УДК 004.056.53 DOI: 10.25206/978-5-8149-3487-1-2022-1–191-197

ЗАЩИТА ТРАФИКА ПРИ ПЕРЕХОДЕ МЕЖДУ КАБЕЛЬНЫМ И БЕСПРОВОДНЫМ УЧАСТКАМИ СЕТИ

В. Н. Кулинченко, А. В. Воруев, М. В. Кузеев

Учреждение образования "Гомельский государственный университет имени Франциска Скорины", г. Гомель, Республика Беларусь

Аннотация. *В статье раскрывается подход к организации перехода L2 Ethernet трафика в L2 WIFI средствами проприетарной RouterOS для формирования изолированного сегмента объединенной кабельной и беспроводной сети.*

Ключевые слова: WiFi, Ethernet, bridge, MikroTik, RouterOS, DNS, DHCP.

PROTECTION OF TRAFFIC BETWEEN CABLE AND WIRELESS SECTIONS OF THE NETWORK

V. N. Kulinchenko, A. V. Varuyeu, M. V. Kuzeev

Francisk Skorina Gomel State University, Gomel, Republic of Belarus

Annotation. *The article reveals an approach to organizing the transition of L2 Ethernet traffic to L2 WIFI using proprietary RouterOS to form an isolated segment of a cable and wireless network.*

Keywords: *WiFi, Ethernet, bridge, MikroTik, RouterOS, DNS, DHCP*.

1. Введение

Информационные потоки вычислительного процесса операционной системы ориентированы на реализацию следующей процедуры: получение данных от внешних источников (IoT), передачи их на удаленную обработку (Cloud), получение результатов вычисления и выдачу пользователю или инициировавшей информационный транзакт программе. Беспроводной сегмент сети охватывает большую часть современной сетевой инфраструктуры на стороне пользователя. Одним из новых направлений, которому следует уделить особое внимание при проведении исследований, является граница перехода сетевого трафика беспроводной сети между разнородными стандартами. Например, WiFi-

Ethernet, WiFi-ZigBee, ZigBee -Bluetooth или Bluetooth-NFC. В рамках гибридного устройства связи такой переход осуществляется с помощью проприетарных программных средств. Примеры уязвимостей информационной безопасности в этой точке движения сетевого трафика были зафиксированы.

2. Решение задачи

Среди широкого выбора бюджетных маршрутизаторов нужно отметить продукцию латвийской фирмы MikroTik. Обладая скромной ценой сопоставимой с самыми бюджетными аналогами, они тем не менее имеют значительное преимущество в функционале. На них установлена операционная система RouterOS, благодаря чему даже в самых дешевых моделях присутствует весь спектр сетевых настроек и возможностей.

RouterOS – сетевая операционная система на базе Linux. RouterOS предназначена для установки на маршрутизаторы MikroTik RouterBOARD. Также данная система может быть установлена на ПК или виртуальную машину.

Маршрутизатор подключается к сети, подается питание и запускается на компьютере winbox. На вкладке Neighbors утилита найдет маршрутизатор. Это может занять какое-то время. На всякий случай можно нажать Refresh, если роутер долго не обнаруживается.

Перед началом настройки маршрутизатора нужно проверить обновления ОС и загрузчика. У компании MikroTik на данный момент есть четыре ветки для загрузки RouterOS.

RouterOS – это операционная система. RouterBOOT – это загрузчик, аналог BIOS на x86.

Обновления выпускаются в трех ветках:

- Long-term (ранее – bugfix only) – только исправление ошибок.

- Stable (ранее – Current) – исправление ошибок и новый функционал, который, в свою очередь, может внести новые ошибки.

- Testing (ранее – Release Candidate) – тестовая версия, которая содержит самый последний функционал и является потенциально нестабильной.

- Development – версии для разработчиков.

Обновление RouterOS для получения актуальных модулей осуществляется через консоль командой:

```
/system package update check-for-updates Install
```

Перед началом настройки сбрасываются настройки по умолчанию через winbox или терминал:

```
system reset-configuration no-defaults=yes
```

Меняется учетная запись по умолчанию admin на уникальную и выставляется пароль необходимой сложности. Запись Admin удаляется.

