

Setting up Internet Access Server on Basis of MikroTik RouterOS and ISP Billing System NetUP UTM5

Introduction

This article is concerned with setting up an Internet access server on basis of MikroTik RouterOS. Access server that blocks/unblocks Internet access is also capable to limit the bandwidth. Internet access is controlled by the firewall by adding/removing rules to the forward chain. Bandwidth is limited by Simple Queues. For managing an access server using billing system UTM5 it is used `utm5_rfw` daemon, which calls auxiliary scripts that automate connections to the access server via ssh or telnet and run commands at the server for operating the firewall or simple queues.

Hereinafter we suppose that the access server connects to the local network 192.168.1.0/24 via the Internet (its IP address in the local network is 192.168.1.1, and subnet mask is 255.255.255.0 or 24 in CIDR notation). An external IP address of the access server is 172.16.1.1 (mask 255.255.255.0). By default the gateway IP is 172.16.1.254. The billing system UTM5 is installed on the server, the IP address is 192.168.1.10. In order to allow users of the network connecting to the Internet IP addresses are transmitted to the external IP address of the access server (SNAT). As in the current configuration the access server also acts as a router, we shall use these two terms as synonyms.

Configuring the access server

Setting up Mikrotik RouterOS is not at all that complicated and is mentioned at the following web site <http://www.mikrotik.com/docs/ros/2.9/guide/basic>

Here we shall review the process of installation from a CD.

Download the CD image from the web site www.mikrotik.com and burn a CD. Place it in your CD-ROM drive and boot up the computer. Now you need to select necessary packages. For an Internet access server it's enough to select *system* and *security*.

```

Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'M'. Press 'i' to install locally or 'r' to
install remote router or 'q' to cancel and reboot.

[ X ] system                [ ] lcd                    [ ] synchronous
[ ] ppp                    [ ] ntp                    [ ] telephony
[ ] dhcp                   [ ] radiolan               [ ] ups
[ ] advanced-tools        [ ] routerboard           [ ] web-proxy
[ ] arlan                  [ ] routing                [ ] webproxy-test
[ ] gps                    [ ] routing-test          [ ] wireless
[ ] hotspot                [ ] rstp-bridge-test      [ ] wireless-legacy
[ ] isdn                   [ X ] security

security (depends on system):
Provides support for IPSEC, SSH and secure connectivity with WinBox.
```

Press 'i' and follow the configurator.

Note

Security package is necessary only to access the router via ssh. If you prefer telnet you need not to install the security package. If you forget to set it up you may find out how to install it below in this article.

After installing the Mikrotik OS you should configure the computer in order to make an access server: set an administrator password, set IP addresses for networking interfaces, set a default gateway, set DNS addresses, enable SNAT and set default firewall rules.

Warning

If you wish your computer to work for more than 24 hours you should register your OS version. For registration go to <http://www.mikrotik.com/docs/ros/2.9/system/license>

Password

After installing Mikrotik OS a user 'admin' is created without a password by default. For setting the password use the command `/password`.

Setting IP addresses and default gateway

In Mikrotik OS networking interfaces can be configured using one of two methods:

1. Command `/setup` and follow the instructions on the screen
2. Menu command `/ip`.

Let's examine the second method.

In order to set the IP addresses for the interfaces run the following commands:

```
> /ip address add address=172.16.1.1/24 interface=ether1 comment="INTERNET"  
> /ip address add address=192.168.1.1/24 interface=ether2 comment="LAN"
```

The following command allows to check IP address settings:

```
> /ip address print  
Flags: X - disabled, I - invalid, D - dynamic  
# ADDRESS NETWORK BROADCAST INTERFACE  
0 ;;; INTERNET  
172.16.1.1/24 172.16.1.0 172.16.1.255 ether1  
1 ;;; LAN  
192.168.1.1/24 192.168.1.0 192.168.1.255 ether2
```

Now set the default gateway:

```
> /ip route add gateway=172.16.1.254
```

For viewing the routing information (especially default gateway) use the command below:

```
> /ip route print  
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip,  
b - bgp, o - ospf  
# DST-ADDRESS PREFSRC G GATEWAY DISTANCE INTERFACE  
0 ADC 172.16.1.0/24 172.16.1.1 ether1  
1 ADC 192.168.1.0/24 192.168.1.255 ether2  
2 A S 0.0.0.0/0 r 172.16.1.254 ether1
```

