MODERN APPROACH OF FIREWALL IN LOCAL NETWORK

UDC: 004.056.52:004.732
DOI: https://doi.org/10.53486/tids2025.18

ANDRONATIEV VICTOR
Academy of Economic Studies of Moldova
andronatiev@ase.md
ORCID ID: 0000-0002-0294-457X

ZGUREANU AURELIU
Academy of Economic Studies of Moldova
zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

Abstract. In modern society, computer networks are increasingly used across a wide range of activities. According to data provided by CISCO, in 2020 the number of users and devices connected to the Internet reached 50 billion. While initially computer networks were used primarily for file sharing, email, and reading news, today they serve many more purposes—such as online conferences, medical appointments, online shopping, remote learning, gaming, social media platforms like YouTube and Facebook, Wikipedia, and more. Given this widespread expansion, hundreds of billions of dollars are invested annually in computer network infrastructure. To ensure proper functionality and user convenience, a high level of security is essential. Without proper protection, users and companies risk losing money, personal data, or intellectual property, which would erode trust in these technologies.

As a result, investments in cybersecurity are critical: better security protocols are being developed, network equipment and operating systems are becoming more secure, cybersecurity experts are being trained, and users are being educated on how to interact safely in a digital environment.

One of the key protection methods in network security is the use of firewalls. Firewalls can be implemented in various ways: on servers to protect the local network from external access (and vice versa), on networking devices such as routers, or built into modern operating systems. Additionally, certain applications that require high levels of security may include their own dedicated firewalls, known as next-generation firewalls (NGFWs).

Keywords: local networks, firewall, network security, filter rules, nat.

JEL Classification: D85, L86

INTRODUCTION

As of 2023, it is estimated that there are over 2 billion personal computers in use globally (UMA Technology, 2025). This data includes desktops and laptops, highlighting the significant prevalence of personal computing devices in households and workplaces. The widespread use of computers necessitates enhanced security measures. No one would use computers if they knew their data could be stolen, falsified, or deleted. One of the first methods of data protection was the firewall. Users access the Internet through local networks, whether from home or work. Initially, firewalls were used to protect users within local networks. With the exponential growth of the Internet, firewalls evolved, and today they are used on routers, servers, operating systems, and applications that require enhanced security.

The importance and relevance of this research topic stem from the fact that billions of dollars are spent annually on security. In 2024, global end-user spending on information security is estimated at $183.9 billion. In 2025, global end-user spending on information security is projected to reach $212 billion, a 15.1% increase from 2024, according to a forecast by Gartner, Inc. (see Table 1). Additionally, enormous sums are spent on training security specialists and regular users.

Table 1. Information Security End-User Spending by Segment, Worldwide, 2023-2025 (Millions of U.S. Dollars)

Segment	2024 Spending	2024 Growth (%)	2025 Spending	2024 Growth (%)
Security Software	87,481	14.2	100,692	15.1
Security Services	74,478	13.6	86,073	15.6
Network Security	21,912	9.6	24,787	13.1
Total	**183,872**	**13.4**	**211,552**	**15.1**

Source: *Gartner (August 2024)*

The first publication related to firewalls appeared in 1988. It described a packet filtering system that operated up to the third level of the OSI model (first-generation firewall). In 1989-1990, second-generation firewalls were introduced - these operated up to Level 4 of the OSI model, taking into account connections between stations. Then, in 1994, third-generation firewalls were launched - these operated up to Level 7 of the OSI model and considered the source and destination applications of packet flows (Bolun I., Andronatiev V., 2014). In 2012, next-generation firewalls (NGFW) were introduced, offering more detailed inspection of application-level aspects of the OSI model, such as intrusion prevention systems and web application firewalls, etc.

MAIN CONTENT

1. Firewall Description

A firewall allows only packets that comply with specific rules to pass through. These firewalls can be of two types: stateful and stateless. Stateful firewalls keep track of the state of data transfer connections (such as TCP streams and UDP communications) and perform dynamic packet filtering. They allow only packets belonging to known connections to pass. When a new connection is established, it is checked against the security policy. Once approved, all packets in the current session related to that connection are accepted. Stateless firewalls, which preceded stateful firewalls, treat each packet independently of others (in isolation) without considering connections. They analyze only the packet header (Greyson C., 2025).

To examine the functionality of the firewall, we will use MikroTik networking equipment, which provides the following capabilities (Haddad M., 2023):

- Filter Rules – define filter rules;
- NAT – define NAT rules;
- Mangle – define Mangle rules;
- Service ports – define service port parameters;
- Connections – characteristics of active connections to the router;
- Address Lists – create groups of IP addresses with common rules;
- Layer7 Protocols – define Application-level rules.