Отключается протокол обнаружения MNDP из внешних интерфейсов.

По умолчанию порты не объединены. Объединение портов может быть сделано с помощью мостового соединения (bridging). Даже если изначально они подключены через один свич-чип. Для того, чтобы коммутация начала работать нужно объединить порты через Bridge-интерфейс.

Каким именно образом будет осуществляться коммутация через ядро ОС или через свич-чип в случае его наличия определяется с помощью опции «Hardware Offload». Если эта опция включена для порта и этот порт входит в состав встроенного коммутатора, то коммутация между портами одного коммутатора будет идти через свич-чип.

Необходимость отключения «Hardware Offload» в зависимости от функционала может изменяться в зависимости от версии RouterOS.

Bridge-интерфейс для локальной сети:

```
interface bridge add name=bridge-LAN.
```

Интерфейсы, которые должны быть в локальной сети, размещаются в bridge-интерфейс локальной сети:

```
interface bridge port add bridge=bridge-LAN interface=ether2
interface bridge port add bridge=bridge-LAN interface=ether3
interface bridge port add bridge=bridge-LAN interface=ether4
interface bridge port add bridge=bridge-LAN interface=ether5
NAT: /ip firewall nat add action=masquerade chain=srcnat out-interface=ether1
```

DHCP-сервер для локальной сети:

```
/ip pool add name=LAN-DHCP-pool ranges=192.168.254.101-192.168.254.200
/ip dhcp-server add address-pool=LAN-DHCP-pool disabled=no interface=bridge-LAN lease-time=1d name=LAN-DHCP-Server
/ip dhcp-server network add address=192.168.254.0/24 dns-server=192.168.254.254 gateway=192.168.254.254
```

Прописываются вышестоящие DNS-серверы и разрешаются запросы к DNS-серверу от других устройств:

```
/ip dns set allow-remote-requests=yes servers= 82.209.213.51
```

Настраивая время используется протокол SNTP и указывается локальный time-сервер:

```
/system ntp client set enabled=yes server-dns-names=belgim.by
```

Перед настройкой Wi-Fi сети нужно создать Security Profiles – профили безопасности, которые содержат информацию о возможных способах шифрования, пароле и др.:

```
/interface wireless security-profiles set [find default=yes]\ supplicant-identity=MikroTik add authentication-types=wpa2-psk\
eap-methods="" management-protection=allowed \
mode=dynamic-keys name=local-profile supplicant-identity="" \
wpa2-pre-shared-key=asoi1_1iosa
/interface wireless security-profiles set [find default=yes] supplicant-identity=MikroTik
add authentication-types=wpa2-psk eap-methods="" management-protection=allowed \
mode=dynamic-keys name=Guest-profile1 supplicant-identity="" \
wpa2-pre-shared-key=asoi1_1iosa
```

Далее настраиваются беспроводные интерфейсы для внутренней и гостевой сети с диапазонами 2Ghz и 5Ghz:

