

# Использование оборудования Микротик для защиты локальных ресурсов.

Дмитрий Калинин  
WiFiMag  
dk@trtg.ru

# Презентацию подготовил

Дмитрий Калинин

Компания Wifimag.ru

Официальный консультант Mikrotik



Сертифицированный тренер Mikrotik



# Безопасность локальных ресурсов

Основные принципы межсетевого экрана MikroTik:

- 1) Выполнение правил с номерами от меньшего к большому
- 2) Логическая схема соответствия «**Если**»-«**То**» (**if, then**)

# Проектирование схемы безопасности

Проектирование доступа к ресурсам по двум принципам:

- 1) Разрешено все, что не запрещено – общедозволятельный тип
- 2) Запрещено все, что не разрешено – разрешительный тип

# Проектирование схемы безопасности



ОБЩЕДОЗВОЛИТЕЛЬНЫЙ ТИП



РАЗРЕШИТЕЛЬНЫЙ ТИП

# Разрешено все что не запрещено

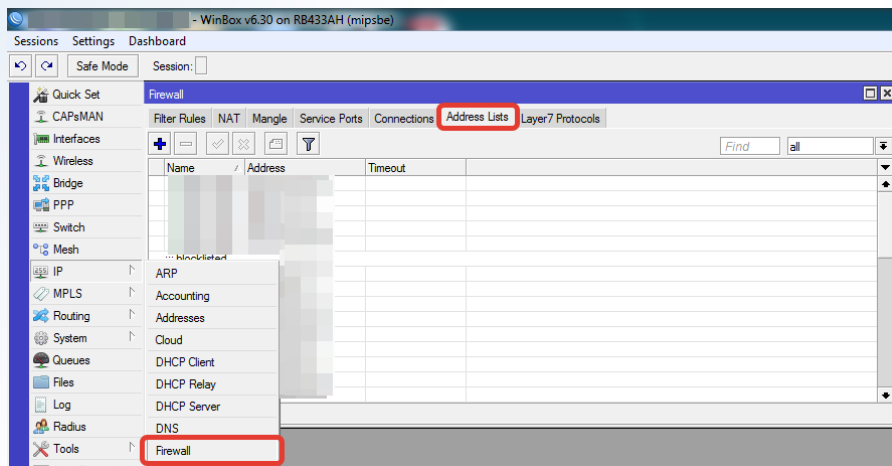
Такая логическая схема в основном используется ISP.

Используется для обеспечения доступа к глобальной сети Internet.

Минимизация возможных проблем с доступом к ресурсам.

# Использование “address list” в RouterOS

- 1) Позволяют формировать списки адресов для использования
- 2) Позволяют минимизировать количество правил
- 3) Могут формироваться как вручную, так и динамически.



# Цепочки Input\output\forward

**Input** – используется для определения пакета, адресом назначения которого является непосредственно маршрутизатор. (трафик приходит на микротик)

**output** – используется для определения пакета, отправителем которого является маршрутизатор (трафик отправляет сам микротик)

**forward** – используется для определения пакета, который маршрутизатор должен перенаправить (например: из локальной сети в интернет или обратно)



# PortKnocking

- 1) Полностью закрытый доступ к маршрутизатору «из вне» до «простукивания».
- 2) Возможность разграниченного доступа при использовании разных последовательностей «простукивания»
- 3) Используется только цепочка **input**
- 4) Возможность использования практически любого устройства для генерации «простукивающих» пакетов

Возможна любое количество портов для «простукивания».

Использование портов двух протоколов для «простукивания» по портам - TCP\UDP.

Можно использовать какой-то один протокол или одновременно оба.

Бесчётное количество возможных комбинаций. (в каждом протоколе по 65536 портов ).