When defining *firewall rules*, it must be taken into account that NAT rules are applied first and only then the others. Depending on the source address and destination address, we distinguish the following types of traffic:

- input - entering the router;
- output - leaving the router;
- forward - forwarding through the router.

When filtering packets, in addition to the type of traffic, the type of service is also used. For example, we allow web browsing, but prohibit copying files. Or, we can prohibit certain web pages with malicious content using the port number, according to the service being examined. Table 2 shows port numbers for the most commonly used services.

Table 2. Widely used port numbers and protocols

Port number	Transport layer or Network (Internet) protocols	Application Layer Protocols
20, 21	TCP	FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
123	UDP	NTP
143	TCP	IMAP4
443	TCP	HTTPS, SSL
465	TCP	SMTP over SSL
989, 990	TCP	FTP over SSL
8080	TCP	Proxy
/1	ICMP	ping

Source: *Prepared by the author*

After identifying which type of traffic the packet corresponds to, we indicate which actions can be performed:

- *accept* – accept the packet;
- *add-dst-to-address-list* – add the destination address to the address list specified by the address-list parameter;
- *add-src-to-address-list* – add the source address to the address list specified by the address-list parameter;
- *drop* – drop the packet without notification;
- *jump* – move to another user-defined chain, by specifying the value of the jump-target parameter – the action is used to check the packet's compliance with a criterion from another chain;
- *log* – add a message to the system log to track the processed traffic. It is used to monitor data traffic;
- *passthrough* – ignore the current rule and move to the next one (it is useful for diagnostics, statistics);

- *reject* – reject the packet and send an ICMP reject message;
- *return* – passing control back to the point where the jump action was applied;
- *tarpit* – capturing and holding TCP connections (to the incoming TCP SYN packet, it is responded with SYN/ACK);

2. Examples of firewall rules

Filter Rules. Let's examine what traffic filtering options we can use. Firewall rules consist of two parts: a set of criteria (IF), to which the packet corresponds, and the action (THEN) that defines what to do with the given packet (RouterOS documentation, 2025).

First, let's protect the router from unauthorized access. For this, we need 2 rules. The first allows access only for the administrator's computer, the second prohibits access for everyone else. For remote connection, the Telnet and SSH protocols are used. The rules that perform these actions are specified below.

```
[admin@user1] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=input action=accept protocol=tcp src-address=192.168.120.10
     in-interface=ether2 dst-port=22 log=no log-prefix=""
 1   chain=input action=drop protocol=tcp dst-port=22,23 log=no log-prefix=""
```

As can be seen from rule number 0, access to the router is only for input traffic, port 22, i.e. SSH protocol. Since Telnet protocol, port 23 is insecure, connection through it is prohibited. In addition, the computer addresses 192.168.120.10 and the ether2 interface, i.e. local network are specified. From rule 1, it can be seen that for all other computers, from other interfaces, port 22 and 23 access is prohibited, because we have the drop action.

Another action, often used, is blocking access to certain services, for all users or some of them. For example, let's say we need to block access to web browsing, for certain users. For web browsing, the HTTP protocol, port 80, and the HTTPS protocol, port 443, are used. In order to indicate the rule for certain users, the most convenient is to use address lists. In the same way, we can block access not for users, but access from the local network to certain web pages on the Internet. Let's say we have a Deny list - a list of addresses that do not have access to web browsing and the other addresses, implicitly, have access to web browsing:

```
[admin@user1] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST          ADDRESS                          CREATION-TIME
 0   Deny          192.168.120.101-192.168.120.200  apr/21/2025 16:14:01
```

As we can see, in the 192.168.120.0/24 network, the Deny list includes computers with addresses from 192.168.120.101 to 192.168.120.200. Then, the web browsing blocking rule looks like this:

```
 1   chain=forward action=drop protocol=tcp src-address-list=Deny dst-port=80,443
     log=no log-prefix=""
```

An important role in the work of the firewall is its speed of operation. Usually, the more rules we have, the more secure the network is, because we give access only to the necessary services. Services that are not needed are blocked, or access to certain services is given only to certain

addresses. But, with an increase in the number of rules, the latency of the firewall increases (Artūrs C., 2024). One of the main methods of increasing the speed of the firewall is the use of connection status. In this way, connections can be classified as: new, established, related, invalid (see figure 1).

