Manual:IP/Hotspot

From MikroTik Wiki
< Manual:IP

Contents

- 1 HotSpot
  - 1.1 Sub Categories
- 2 HotSpot Setup
- 3 ip hotspot
- 4 ip hotspot active
- 5 ip hotspot host
- 6 IP Bindings
- 7 Cookies

HotSpot

The MikroTik HotSpot Gateway provides authentication for clients before access to public networks .

HotSpot Gateway features:

- different authentication methods of clients using local client database on the router, or remote RADIUS server;
- users accounting in local database on the router, or on remote RADIUS server;
- walled-garden system, access to some web pages without authorization;
- login page modification, where you can put information about the company;
- automatic and transparent change any IP address of a client to a valid address;

Hotspot can work reliably only when IPv4 is used. Hotspot relies on Firewall NAT rules which currently are not supported for IPv6.

Sub Categories

List of reference sub-pages	Case studies	List of examples
- IP/Hotspot - Profile - User - Walled Garden	- Hotspot Introduction	- Hotspot with PCC - Hotspot HTTPS example - Hotspot manual login - Trial user limits - Customizing Hotspot

HotSpot Setup

The simplest way to setup HotSpot server on a router is by **`/ip hotspot setup`** command. Router will ask to enter parameters required to successfully set up HotSpot. When finished, default configuration will be added for HotSpot server.

```
[admin@MikroTik] /ip hotspot> setup
Select interface to run HotSpot on

hotspot interface: ether3
Set HotSpot address for interface

local address of network: 10.5.50.1/24
masquerade network: yes
Set pool for HotSpot addresses

address pool of network: 10.5.50.2-10.5.50.254
Select hotspot SSL certificate

select certificate: none
Select SMTP server

ip address of smtp server: 0.0.0.0
Setup DNS configuration

dns servers: 10.1.101.1
DNS name of local hotspot server

dns name: myhotspot
Create local hotspot user

name of local hotspot user: admin
password for the user:
[admin@MikroTik] /ip hotspot>
```

What was created:

```
[admin@MikroTik] /ip hotspot> print
Flags: X - disabled, I - invalid, S - HTTPS
 #   NAME        INTERFACE       ADDRESS-POOL       PROFILE       IDLE-TIMEOUT
 0   hotspot1    ether3          hs-pool-3          hsprof1       5m
[admin@MikroTik] /ip hotspot>
[admin@MikroTik] /ip pool> print
 # NAME                                        RANGES
 0 hs-pool-3                                   10.5.50.2-10.5.50.254
[admin@MikroTik] /ip pool> /ip dhcp-server
[admin@MikroTik] /ip dhcp-server> print
Flags: X - disabled, I - invalid
 #   NAME      INTERFACE    RELAY           ADDRESS-POOL    LEASE-TIME ADD-ARP
 0   dhcp1     ether3                       hs-pool-3       1h
[admin@MikroTik] /ip dhcp-server> /ip firewall nat
[admin@MikroTik] /ip firewall nat> print
Flags: X - disabled, I - invalid, D - dynamic
 0 X ;;; place hotspot rules here
     chain=unused-hs-chain action=passthrough

 1   ;;; masquerade hotspot network
     chain=srcnat action=masquerade src-address=10.5.50.0/24
[admin@MikroTik] /ip firewall nat>
```

Parameters asked during setup process

Parameter	Description
`hotspot interface` (*string*; Default: **allow**)	Interface name on which to run HotSpot. To run HotSpot on a bridge interface, make sure public interfaces are not included to the bridge ports.
`local address of network` (*IP*; Default: **10.5.50.1/24**)	HotSpot gateway address
`masquerade network` (*yes | no*; Default: **yes**)	Whether to masquerade HotSpot network, when **yes** rule is added to */ip firewall nat* with *action=masquerade*
`address pool of network` (*string*; Default: **yes**)	Address pool for HotSpot network, which is used to change user IP address to a valid address. Useful if providing network access to mobile clients that are not willing to change their networking settings.
`select certificate` (*none | import-other-certificate*; Default:)	Choose SSL certificate, when HTTPS authorization method is required.
`ip address of smtp server` (*IP*; Default: **0.0.0.0**)	IP address of the SMTP server, where to redirect HotSpot's network SMTP requests (25 TCP port)
`dns servers` (*IP*; Default: **0.0.0.0**)	DNS server addresses used for HotSpot clients, configuration taken from */ip dns* menu of the HotSpot gateway
`dns name` (*string*; Default: "")	domain name of the HotSpot server, full quality domain name is required, for example www.example.com
`name of local hotspot user`	username of one automatically created HotSpot user,

(*string*; Default: "**admin**")	added to */ip hotspot user*
`password for the user'` (*string*; Default:)	Password for automatically created HotSpot user

ip hotspot

Menu is designed to manage HotSpot servers of the router. It is possible to run HotSpot on Ethernet, wireless, VLAN and bridge interfaces. One HotSpot server is allowed per interface. When HotSpot is configured on bridge interface, set HotSpot interface as *bridge* interface not as *bridge port*, do not add public interfaces to bridge ports. You can add HotSpot servers manually to */ip hotspot* menu, but it is advised to run */ip hotspot setup*, that adds all necessary settings.