For finishing setting up the network define DNS addresses:

```
> /ip dns set primary-dns=172.16.1.254  
> /ip dns set secondary-dns=172.16.1.253
```

To check the defined DNS use the command:

```
> /ip dns print
    primary-dns: 172.16.1.254
    secondary-dns: 172.16.1.253
allow-remote-requests: no
    cache-size: 2048KiB
    cache-max-ttl: 1w
    cache-used: 16KiB
```

Check if the settings are correct by the command /ping

SNAT and firewall

In order to allow the users using the Internet their local IP addresses at the external interface of the router should be translated to the external IP address:

```
> /ip firewall nat add chain=srcnat src-address=192.168.1.0/24 \
\... out-interface=ether1 action=src-nat to-addresses=172.16.1.1
```

In order to check the settings of IP address translation, use the following command:

```
> ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0 chain=srcnat out-interface=ether1 src-address=192.168.1.0/24
  action=src-nat to-addresses=172.16.1.1 to-ports=0-65535
```

After setting up translation of IP addresses every computer of the local network is allowed to access the Internet. To manage access of users add the following rules to the forward chain of the firewall:

```
> /ip firewall filter add chain=forward action=jump jump-target=utm5_forward
> /ip firewall filter add chain=forward action=drop
```

The first rule redirects packages from the forward chain to chain utm5_forward. In this article we add to this chain only the rules that permit Internet access. The second rule rejects all packets which are explicitly not allowed to pass. After the second rule has been added Internet access from the local network shall be denied.

Now we have finished configuring the router. The access server is managed by the utm5_rfw daemon using scripts from the package utm5_mikrotic according to the commands of the billing system core utm5_core.

Setting up ssh server

Note: If you already have the *security* package installed skip this section.

SSH server is located in the *security* package. In order to view all installed packages run `/system package print`. If *security* package is absent from the list of installed packages it should be installed.

Before installation it is necessary to check the free space `/system resource print`. To install the package just download from the web site www.mikrotik.com the following file: **all_packages_2.9.xx.zip**, unpack it and load **security-2.9.xx.npk** to the router via ftp protocol in the binary mode. Then reboot the access server `/system reboot` - the package will be installed while the server is preparing for restart. You can watch the installation process from the monitor connected to the access server. After rebooting, the installed packages are reflected in the list `/system packages print`. Please, draw attention that the *security* package must not be disabled.

```
> /system package print
Flags: X - disabled
#   NAME                               VERSION
SCHEDULED
0   security                            2.9.13
1   system                               2.9.13
```

Also make sure that ssh service is not disabled. For this use the command `/ip service print`.

Also check the ability of connection to the access server using the SSH client.

Configuring utm5_rfw daemon

Note

Hereinafter it is supposed that you have already configured traffic classes, services and tariffs. Also it is proposed that the system user rfw has been already created (under this name utm5_rfw connects to the system core). If you have not yet performed this, use the UTM5 user's guide.

Note

In this article *utm5_rfw* daemon is configured under *Gentoo Linux OS*. In any other OS configuring can be accomplished in a similar way.

utm5_rfw daemon may be set up at any server which is able to connect to *utm5_core* via *tcp* protocol. Here it is supposed that *utm5_rfw* and *utm5_core* are located at the same physical server.

Format and options of the *utm5_rfw* configuration file are described in the UTM5 user's guide. In order to configure *utm5_rfw* daemon create the following configuration file `/netup/utm5/rfw.cfg`:

```
firewall_path=/usr/bin/expect
dont_fork=yes
rfw_name=Mikrotik
core_host=127.0.0.1
core_port=11758
rfw_login=rfw
rfw_password=rfwpass
```

Due to the message sent from the system core, *utm5_rfw* calls the command, defined in the *firewall_path*, transmitting information, set in the UTM5 Administrator Interface, as an argument. Here we transmit the name of the script from the package *utm5_mikrotik* with additional parameters. Let's review the package and all scripts it contains in details.