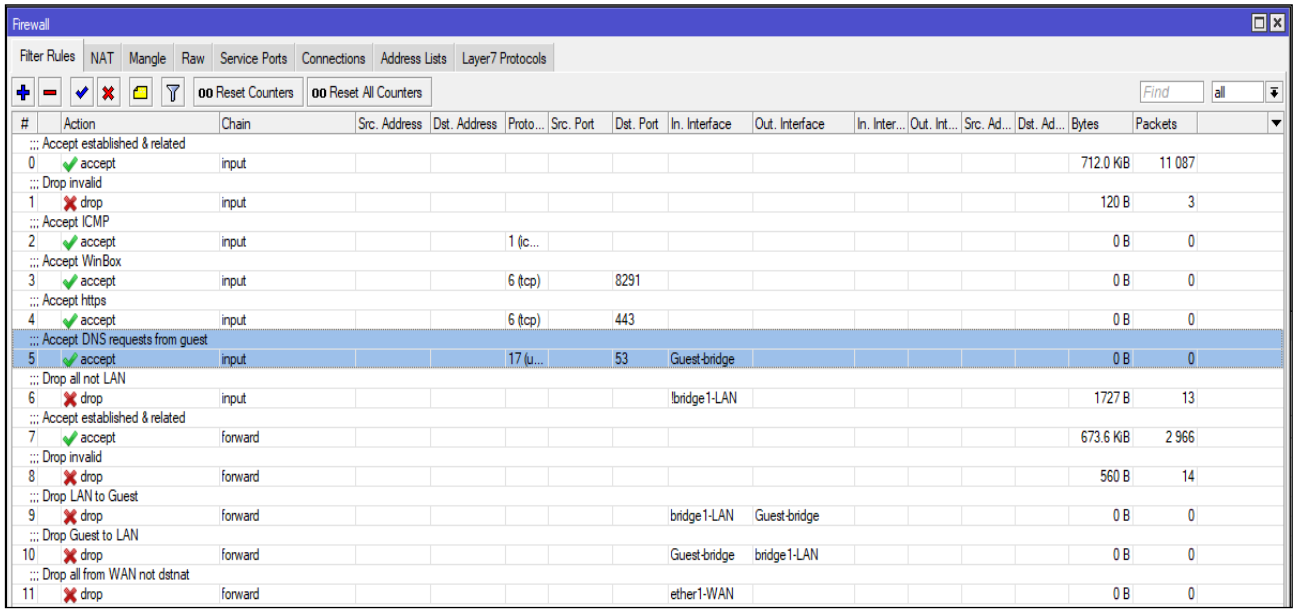
```
/interface wireless
set [find default-name=wlan1] band=2ghz-b/g/n country=belarus disabled=no \
hide-ssid=yes mode=ap-bridge name=wlan1-2Ghz ssid=WiFi-2Ghz\
wireless-protocol=802.11 wps-mode=disabled
add default-forwarding=no disabled=no keepalive-frames=disabled mac-address=\
XX:XX:XX:XX:XX:XX master-interface=wlan1-2Ghz multicast-buffering=disabled \
name=wlan-Guest-2Ghz ssid=Guest-2Ghz wds-cost-range=0 \
wds-default-cost=0 wps-mode=disabled
/interface wireless
set [find default-name=wlan2] band=5ghz-a/n/ac country=belarus disabled=no \
hide-ssid=yes mode=ap-bridge name=wlan2-5Ghz security-profile=local-profile \
ssid=WiFi-5Ghz wireless-protocol=802.11 wps-mode=disabled
add default-forwarding=no disabled=no keepalive-frames=disabled mac-address=\
XX:XX:XX:XX:XX:XX master-interface=wlan2-5Ghz multicast-buffering=disabled \
name=wlan-Guest-5Ghz ssid=Guest-5Ghz wds-cost-range=0 \
wds-default-cost=0 wps-mode=disabled
```

Потом интерфейсы добавляются в локальный и гостевой Bridge:

```
add bridge=bridge-LAN interface=wlan1-2Ghz
add bridge=bridge-LAN interface=wlan2-5Ghz
add bridge=Guest-bridge interface=wlan-Guest-2Ghz
add bridge=Guest-bridge interface=wlan-Guest-5Ghz
```

MikroTik RouterOS упрощает создание и развертывание сложных политик безопасности. Фактически можно легко создавать простой фильтр для трансляции адресов даже не задумываясь о том, как пакет обрабатывается маршрутизатором. Но если нужно развернуть более сложную политику безопасности необходимо знать некоторые детали процесса.

Для цепочки Forward настроить ACL в нормально закрытый режим доступа из всех сетей, кроме локальной. Для локальной сети оставить нормально открытый режим работы. Сделать исключения для правил проброса портов. При настройке ACL в правильном порядке расположить правила ACE (Рис. 1), что бы они не мешали работе друг друга (при неправильном расположении трафик может не дойти до нужного правила, будучи отброшенным другим).



