Address Lists

Document revision 2.7 (Mon May 02 10:18:10 GMT 2005)
This document applies to V2.9

Table of Contents

Table of Contents
  Summary
  Specifications
  Related Documents
Address Lists
  Description
  Property Description
  Example

General Information

Summary

Firewall address lists allow to create a list of IP addresses to be used for packet matching.

Specifications

Packages required: system
License required: level1
Home menu level: /ip firewall address-list
Standards and Technologies: IP
Hardware usage: Not significant

Related Documents

- Software Package Management
- NAT
- Filter
- Packet Flow
- Packet Flow

Address Lists

Description

Firewall address lists allow user to create lists of IP addresses grouped together. Firewall filter, mangle and NAT facilities can use address lists to match packets against them.
The address list records could be updated dynamically via the `action=add-src-to-address-list` or `action=add-dst-to-address-list` items found in NAT mangle and filter facilities.

**Property Description**

**list** (*name*) - specify the name of the address list to add IP address to

**address** (*IP address | netmask | IP address | IP address*) - specify the IP address or range to be added to the address list. Note that console converts entered address/netmask value to a valid network address, i.e.: 1.1.1.1/24 is converted to 1.1.0.0/24

**Example**

The following example creates an address list of people that are connecting to port 23 (telnet) on the router and drops all further traffic from them. Additionally, the address list will contain one static entry of `address=192.0.34.166/32` (www.example.com):

```
[admin@MikroTik] > /ip firewall address-list add list=drop_traffic address=192.0.34.166/32
[admin@MikroTik] > /ip firewall address-list print
Flags: X - disabled, D - dynamic
# LIST ADDRESS
0 drop_traffic 192.0.34.166
[admin@MikroTik] > /ip firewall mangle add chain=prerouting protocol=tcp dst-port=23 \... action=add-src-to-address-list address-list=drop_traffic
[admin@MikroTik] > /ip firewall filter add action=drop chain=input src-address-list=drop_traffic
[admin@MikroTik] > /ip firewall address-list print
Flags: X - disabled, D - dynamic
# LIST ADDRESS
0 drop_traffic 192.0.34.166
1 D drop_traffic 1.1.1.1
2 D drop_traffic 10.5.11.8
[admin@MikroTik] >
```

As seen in the output of the last `print` command, two new dynamic entries appeared in the address list. Hosts with these IP addresses tried to initialize a telnet session to the router.