utm5_mikrotik scripts

In order to manage the access server at Mikrotik OS remotely we need to use scripts from the package `utm5_mikrotik-x.x.tar.gz`. Download this package from the official NetUP web site (<http://www.netup.biz>) and install it.

```
$ ./configure
$ make
# make install
```

As a result the following files are installed:

```
/etc/utm5/mikrotik.conf
/netup/utm5/bin/mik_functions
/netup/utm5/bin/mik_add
/netup/utm5/bin/mik_rm
```

mik_add and *mik_rm* are scripts that automate connection to the access server and execute all necessary commands on this server (e.g., add/remove firewall rules or simple queues). The *mik_functions* file contains common (for *mik_add* and *mik_rm*) operations. *mikrotik.conf* is a configuration file.

Set in the configuration file address of the access server, login and a password.

```
set host "192.168.1.1"
set user "admin"
set password "password"
```

Despite in this example it is not necessary, you may if you wish select *ssh* or *telnet* (relient) as a protocol for connection to the access server, prompt appearance and name of the chain the rules are added to on the remote server.

Note

For automatic executing of these scripts on the server it is used a tool *expect* (<http://expect.nist.gov/>) which uses *tcl* programming language. Key word “*set*” is a command in the *tcl* programming language; don’t remove it from the configuration file.

Let’s examine scripts *mik_add* and *mik_rm* in details. *mik_add* is a script adding rules to the firewall and creating queues; *mik_rm* removes them. If you execute any of these scripts with no parameters then you will see the following:

```
usage: ./mik_add IP=<ip> [MASK=<mask>] [MAC=<mac>]
[BPSIN=<bytes/sec>] [BPSOUT=<bytes/sec>] [GBPSIN=<bytes/sec>] [GBPSOUT=<bytes/sec>]
```

Where:

```
IP=<ip>           - User IP address.
MASK=<mask>       - User MASK. Default is 255.255.255.255 or in CIDR notation 32.
MAC=<mac>        - User MAC address. Default is undefined.
BPSIN=<bytes/sec> - Internet->user data rate (max-limit option in simple queue).
BPSOUT=<bytes/sec> - User->internet data rate (max-limit option in simple queue).
GBPSIN=<bytes/sec> - Internet->user guaranteed data rate (limit-at option in simple
queue).
GBPSOUT=<bytes/sec> - User->internet guaranteed data rate (limit-at option in simple
queue).
```

In order to let the user on IP address 192.168.1.2 access to the Internet run:

```
/netup/utm5/bin/mik_add IP=192.168.1.2
```

In order to deny access run:

```
/netup/utm5/bin/mik_rm IP=192.168.1.2
```

You can also set a mask or MAC address. Between MAC and mask there stands “or” because the mask is by default 32. If you set a different mask then the MAC address loses its meaning as the group of computers has different MAC addresses. However nothing forbids you from doing this. Moreover, you can set the maximum speed toward (BPSIN) and outward (BPSOUT) for the user, and also guaranteed user traffic speed GBPSIN, GBPSOUT. For example:

```
/netup/utm5/bin/mik_add IP=192.168.1.2 MAC=00:0c:29:0e:26:65 BPSIN=128
```

Note

To know more about the difference between guaranteed speed and maximum available speed turn to documentation at <http://www.mikrotik.com/docs/ros/2.9/root/queue>