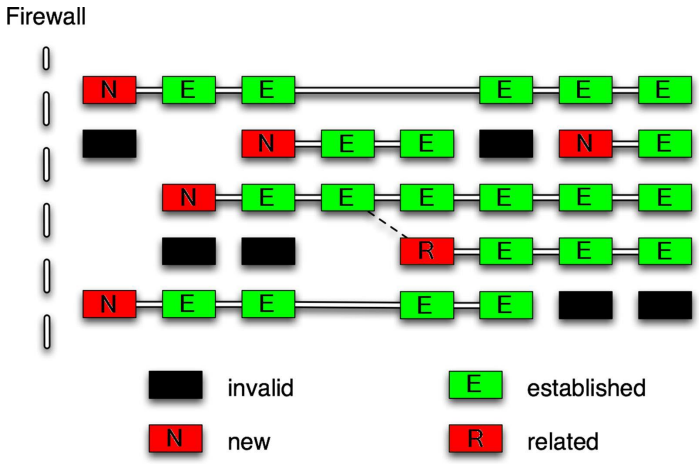


Figure 1. Classification of connections depending on their status

Source: *Mikrotik. First Time Setup. Available at: https://docs.calebsargeant.com/en/latest/networking/mikrotik.html#firewall.*

As can be seen from Figure 1, we have 5 connections, that contain packets of different types. It is recommended to check the first packets, of the *new* and *related* type. If these packets are accepted, then the other packets in the connection (*established*) can also be considered valid and *invalid* packets have been modified during transmission, so they are erroneous or malicious, and in this case, they must be rejected. Another important point is to let only new packets pass through the firewall, which means that the place of their placement is important. If they remain in the queue, then they are of no use, because new packets, anyway, pass through the entire firewall. In this case, they must be placed at the beginning of the firewall. Let's say that on average, each connection has 50 packets. Then using this method, theoretically, the speed of the firewall increases by 50 times. In this way, the mentioned rules look like this:

```
0  chain=forward action=drop connection-state=invalid log=no log-prefix=""
1  chain=forward action=accept connection-state=established, related log=no log-prefix=""
```

NAT Rules. Another type of firewall rules is *nat* rules. Network Address Translation (NAT) is necessary to transmit data from the local network to the Internet, and vice versa. Since the local network uses private addresses and the Internet uses public addresses, NAT changes the private address to a public one. This can be the external address of the router or server. When the response of the requested data comes, the reverse procedure takes place.

Depending on the number of public addresses used, NAT can be: one-to-one, one-to-many, many-to-many. One-to-one is when a single public address corresponds to a single private address. As an example, this method can be assigned to servers. Computers on the local network connect to the server via private addresses. And, computers on the outside via public addresses. One-to-many allows all computers on the local network to access the Internet via a single public address, thus saving enormous amounts of public addresses. In the case of large networks, several public addresses are used. This allows a large number of computers to access the Internet through several public

addresses. This method allows computers to access the Internet at a higher speed, compared to the one-to-many method.

Depending on the purpose of using NAT rules, they can be:

- *accept* – accept the packet;
- *add-dst-to-address-list* – add the destination address to the address list specified by the address-list parameter;
- *add-src-to-address-list* – add the source address to the address list specified by the address-list parameter;
- *dst-nat* – perform the destination NAT function;
- *jump* – jump to another user-defined chain;
- *log* – add a message to the system log to track the processed traffic.
- *masquerade* – perform the source NAT function, when the public address of the external interface (Out. Interface) of the router is not known;
- *netmap* – static 1:1 mapping of a set of IP addresses to another set. It is often used to distribute public IP addresses to stations in private networks;
- *passthrough* – ignore the current rule and move on to the next one (useful for diagnostics, statistics);
- *redirect* – replacing the destination address of IP packets with one of the local addresses of the router, redirecting the packets to the router;
- *src-nat* – performing the source NAT function, when the public address of the external interface (Out. Interface) of the router is known.

Next, let's get acquainted with how some rules work:

1. As can be seen in Figure 2, the computer on the local network uses the private address, but in order to send information to the Internet, this address is changed to the public address using the src-nat rule.