# PortKnocking

```
/ip firewall filter
```

```
add action=add-src-to-address-list address-list=knock-stage-1 \  
    address-list-timeout=5s chain=input dst-port=10000 protocol=tcp \  
add action=add-src-to-address-list address-list=knock-stage-2 \  
    address-list-timeout=5s chain=input dst-port=20000 protocol=udp \  
    src-address-list=knock-stage-1 \  
add action=add-src-to-address-list address-list=knock-success \  
    address-list-timeout=30m chain=input dst-port=30000 protocol=tcp \  
    src-address-list=knock-stage-2 \  
add chain=input src-address-list=knock-success \  
add action=drop chain=input disabled=yes
```

# PortKnocking

admin@ (mipsbe)

Sessions Settings Dashboard

Safe Mode Session:

Quick Set  
Interfaces  
Wireless  
Bridge  
PPP  
Switch  
Mesh  
IP  
MPLS

Firewall

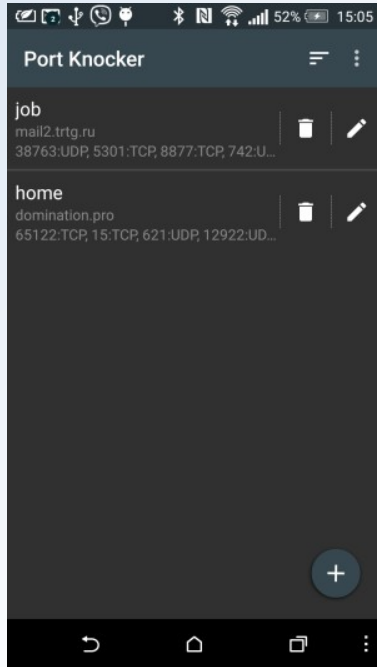
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

+ - [check] [x] [info] [filter] 00 Reset Counters 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	add...	input			6 (tcp)		10000			0 B	0
1	add...	input			17 (u...		20000			0 B	0
2	add...	input			6 (tcp)		30000			0 B	0
3	acc...	input								2638 B	29
4	drop	input								123 B	1

# PortKnocking mobile client

Android



iOS



# PortKnocking desktop client

Клиент, который будет «простукиваться» может быть установлен и на любую десктопную OS. Например Windows, MacOS, Linux, Unix и другие.

# ICMP Knocking

Может быть использован для открытия доступа, например, для другого устройства Mikrotik. В том случае, когда необходимо организовать, допустим PPTP соединение, к PPTP-серверу, организованному на устройстве под управлением RouterOS

Отличается от стандартного PortKnock тем, что в данной системе используются не номера портов, а размер ICMP пакета. Когда несколько последовательных ICMP-пакетов с заранее определенными размерами «открывают» доступ.

# ICMP Knocking

```
/ip firewall filter
add chain=input src-address-list=knock-success
add action=add-src-to-address-list address-list=icmp-knock-1 \
    address-list-timeout=5s chain=input packet-size=68 protocol=icmp
add action=add-src-to-address-list address-list=icmp-knock-2 \
    address-list-timeout=5s chain=input packet-size=39 protocol=icmp \
    src-address-list=icmp-knock-1
add action=add-src-to-address-list address-list=knock-success \
    address-list-timeout=30m chain=input packet-size=115 protocol=icmp \
    src-address-list=icmp-knock-2
add action=drop chain=input
```

# ICMP Knocking Client

В качестве клиента для «простукивания» может выступать любая ОС, поддерживающая возможность ICMP – echo запросов (ping)  
В зависимости от настройки времени, можно задать интервал пакетов 60 секунд и, если пользуетесь ОС Windows, отправлять пакеты вручную.



# ICMP Knocking Client

```
Обмен пакетами с 172.16.16.1 по с 68 байтами данных:
Превышен интервал ожидания для запроса.

Статистика Ping для 172.16.16.1:
  Пакетов: отправлено = 1, получено = 0, потеряно = 1
  (100% потеря)
Control-C
^C
C:\Users\Deneb>ping 172.16.16.1 -l 39

Обмен пакетами с 172.16.16.1 по с 39 байтами данных:
Превышен интервал ожидания для запроса.

Статистика Ping для 172.16.16.1:
  Пакетов: отправлено = 1, получено = 0, потеряно = 1
  (100% потеря)
Control-C
^C
C:\Users\Deneb>ping 172.16.16.1 -l 115

Обмен пакетами с 172.16.16.1 по с 115 байтами данных:
Превышен интервал ожидания для запроса.

Статистика Ping для 172.16.16.1:
  Пакетов: отправлено = 1, получено = 0, потеряно = 1
  (100% потеря)
Control-C
^C
C:\Users\Deneb>ping 172.16.16.1

Обмен пакетами с 172.16.16.1 по с 32 байтами данных:
Ответ от 172.16.16.1: число байт=32 время<1мс TTL=64
Ответ от 172.16.16.1: число байт=32 время<1мс TTL=64
Ответ от 172.16.16.1: число байт=32 время<1мс TTL=64
Ответ от 172.16.16.1: число байт=32 время<1мс TTL=64
```

