SSH (Secure Shell) Server and Client

Document revision 2.0 (Fri Mar 05 09:09:40 GMT 2004)
This document applies to V2.9

Table of Contents

Table of Contents
  Summary
  Specifications
  Related Documents
  Additional Documents
SSH Server
  Description
  Property Description
  Example
SSH Client
  Property Description
  Example

General Information

Summary

SSH Client authenticates server and encrypts traffic between the client and server. You can use SSH just the same way as telnet - you run the client, tell it where you want to connect to, give your username and password, and everything is the same after that. After that you won't be able to tell that you're using SSH. The SSH feature can be used with various SSH Telnet clients to securely connect to and administrate the router.

The MikroTik RouterOS supports:

- SSH 1.3, 1.5, and 2.0 protocol standards
- server functions for secure administration of the router
- telnet session termination with 40 bit RSA SSH encryption is supported
- secure ftp is supported
- preshared key authentication is not supported

The MikroTik RouterOS has been tested with the following SSH telnet terminals:

- PuTTY
- Secure CRT
- OpenSSH GNU/Linux client

Specifications
Packages required: security
License required: level 1
Home menu level: /system ssh
Standards and Technologies: SSH
Hardware usage: Not significant

Related Documents

- Package Management

Additional Documents

- http://www.freessh.org/

SSH Server

Home menu level: /ip service

Description

SSH Server is already up and running after MikroTik router installation. The default port of the service is 22. You can set a different port number.

Property Description

**name (name)** - service name

**port (integer: 1..65535)** - port the service listens to

**address (IP address | netmask; default: 0.0.0.0/0)** - IP address from which the service is accessible

Example

Let's change the default SSH port (22) to 65 on which the SSH server listens for requests:

```
[admin@MikroTik] ip service> set ssh port=65
[admin@MikroTik] ip service> print
Flags: X - disabled, I - invalid
#  NAME    PORT  ADDRESS          CERTIFICATE
 0  telnet  23     0.0.0.0/0
 1   ftp    21     0.0.0.0/0
 2    www   80     0.0.0.0/0
 3     ssh  65     0.0.0.0/0
 4  www-ssl 443    0.0.0.0/0
[admin@MikroTik] ip service>
```

SSH Client

Command name: /system ssh

Property Description

**port (integer; default: 22)** - which TCP port to use for SSH connection to a remote host
**user** *(text; default: admin)* - username for the SSH login

**Example**

```
[admin@MikroTik] > /system ssh 192.168.0.1 user=pakalns port=22
admin@192.168.0.1's password:
```

MikroTik RouterOS 2.9rc7 (c) 1999-2005  http://www.mikrotik.com/

Terminal unknown detected, using single line input mode
[admin@MikroTik] >