USING MIKROTIK RB-951 ROUTERS AS A MEANS OF PROTECTING THE INFORMATION INFRASTRUCTURE OF SMALL ORGANIZATIONS

Shamsutdinov R.R. (Russian Federation) Email: Shamsutdinov337@scientifictext.ru

Shamsutdinov Rinat Rustemovich – Master's Degree Students,
DEPARTMENT OF COMPUTER ENGINEERING AND INFORMATION PROTECTION,
UFA STATE AVIATION TECHNICAL UNIVERSITY, UFA

Abstract: *the article analyzes the possibility of using Mikrotik RB-951 routers as a means of protection from network attacks: as a firewall and virtual private network client for small organizations whose budget can't purchase expensive network protection equipment. The article also analyzes the router firewall protection possibilities, possibilities of tunneling the network traffic. The author proposes complementary settings for this router to improve the local area network security level and increase the security level of this router.*
Keywords: *router, firewall, VPN, network attacks.*

ИСПОЛЬЗОВАНИЕ МАРШРУТИЗАТОРОВ MIKROTIK RB-951 В КАЧЕСТВЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ МАЛЫХ ОРГАНИЗАЦИЙ

Шамсутдинов Р.Р. (Российская Федерация)

Шамсутдинов Ринат Рустемович – магистрант,
кафедра вычислительной техники и защиты информации,
Уфимский государственный авиационный технический университет, г. Уфа

Аннотация: *в статье рассматривается возможность использования маршрутизаторов Mikrotik RB-951 в качестве средств защиты от сетевых атак: межсетевых экранов, клиентов виртуальных частных сетей для малых организаций, бюджет которых не позволяет закупить дорогостоящее оборудование сетевой защиты. В статье также рассмотрены возможности файервольной защиты данного маршрутизатора, туннелирования сетевого трафика, предложены дополнительные настройки данного роутера по повышению уровня защищенности локальной вычислительной сети, защищенности самого маршрутизатора.*
Ключевые слова: *роутер, межсетевой экран, VPN, сетевые атаки.*

В настоящее время защита от сетевых атак для любых организаций, осуществляющих свою деятельность с применением информационных технологий, является одной из ключевых потребностей, обеспечение которых необходимо для существования. К примеру, в 2017 г. «Лаборатория Касперского» зафиксировала около 45 тыс. атак программой-шифровальщиком WannaCry в 74 странах по всему миру» [1]. Распространение червя осуществлялось через уязвимости протокола SMB и нанесло урон даже таким крупным организациям, как «Роснефть», очевидно, что потенциал защиты организаций, не имеющих возможности закупить современные средства защиты инфраструктуры, ничтожен.

Рассматриваемый маршрутизатор может быть сконфигурирован посредством ssh-подключения, через web-интерфейс или через специальное ПО «Winbox». Наиболее удобным является последнее, поскольку позволяет более гибко настраивать роутер, нежели web-интерфейс, а синтаксис команд в ssh часто отличается в зависимости от поколения «прошивки».

В работе не рассматривается настройка оборудования для маршрутизации в сети, предполагается, что роутер уже сконфигурирован для данной цели. В меню «IP» находится раздел конфигурации правил межсетевого экранирования «Firewall». Добавление правил доступа представлено на рисунке 1.

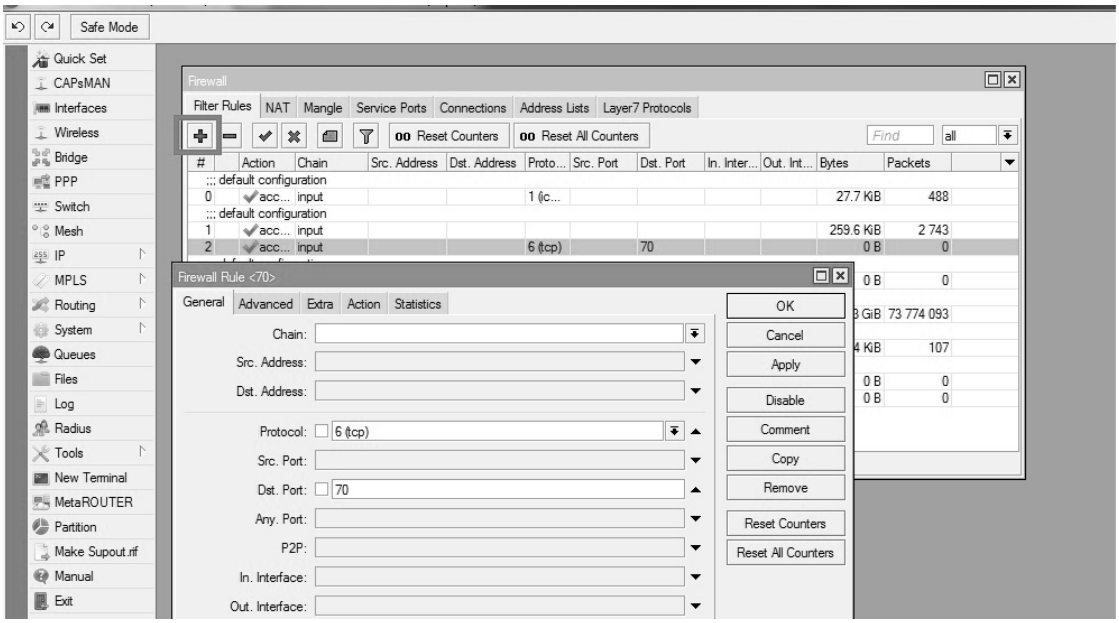

Рис. 1. Настройки межсетевого экранирования Mikrotik RB-951

Как видно из рисунка 1, в правилах доступа можно задать IP-адреса и порты отправителя и получателя пакетов, входящий и исходящий интерфейсы к которым применено правило. Таким образом, данный роутер может выполнять функцию межсетевого экрана L4.

Для организаций, не имеющих средств межсетевого экранирования, рекомендуется установка данного роутера между сетью Интернет и ЛВС. Причем необходимо как минимум запретить входящие внешние подключения по портам сервисов, не используемых при работе с Интернет.

В лучшем случае же указать конкретные IP-адреса хостов, между которыми разрешен доступ, конкретные протоколы, все остальное необходимо заблокировать. Также рекомендуется разделить сеть на сегменты, критичные ресурсы выделить в отдельный сегмент и отделить его дополнительным межсетевым экраном с минимально необходимыми правилами доступа.

В дополнение данный роутер может быть сконфигурирован для реализации VPN-соединения через Интернет между территориально распределёнными сегментами, что позволяет обмениваться информацией между ними по криптографически защищенному каналу связи.

Дополнительно рекомендуется отключить все неиспользуемое в «system» → «packages»; в «system» → «users» задать логины, пароли и IP-адреса администраторов роутера; в «IP» → «Services» отключить все, кроме Winbox и ssh; в «IP» → «SNMP» отключить SNMP; отключить неиспользуемое в «IP» → «Firewall» → «Service ports».

Таким образом, маршрутизаторы Mikrotik RB-951 могут использоваться в качестве экранирующих маршрутизаторов и VPN-клиентов небольшими организациями, бюджет которых не позволяет закупить дорогостоящие современные средства защиты от сетевых атак.

Список литературы / References

1. Атаки вируса-вымогателя WannaCry зафиксированы в 74 странах. [Электронный ресурс]: Интерфакс. Режим доступа: http://www.interfax.ru/world/562139/ (дата обращения: 03.02.2018).