- **name** (text) : HotSpot server's name or identifier
- **address-pool** (name **/** none; default: *none*) : address space used to change HotSpot client *any* IP address to a valid address. Useful for providing public network access to mobile clients that are not willing to change their networking settings
- **idle-timeout** (time **/** none; default: *5m*) : period of inactivity for unauthorized clients. When there is no traffic from this client (literally client computer should be switched off), once the timeout is reached, user is dropped from the HotSpot host list, its used address becomes available
- **keepalive-timeout** (time **/** none; default: *none*) : Value of how long host can stay out of reach to be removed from the HotSpot.
- **login-timeout** (time **/** none; default: *none*) : period of time after which if host hasn't been authorized it self with system the host entry gets deleted from host table. Loop repeats until host logs in the system. Enable if there are situations where host cannot login after being to long in host table unauthorized.
- **interface** (name of interface) : interface to run HotSpot on
- **addresses-per-mac** (integer **/** unlimited; default: 2) : number of IP addresses allowed to be bind with the MAC address, when multiple HotSpot clients connected with one MAC-address
- **profile** (name; default: *default*) - HotSpot server default HotSpot profile, which is located in */ip hotspot profile*

keepalive-timeout (read-only; time) : the exact value of the keepalive-timeout, that is applied for user. Value shows how long host can stay out of reach to be removed from the HotSpot

ip hotspot active

HotSpot active menu shows all clients authenticated in HotSpot, menu is informational it is not possible to change anything here.

- **server** (read-only; name) : HotSpot server name client is logged in
- **user** (read-only; name) : name of the HotSpot user
- **domain** (read-only; text) : domain of the user (if split from username), parameter is used only with RADIUS authentication
- **address** (read-only; IP address) : IP address of the HotSpot user
- **mac-address** (read-only; MAC-address) : MAC-address of the HotSpot user
- **login-by** (read-only; multiple choice: cookie **/** http-chap **/** http-pap **/** https **/** mac **/** mac-cookie **/** trial) : authentication method used by HotSpot client
- **uptime** (read-only; time) : current session time of the user, it is showing how long user has been logged in
- **idle-time** (read-only; time) : the amount of time user has been idle
- **session-time-left** (read-only; time) : the exact value of session-time, that is applied for user. Value shows how long user is allowed to be online to be logged of automatically by **uptime** reached
- **idle-timeout** (read-only; time) : the exact value of the user's idle-timeout
- **keepalive-timeout** (read-only; time) : the exact value of the keepalive-timeout, that is applied for user. Value shows how long host can stay out of reach to be removed from the HotSpot
- **limit-bytes-in** (read-only; integer) : value shows how many bytes received from the client, option is active when the appropriate parameter is configured for HotSpot user
- **limit-bytes-out** (read-only; integer) : value shows how many bytes send to the client, option is active when the appropriate parameter is configured for HotSpot user
- **limit-bytes-total** (read-only; integer) : value shows how many bytes total were send/received from client, option is active when the

appropriate parameter is configured for HotSpot user

ip hotspot host

Host table lists all computers connected to the HotSpot server. Host table is informational and it is not possible to change any value there

- **mac-address** (read-only; MAC-address) : HotSpot user MAC-address
- **address** (read-only; IP address) : HotSpot client original IP address
- **to-address** (read-only; IP address) : New client address assigned by HotSpot, it might be the same as original **address**
- **server** (read-only; name) : HotSpot server name client is connected to
- **bridge-port** (read-only; name) : /interface bridge port client connected to, value is unknown when HotSpot is not configured on the bridge
- **uptime** (read-only; time) : value shows how long user is online (connected to the HotSpot)
- **idle-time** (read-only; time) : time user has been idle
- **idle-timeout** (read-only; time) : value of the client idle-timeout (unauthorized client)
- **keeaplive-timeout** (read-only; time) : keepalive-timeout value of the unauthorized client
- **bytes-in** (read-only; integer) : amount of bytes received from unauthorized client
- **packet-in** (read-only; integer) : amount of packets received from unauthorized client
- **bytes-out** (read-only; integer) : amount of bytes send to unauthorized client
- **packet-out** (read-only; integer) : amount of packets send to unauthorized client

IP Bindings

Sub-menu: `/ip hotspot ip-binding`

IP-Binding HotSpot menu allows to setup static One-to-One NAT translations, allows to bypass specific HotSpot clients without any authentication, and also allows to block specific hosts and subnets from HotSpot network

Property	Description
`address` (*IP Range*; Default: "")	The original IP address of the client
`mac-address` (*MAC*; Default: "")	MAC address of the client
`server` (*string | all*; Default: "**all**")	Name of the HotSpot server. ▪ **all** - will be applied to all hotspot servers
`to-address` (*IP*; Default: "")	New IP address of the client, translation occurs on the router (client does not know anything about the translation)
`type` (*blocked | bypassed | regular*; Default: "")	Type of the IP-binding action ▪ **regular** - performs One-to-One NAT according to the rule, translates **address** to **to-address** ▪ **bypassed** - performs the translation, but excludes client from login to the HotSpot ▪ **blocked** - translation is not performed and packets from host are dropped

Cookies

Sub-menu: `/ip hotspot cookie`

Menu contains all cookies sent to the HotSpot clients, which are authorized by cookie method, all the entries are read-only.

Property	Description
`domain` (*string*)	Domain name (if split from username)
`expires-in` (*time*)	How long the cookie is valid
`mac-address` (*MAC*)	Client's MAC-address
`user` (*string*)	HotSpot username

[Top | Back to Content **]**

Retrieved from "https://wiki.mikrotik.com/index.php?title=Manual:IP/Hotspot&oldid=29644"

Categories: Manual | Hotspot | AAA

- This page was last edited on 15 August 2017, at 09:16.