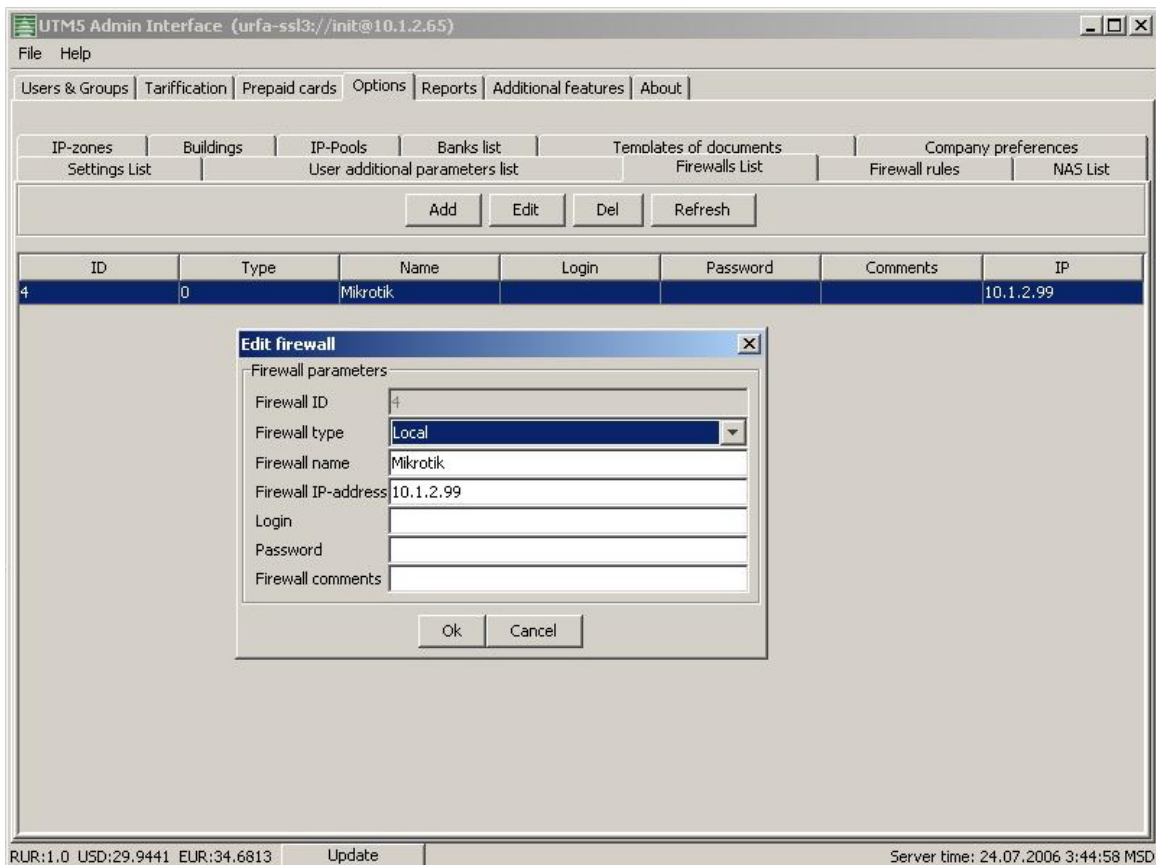
Warning

By default, if you set only BPSIN then BPSOUT will be set to the same value (and vice versa). If you wish to limit traffic for only one direction set the parameter of another direction equal to 0.

Check efficiency of the scripts. Launch them with the same user privileges that *utm5_rfw* daemon has. When you are sure that everything works correctly add the access server to the list of firewalls and define the command which will permit/deny access to the Internet in the administrator interface.

UTM5 billing system settings

Firstly connect to the core of ISP billing system UTM5 via Administrator Interface and add the daemon to the list of firewalls:



Check that the IP address is set to the same value of what parameter *rfw_name* has in the configuration file `/netup/utm5/rfw5.cfg`. Launch the daemon *utm5_rfw*:

```
# /etc/init.d/utm5_rfw start
```

After that add the firewall rules:

The screenshot shows a dialog box titled "Edit rule" with a close button (X) in the top right corner. The dialog is divided into a "Rule parameters" section and a bottom section with "Ok" and "Cancel" buttons. The "Rule parameters" section contains the following fields:

Rule ID	4
All users affected	<input checked="" type="checkbox"/>
All match	<input type="checkbox"/>
Execute when adding user	<input type="checkbox"/>
Execute when editing user	<input type="checkbox"/>
Execute when deleting user	<input type="checkbox"/>
User id	0
Group id	0
Tariff id	0
"On" rule	/netup/utm5/bin/mik_add IP=UIP MASK=UBITS
"Off" rule	/netup/utm5/bin/mik_rm IP=UIP MASK=UBITS
Router ID	4

For example, to create unlimited tariffs (flat rates) it's enough to create different tariffs containing the IP traffic service with different periodical cost component, and for each tariff create its own rules for enabling/disabling the Internet with different bandwidth.