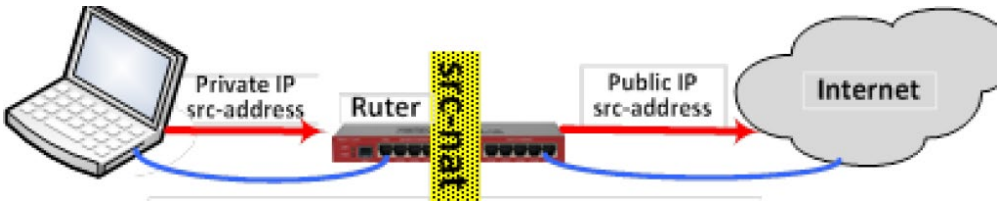


Figure 2. The src-nat rule

Source: *Bolun I., Andronatiev V., 2014. Internet şi Intranet.*

2. Another case is when someone from outside wants to connect to a server on the local network. This server can be: web server, ftp server, etc. Normally, local network users can connect without adding any rules, but users from outside the network need to add a *dst-nat rule*.

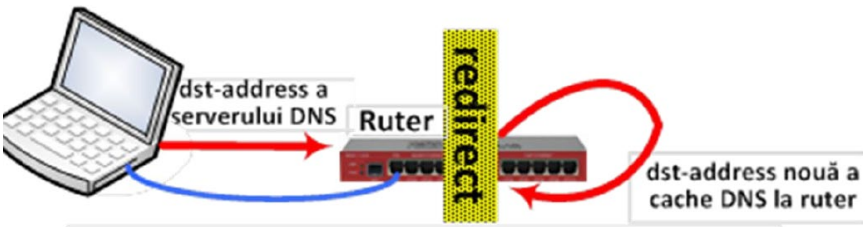


Figure 3. The redirect rule

Source: *Bolun I., Andronatiev V., 2014. Internet şi Intranet.*

3. In some cases, to save traffic or increase security, the redirect rule can be used. For example, in many cases users use the server address of Google (8.8.8.8) as a DNS server. Adding the redirect rule allows to reduce the use of external traffic, because the router instead of forwarding the DNS request outside, uses the cache on the router, (see Figure 3). This is very important when the Internet access speed is low or the network is under maximum load.

CONCLUSIONS

Nowadays, computers are used in practically all activities: at work, at home, for communication, online shopping, reading news, social networks, for tourism, weather forecasting, information search and many others. This is where the importance of securing user data comes from, because no one will use the Internet if they know that the user's sensitive data can be stolen, deleted, modified. Since the early days of the use of computer networks, one of the first means of protecting data has been firewalls.

If from the beginning the firewall worked at layer 3 of the OSI model (generation 1) and was used to protect the user's local network, with the evolution of the Internet and the exponential growth in the use of computer networks, the firewall also evolved. Today, 4th generation firewalls are used, which work within applications that require a high level of security. Even though every modern operating system has its own firewall, we see that firewalls are also widely used by applications at level 7 of the OSI model. In addition, if better security is needed, more powerful firewalls can be installed on computer, even though every operating system has its own firewall. So, we see that if initially the firewall was used only on the router, now it is used in different places: on the router, in the operating system and in applications.

In this paper, we examined what a firewall is and how it works, for this we examined Filter Rules and NAT rules. Since the firewall increases the latency of data transfer, special attention was paid to the performance of the firewall. For example, the use of address lists, connection status, redirect rule and correct programming allow to secure the transmitted information without annoying retentions.

REFERENCES

1. Bolun I., Andronatiev V., 2014. *Internet şi Intranet.* Chişinău: Editura ASEM.
2. Haddad M., 2023. *MikroTik MTCNA- Student Guide*. Independently published, ISBN-13: 979-8391913528.
3. Greyson C., 2025. *Firewall Configuration and Management: Advanced Strategies for Securing Your Network.* Kindle Edition.
4. *RouterOS documentation*, 2025. Available at: https://box.mikrotik.com/d/1a069dba20724f279e30/files/?p=%2FROS-200525-1501-900.pdf, [Accessed 07.06.2025].
5. Artūrs C., last updated by Normunds R. on Nov 29, 2024. *NAT.* https://help.mikrotik.com/docs/spaces/ROS/pages/3211299/NAT, [Accessed 07.06.2025].
6. UMA Technology, 2025. *How Many Computers Are In The World?* Available at: https://umatechnology.org/how-many-computers-are-in-the-world-up-to-date-stats/, [Accessed 04.06.2025].
7. STAMFORD, Conn., August 28, 2024. *Gartner Forecasts Global Information Security Spending to Grow 15% in 2025.* Available at: https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025, [Accessed 04.06.2025].
8. *Mikrotik. First Time Setup.* Available at: https://docs.calebsargeant.com/en/latest/networking/mikrotik.html#firewall, [Accessed 01.06.2025].