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interface	Out. Interface	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
	;;; Accept established & related														
0	accept	input												712.0 KiB	11 087
	;;; Drop invalid														
1	drop	input												120 B	3
	;;; Accept ICMP														
2	accept	input			1 (ic...									0 B	0
	;;; Accept WinBox														
3	accept	input			6 (tcp)		8291							0 B	0
	;;; Accept https														
4	accept	input			6 (tcp)		443							0 B	0
	;;; Accept DNS requests from guest														
5	accept	input			17 (u...		53	Guest-bridge						0 B	0
	;;; Drop all not LAN														
6	drop	input						!bridge1-LAN						1727 B	13
	;;; Accept established & related														
7	accept	forward												673.6 KiB	2 966
	;;; Drop invalid														
8	drop	forward												560 B	14
	;;; Drop LAN to Guest														
9	drop	forward						bridge1-LAN	Guest-bridge					0 B	0
	;;; Drop Guest to LAN														
10	drop	forward						Guest-bridge	bridge1-LAN					0 B	0
	;;; Drop all from WAN not dstnat														
11	drop	forward						ether1-WAN						0 B	0

Рис. 1. Порядок правил в конфигурации

Порядок размещения правил для цепочки input:

- Разрешаем все established (установленные) и related (связанные) подключения;
- Запрещаем invalid (не идентифицированное);
- Разрешаем ICMP;
- Разрешаем WinBox;

- Разрешаем DNS запросы для гостевой сети;

- Запрещаем все, что не из локальной сети.

```
/ip firewall filter
add action=accept chain=input comment="Accept established&related"\
connection-state=established,related
add action=drop chain=input comment="Drop invalid" connection-
state=invalid
add action=accept chain=input comment="Accept ICMP" protocol=icmp
add action=accept chain=input comment="Accept WinBox" dst-port=8291
protocol=tcp
add action=accept chain=input comment="Accept https" dst-port=443
protocol=tcp
add action=accept chain=input comment="Accept DNS requests from
guest"
dst-port=53 in-interface=Guest-bridge protocol=udp
add action=drop chain=input comment="Drop all not LAN" in-
interface=\
```

Порядок размещения правил для цепочки forward:

- Разрешаем все established (установленные) и related (связанные) подключения;

- Запрещаем invalid (не идентифицированное);

- Запрещаем трафик из гостевой сети в локальную и наоборот;

- Запрещаем весь трафик из вне (интернета), кроме dstnat.

```
/ip firewall filter
add action=accept chain=forward comment="Accept established & relat-
ed" \connection-state=established,related
add action=drop chain=forward comment="Drop invalid" connection-
state=invalid
add action=drop chain=forward comment="Drop LAN to Guest" in-
interface=
bridge1-LAN out-interface=Guest-bridge
add action=drop chain=forward comment="Drop Guest to LAN" in-
interface=
Guest-bridge out-interface=bridge1-LAN
add action=drop chain=forward comment="Drop all fromWAN not dstnat"\
connection-nat-state=!dstnat in-interface=ether1-WAN
```

3. Заключение

Задача защиты трафика при переходе между кабельным и беспроводным участками сети решена на основе настроек операционной системы RouterOS маршрутизаторов MikroTik созданием гостевой сети доступа к внутренним ре-

сурсам локальной сети и назначением базовых сетевых параметров, включая парольный доступ и фильтрацию трафика.

Исследование выполнено в рамках НИР «Диагностика и многофакторное обследование безопасности беспроводных сетей WiFi (стандарт IEEE 802.11) предприятий и организаций» подпрограммы 5.1 «Цифровые технологии и космическая информатика» государственной программы научных исследований «Цифровые и космические технологии, безопасность человека, общества и государства» РБ.

ЛИТЕРАТУРА

1. *Демиденко О.М., Кулинченко В.Н., Бычков П.В. Контроль и диагностика внутрипериметральных каналов независимых (смежных) беспроводных сегментов сети / В.Н.Кулинченко, О.М.Демиденко, П.В.Бычков // Известия Гомельского государственного университета имени Ф. Скорины, № 6 (129), 2021. – С. 85-89.*

2. *Khludnev A.M., Kovtunenko V.A.* Analysis of cracks in solids. Southampton. Boston: WIT Press, 2000. 120 p.

Статья представлена к публикации д.т.н., профессором В.Н. Задорожным

Воруев Андрей Валерьевич, к.т.н., доцент, зав. кафедрой, varuyeu@gmail.com

Кулинченко Владимир Николаевич, kulinchenko@gsu.by

Кузеев Максим Владимирович, kuzeev2001@mai.ru