Address-lists

Summary

```
/ip firewall address-list
```

Firewall address lists allow a user to create lists of IP addresses grouped together under a common name. Firewall filter, mangle, and NAT facilities can then use those address lists to match packets against them.

The address list records can also 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.

Firewall rules with action `add-src-to-address-list` or `add-dst-to-address-list` work in passthrough mode, which means that the matched packets will be passed to the next firewall rules.

Properties

Property	Description
address (*DNS Name | IP address/netmask | IP-IP*; Default:)	A single IP address or range of IPs to add to the address list or DNS name. You can input for example, '192.168.0.0-192.168.1.255' and it will auto modify the typed entry to 192.168.0.0/23 on saving.
dynamic (*yes,* no)	Allows creating data entry with dynamic form.
list (*string*; Default:)	Name for the address list of the added IP address.
timeout (*time*; Default:)	Time after address will be removed from the address list. If the timeout is not specified, the address will be stored in the address list permanently.
creation-time (*time*; Default:)	The time when the entry was created.

⚠ If the timeout parameter is not specified, then the address will be saved to the list permanently on the disk. If a timeout is specified, the address will be stored on the RAM and will be removed after a system's reboot.

Example

The following example creates a dynamic address list of people who are connecting to port 23 (telnet) on the router and drops all further traffic from them for 5 minutes. Additionally, the address list will also contain one static address list entry of 192.0.34.166/32 (www.example.com):

```
/ip firewall address-list add list=drop_traffic address=192.0.34.166/32
```

```
/ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST         ADDRESS
 0   drop_traffic 192.0.34.166
```

```
/ip firewall mangle add action=add-src-to-address-list address-list=drop_traffic address-list-timeout=5m
chain=prerouting dst-port=23 protocol=tcp
/ip firewall filter add action=drop chain=input src-address-list=drop_traffic
```

```
/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
```

As seen in the output of the last print command, two new dynamic entries appeared in the address list (marked with a status of 'D'). Hosts with these IP addresses tried to initialize a telnet session to the router and were then subsequently dropped by the filter rule.