# RouterOS ICMP Knocking Client

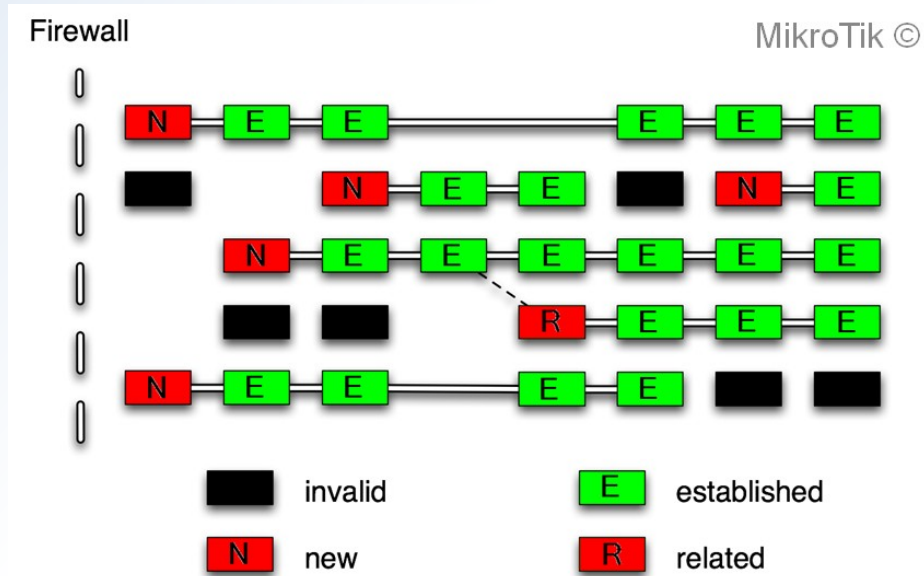
```
:if ([:len [/interface find name=tunnel-pptp  
running=no disabled=no ]] > 0) do={  
/ping address=217.197.241.18 count=1 size=68  
/ping address=217.197.241.18 count=1 size=39  
/ping address=217.197.241.18 count=1 size=115  
}
```

name=**tunnel-pptp** – имя интерфейса pptp клиента, устанавливаемого до устройства.

# Connection State

Существует 4 основных типа состояния соединения:

- 1) New
- 2) Established
- 3) Related
- 4) Invalid



# ICMP Knocking

## Connection State

- 1) Позволяет снизить вычислительную нагрузку маршрутизатора
- 2) Позволяет подключаться и использовать соединения больше времени разрешенного правилами portknocking'a
- 3 )Отличная возможность чтобы открыть доступ на несколько секунд, за время которых будет произведено подключение к удаленному сервису или туннельному серверу и оставаться «подключенными» при закрытии временного разрешения на подключения.

# Port Scanning prevention

Достаточно серьезно усиливает общую безопасность, особенно при использовании вместе с portknocking'ом

```
/ip firewall filter
add action=drop chain=input comment="drop port scanners" src-address-list="port scanners"
add action=jump chain=input comment="port scanning check" jump-target=port-scan protocol=tcp
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=port-scan comment="Port PSD scan" protocol=tcp psd=21,3s,3,1
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=port-scan comment="NMAP FIN Stealth scan" protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=port-scan comment="SYN/FIN scan" protocol=tcp tcp-flags=fin,syn
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=port-scan comment="SYN/RST scan" protocol=tcp tcp-flags=syn,rst
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=port-scan comment="FIN/PSH/URG scan" protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=port-scan comment="ALL/ALL scan" protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
|chain=port-scan comment="NMAP NULL scan" protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
```

# ***Ваши вопросы?***

Web: <http://wifimag.ru/teaching/>

Email: [dk@trtg.ru](mailto:dk@trtg.ru)

Tel: +7(495)226-37-87

Tel: 8(800)250-37-87

Компания WiFimag проводит набор в группы для проведения тренингов по курсам:  
MTCMA, MTCWE, MTCTCE, MTCRE

Предварительные даты проведение – окончание Ноября.

Более точная информация на нашем сайте - <http://wifimag.ru/teaching/>

***Спасибо за внимание!***