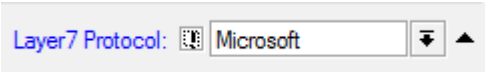
Mikrotik — L7 Protocol
Блокировка Сайтов

Сразу скажу, что использовать нужно L7 Protocol. Казалось бы, чего сложного: просто применить правило «все кроме».



Но нет, это не работает. Если хотите, проверьте сами. Что делать? Одним фильтром разрешить нужные ресурсы и вторым запретить все остальные.

**Разрешающий L7 имеет вид ^.+*(какой-то_сайт|еще какой-то_сайт).*$*.
С запрещающими сложнее. Можно зафильтровать вообще все через ^.+$. Но я бы посоветовал фильтровать протокол HTTP по URI, то есть так — ^.+*(HTTP\/[0-2]).+$*.
К сожалению, через терминал необходимые L7-фильтры добавляются с пустым полем regexp. Используйте вместо этого Winbox.**

```
/ip firewall layer7-protocol add name=Allow regexp="^.+(какой-то_сайт|еще_какой-
то_сайт).*$"
/ip firewall layer7-protocol add name=Deny regexp="^.+(HTTP\/[0-2]).+$"
```

Добавление самих фильтры, по 2 на 'разрешить' и 'запретить' согласно вики Микротик

```
/ip firewall filter add chain=forward protocol=tcp out-interface=ваш_интерфейс
layer7-protocol=Allow action=accept
/ip firewall filter add chain=forward protocol=tcp in-interface=ваш_интерфейс
layer7-protocol=Allow action=accept
/ip firewall filter add chain=forward protocol=tcp out-interface=ваш_интерфейс
layer7-protocol=Deny action=reject reject-with=tcp-reset
/ip firewall filter add chain=forward protocol=tcp in-interface=ваш_интерфейс
layer7-protocol=Deny action=reject reject-with=tcp-reset
```

Небольшое уточнение для тех, кому все-таки требуется разрешить строго определенные сайты: проверяйте, какие еще ресурсы задействованы на сайте. К примеру, это могут быть подгружаемые карты. Я использую Opera для серфинга в сети, а так же входящий в нее DevTools, вкладка «Console» для определения ошибок.

Доменные имена в адресных листах

И на сладкое: начиная с версии v6.36, в адресные листы можно добавлять доменные имена!

> *) firewall — allow to add domain name to address-lists (dynamic entries for resolved addresses will be added to specified list);

Если вы еще не прыгаете от радости как я, то самое время начать. Эта фича позволяет практически полностью уйти от использования затратного L7 с его ограничениями.
В качестве примера приведу маршрутизацию разных сайтов в разные шлюзы. Это актуально в связи с действительностью в нашей стране.

Заворачивать будем web-интерфейсы почтовых серверов mail.google.com и e.mail.ru. В почту Google будем ходить по OVPN, а в Mail — по L2TP.

```
/ip firewall address-list add list=ovpn address=mail.google.com
/ip firewall address-list add list=l2tp address=e.mail.ru
/ip firewall mangle add chain=prerouting protocol=tcp src-address=192.168.1.0/24
dst-address-list=ovpn action=mark-routing new-routing-mark=ovpn-route
/ip firewall mangle add chain=prerouting protocol=tcp src-address=192.168.1.0/24
dst-address-list=l2tp action=mark-routing new-routing-mark=l2tp-route
/ip route add dst-address=0.0.0.0/0 gateway=ovpn-out1 distance=1 routing-
mark=ovpn-route
/ip route add dst-address=0.0.0.0/0 gateway=l2tp-out1 distance=1 routing-
mark=l2tp-route
```

Таким образом, при добавлении нужного имени в определенный лист, мы фактически определяем по какому каналу будет установлена связь.
Еще один пример, который многим пригодится: перенаправлять все TCP-соединения в шлюз OVPN, а rkn.gov.ru — в шлюз по умолчанию.

```
/ip firewall address-list add list=RKN address=rkn.gov.ru
/ip firewall mangle add chain=prerouting protocol=tcp src-address=192.168.1.0/24
dst-address-list=RKN action=accept
/ip firewall mangle add chain=prerouting protocol=tcp src-address=192.168.1.0/24
dst-address=!192.168.0.0/16 action=mark-routing new-routing-mark=ovpn-route
/ip route add dst-address=0.0.0.0/0 gateway=ovpn-out1 distance=1 routing-
mark=ovpn-route
```

Важное замечание: если вы используете Fasttrack, то обязательно смотрите его описание. А именно:

> Fasttracked packets bypass firewall, connection tracking, simple queues, queue tree with parent=global, ip traffic-flow(restriction removed in 6.33), ip accounting, ipsec, hotspot universal client, vrf assignment, so it is up to administrator to make sure fasttrack does not interfere with other configuration;

Что значит, что соединения такого типа не попадают в файервол, обработку пакетов, очереди и т.д.