Как сделать умную защиту от атак на Микротике ?

Оригинальная инструкция лежит [здесь](https://wiki.merionet.ru/articles/umnaya-zashhita-ot-atak-mikrotik).

*Данный метод основан на простом блокировании заведомо*

*вредоносных IP адресов, которые были замечены в подозрительной*

*активности – сканирование, брутфорс, неудачные попытки доступа к различным сервисам,*

*только всё это делается не вручную, а в автоматическом режиме.*

*Существует много открытых ресурсов, которые собирают информацию о таких «чёрных» IP адресах и генерируют актуальные списки, которые мы можем просто загружать на наш роутер с помощью нехитрого скрипта.*

*К таким ресурсам относятся:*

***Blocklist.de –*** *бесплатный открытый ресурс, чьи сервера часто подвергаются различного рода атакам, таким как атаки на ssh, почтовых и файловых сервисов, веб-серверов и т.д. IP адреса атакующих заносятся в список и выкладываются в общий доступ;*

***dshield.org –*** *генерирует списки из топ-20 подсетей, из которых за последние трое суток совершалось наибольшее количество атак;*

***Spamhaus –*** *генерирует списки IP адресов, замеченных в «спаммерской» активности, а также «угнанных» устройств, с помощью которых также осуществляется вредоносная деятельность;*

*Итак, чтобы заблокировать адреса из этих списков, нужно сначала создать блокирующее правило на нашем роутере.*

1. Заходим на Микротик через Winbox и открываем терминал (New Terminal) и копируем туда следующие команды:

ip firewall raw add chain=prerouting src-address-list="sbl dshield" action=drop comment="sbl dshield"

ip firewall raw add chain=prerouting src-address-list="sbl spamhaus" action=drop comment="sbl spamhaus"

ip firewall raw add chain=prerouting src-address-list="sbl blocklist.de" action=drop comment="sbl blocklist.de"

Таким образом, мы создали 3 правила во вкладке Raw, по цепочке prerouting, которые будут блокировать подключения к нашему роутеру из списков каждого ресурса – dshield, smaphaus и blocklist.de.

Все эти подключения будут блокироваться ещё до того, как попадут в Firewall.

1. Теперь нужно настроить автоматический загрузчик, который будет обращаться на данные ресурсы за актуальными списками и загружать их в конфиг роутера.  
   Для этого открываем вкладку:

**System – Scheduler – (+)**

Задачу на проверку обновления списков вредоносных ресурсов ставим,

начиная с полуночи следующего числа каждые 12 часов.

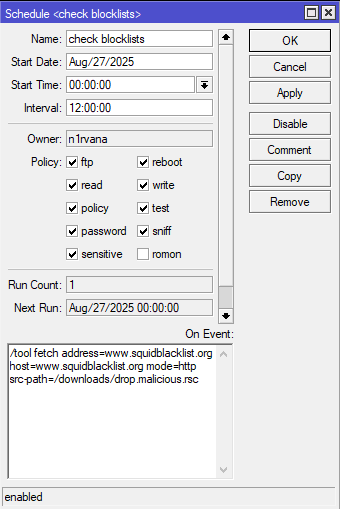
Обращение будет происходить посредством простого http запроса к ресурсу

[www.squidblacklist.org/downloads/drop.malicious.rsc](http://www.squidblacklist.org/downloads/drop.malicious.rsc).

Для этого, в поле **On Event** прописываем вот такую команду:

/tool fetch address=www.squidblacklist.org host=www.squidblacklist.org mode=http src-path=/downloads/drop.malicious.rsc

Должно получиться вот так:



1. Теперь создадим ещё одну задачу на импорт списка в конфиг роутера, спустя минуту после того, как отработает проверка актуальности списков из первой задачи.

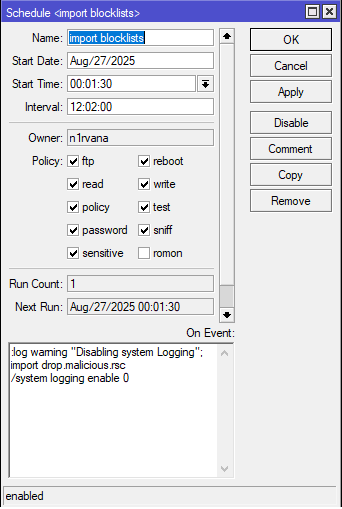
На этот раз в поле **On Event** напишем:

:log warning "Disabling system Logging";

import drop.malicious.rsc

/system logging enable 0

Должно получиться вот так:



*Теперь наш роутер будет автоматически запрашивать актуальные списки вредоносных IP адресов и добавлять их в блок.*

Общий план, как это должно выглядеть в боевых условиях.

