Intelligent Firewall for complete data confidence

Easy to manage system

Fully optimizes your network usage

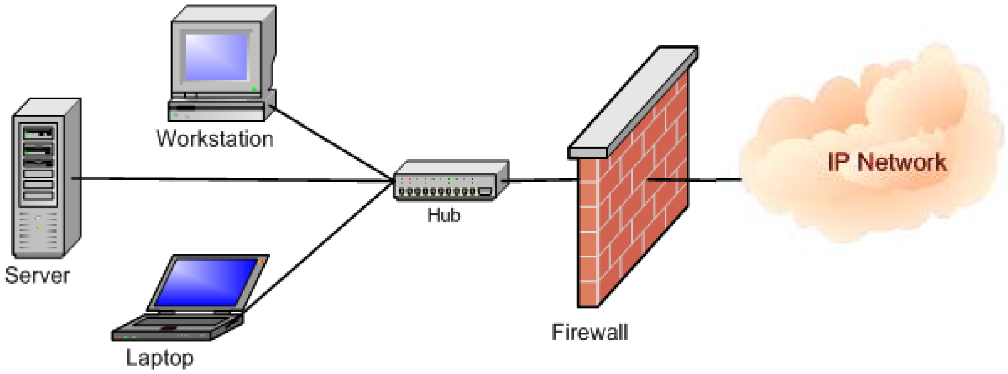
Controlled access to networks, machines or services

Enhanced logging and auditing of traffic

Ability to track network use and locate network abuse

Firewall

MikroTik RouterOS Firewall stands between the company's network and a public netvork, effectively shielding your computers from malicious hacker activity, and controlling the flow of data to the router, through the router, and from the router. *MikroTik RouterOS* firewall supports filtering and security functions that form your Internet using policy.



Stateful Filtering

MikroTik RouterOS Firewall is based on Stateful Filterig technology that can be used to detect and block many stealth scans, DoS attacks, SYN floods. Network communication is made up of small chunks of data called packets, and several of these packets are used solely to create, maintain, and finish the connection. The *MikroTik RouterOS* Stateful Firewall keeps in memory informtion on each connection passing through it. When a foreign packet tries to enter the network, claiming to be part of an existing connection, the firewall consults it's list of connections. When it finds that the packet doesn't match any of these, it can drop that packet and defeat the scan!

System Administration

MikroTik RouterOS Firewall is very easy to manage! System's architecture allows easy configuration of network address translation (NAT), transparent proxies, and redirection. The Firewall filtering rules are grouped together in chains. It is very advantageous, if packets can be matched against one common criteria in one chain, and then passed over for processing against some other common criteria to another chain. That makes the system a whole lot easier to administrate, using a smaller number of rules to create much more precise fire-walling.

Better stealth scan defence

Smarter Network Adress Translation

Blocks more DoS attacks

MikroTik RouterOS Firewall is based on:

- IP address filtering
- Port protocol filtering
- Network interface filtering
- Source MAC address filtering
- TCP protocol option

Applications:

- **Protection of the Router from unauthorized access**
  You can monitor connections to the addresses assigned to the router itself and allow access only from certain hosts to certain TCP ports of the router. The Firewall controlls all Internet information and warns and blocks intrusion attempt based on rules, customized by the user.

- **Protection of the customer's hosts**
  You can monitor connections to the addresses assigned to the customer's network and allow access only to certain hosts and services. You endow your customers with effective and proactive defence against malicious attacks.

- **Using Masquerading to hide the private network behind one external address**
  All connections from the private addresses can be masqueraded, and thay appear as coming from one external address - that of the router. The firewall will act as a gateway for your entire network to enable the office's network to share a single, safe connection to the Internet.

- **Enforcing the Internet Usage Policy from the Customer's Network**
  The Firewall allows you to controll connections from Customer’s Network and provides detailed traffic statistics of all the links.

- **Prioritizing traffic**
  You can mark packets by priority to ensure fastest connection to more important packets. This guarantees that all groups always get the appropriate bandwidth, providing controlable flow of network traffic and preventing bandwidth starvation.

- **Applying queuing to the outgoing packets**
  This feature allows to limit connection speed to certain group of packets. The hierarchy of class enables you to build a flexible, and very logical representation of your traffic.

For ordering information, contact sales@mikrotik.com

Office Address
Mikrotikls SIA
Pernavas 46
LV-1009, Riga, LATVIA
Phone: +371 7317700
Fax: +371 7317701
URL: http://www.mikrotik.com

OEM Sales Representatives
USA
EUROPE
ASIA
AFRICA
See our Web Page for addresses!