet sharing](#)

'ом на определенные IP-адреса, чтобы не возникало вопросов с остатками канала . Для большей уверенности в собственной защищенности почитайте

[эту](#)

статью.

[Вот](#)

статья, которая мне помогла в решении первого и, самое главное, последнего вопроса. В случае со Squid'ом, логичнее всего использовать описанный

[выше](#)

[метод](#)

. Но в таком случае не возможно реализовать синхронный канал! Мои эксперименты по заварачиванию исходящего трафика в трубы сквида закончились неудачей (если кому удавался сей фокус, отпишитесь плз).

Ответом на второй вопрос послужит [эта](#) статья. Я лишь могу отметить, что дисциплина обработки очереди

[CBQ](#) является более

сложной в настройке и требует глубоких знаний от системного администратора. Но позволяет производить более тонкую настройку распределения разных видов трафика, т.е. резать скорость по разным портам (грубо говоря...).

[HTB](#)

проще и не требует классификации по виду трафика, хотя обе дисциплины настраиваются практически аналогично...

Для VPN-клиентов также применимы описанные выше дисциплины. Отличие состоит лишь в том, что при создании конфигурационных файлов, лежащих в /etc/sysconfig/htb для HTB необходимо назвать их в соответствии с поднятым VPN-сервером интерфейсом. Например: pppX, pppX-2.root, pppX-2:05.default, pppX-2:06.lanload, pppX-2:07.client и т.д. Для real-админов можно сразу настроить tc, как написано [тут](#) .
Есть несколько вариантов:

- [Webmin](#) и устанавливаемые под него модули [webmin-cbq](#) и [webmin-htb](#) .

Инструкция по установке webmin-htb

[тут](#)

. Инструкцию по установке webmin-cbq потерял... Найдете, отпишитесь... Кста, установка

[webmin](#)

на "свежий" сервак для меня давно обычное дело на ряду с настройкой системного времени, которое я через него и настраиваю . Но есть один недостаток. При помощи лишь этих модулей нельзя настроить синхронный канал. придется подправить ручками конфиги, как указано в

[статье](#)

и вручную, но в модуле "Межсетевой экран (firewall)" вебмина добавить правила маркировки пакетов и заворачивания их в трубы. Со встроенным модулем "Прокси-сервер Squid" в вебмин "Delay Pools" настраивается в два клика.

- [WebCBQ Bandwidth Manager](#) , который я нашел в процессе написания поста .

[MasterShaper](#) , который я установил, запустил, но не смог применить сгенерированные им правила. Инструкция по установке в архиве с программой. Достоинства: есть возможность задания разных дисциплин, доступ по паролю, графическое отображение загрузки канала в виде графика, пошаговая компиляция правил для tc с возможностью коррекции (не плохо, как для ОпенСорс). Недостатки: нет возможности создавать каналы более чем на двух интерфейсах (входящий/исходящий), в инструкции нет указаний с какими правами должен работать мастер (мне не удалось применить правила. У кого получилось, отпишитесь плз). [Вот](#) типичная настройка для использования данной софтины.

оригинал: <http://forum.ubuntu.ru/index.php?topic=33853.75>