Setting up firewalls to keep your networks secure

Lobastov Denis

Abstract

This article provides an overview and practical recommendations for setting up a firewall to protect your networks. We will look at the role of firewalls in protecting against attacks, the principles of network security, and methods for configuring firewalls. We demonstrate with specific configuration examples that how a firewall can effectively block unwanted traffic and keep your network secure. This article intended for beginners and professionals, as well as information security enthusiasts.

Key words: Firewall configuration, network security, unwanted traffic.

In today's media environment, network security is a top priority for organizations and individuals. The ever-increasing number of digital threats and attacks targeting data confidentiality, integrity and availability underscores the need for effective security measures. In this context, the creation of a firewall as a critical component of network security becomes a key task in protecting networks. Firewalls play an important role in creating barriers between the external environment and internal network resources. They can monitor and modify network traffic, allowing only authorized packets to enter the network, thereby preventing potential attacks and unauthorized access. However, for a firewall to be effective, it must configured based on the specific needs and threats of the network.

For further understanding, it is necessary to explain what a firewall is, what its role is, and the dangers that a firewall is designed to combat.

A firewall is a network device or software designed to provide security to computer networks. Its main function is to monitor traffic between networks and determine what data can and cannot pass through it. Firewalls used to protect networks from unauthorized users, Internet-attacks and other security threats. Firewalls can operate at different layers of a network, including the network layer (network firewall) and the application layer (application firewall). It can configured to block or allow certain types of traffic based on various criteria such as IP addresses, ports, protocols and applications.

In addition to the firewall built into the Windows operating system, there are many other firewalls, both free and commercial, designed to provide network security. Here are some of them:

Norton Internet Security
Mcafee Firewall
Bitdefender Total Security
Avast Free Antivirus
Comodo Firewall
Glasswire

All of these software have their own characteristics, advantages and disadvantages, but without exception, all of them are designed to fulfill their task - to take on the role of our Firewall. However, in this article we will be looking at a standard firewall, the Windows Firewall. Despite the fact that this is a system application, i.e. Already built into the system,this does not mean that it is inferior to its competitors described in the list above.

We will also touch on the threats that the firewall protects us from. Let's list some of them:

Unauthorized access: Firewalls can prevent unauthorized attempts to access a network or computer. This may include hacking attempts or unauthorized access.

Malicious Software: Firewalls can detect and block malicious software such as viruses, Trojan horses and spyware, preventing it from entering your network or computer.

Spam and email attacks: Firewalls can filter spam, protect against various email-related attacks, such as phishing, and email attacks using malicious attachments.

Ddos-attacks: Firewalls can help prevent denial of service (ddos) attacks, which aim to overwhelm a network by flooding it with traffic.
Unauthorized applications: Firewalls can block unwanted or unauthorized applications installed on computers on a network to prevent potential security threats.
Attacks on operating systems and services: Firewalls can filter traffic to operating systems and services to prevent vulnerabilities and attacks associated with them.
The purpose of this study is to configure and test the Windows Firewall. Creation of a practical setup guide, as well as analysis of the results.
The Windows firewall was chosen for work because of its availability; as mentioned earlier, it is already built into the system, which means that all users, both advanced, likewise, beginners, when starting a computer on the Windows operating system for the first time, will encounter this particular firewall. Detailed setup steps, how to open the firewall, navigation, and an explanation of the various steps and components will be covered. In addition, the autonomous operation of the firewall will be demonstrated.
For testing, applications that have not previously opened and require access to the network will be launched, and through the service on the Internet we will check whether the firewall is able to prevent unauthorized access to the network.
First, we need to find a firewall on our device. The operating system of the experimenter's computer is Windows 10. First, in the search bar (Fig. 1) or directly from the executable file (Fig. 2) on the desktop, open the control panel.

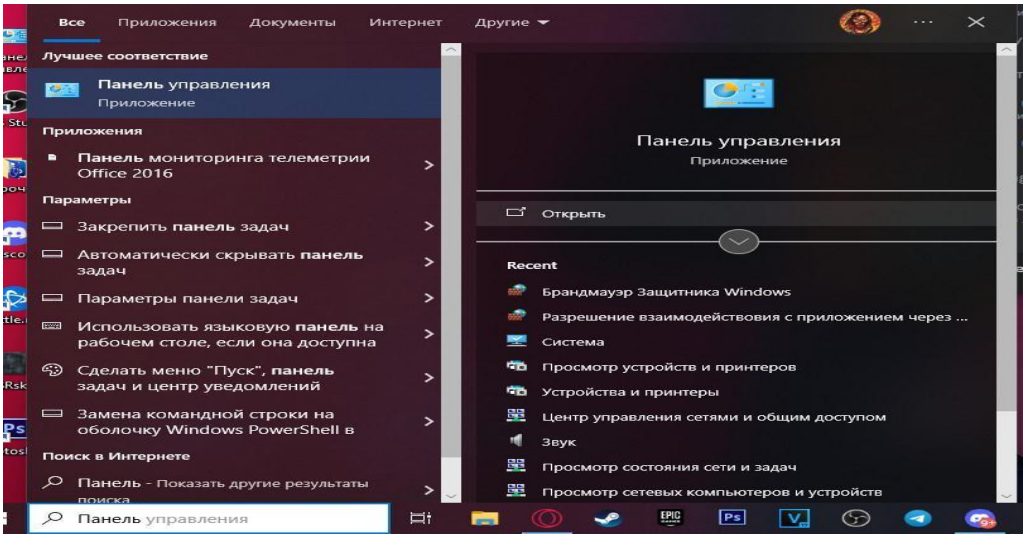

Figure 1. Finding the control panel in the search bar

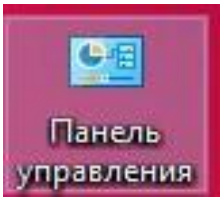

Figure 2. File opening the control panel

Having opened the control panel, many elements appear in the window, among them we are looking for “Windows Defender Firewall” (Fig. 3).
Having opened the firewall, its window appears in front of us (Fig. 5). There is little information in this window; the only thing that interests us here is which network is connected to the protection. It can be seen that the user’s network profile is guest/public. The difference between private and guest profiles can be found in the network settings (Fig. 4)

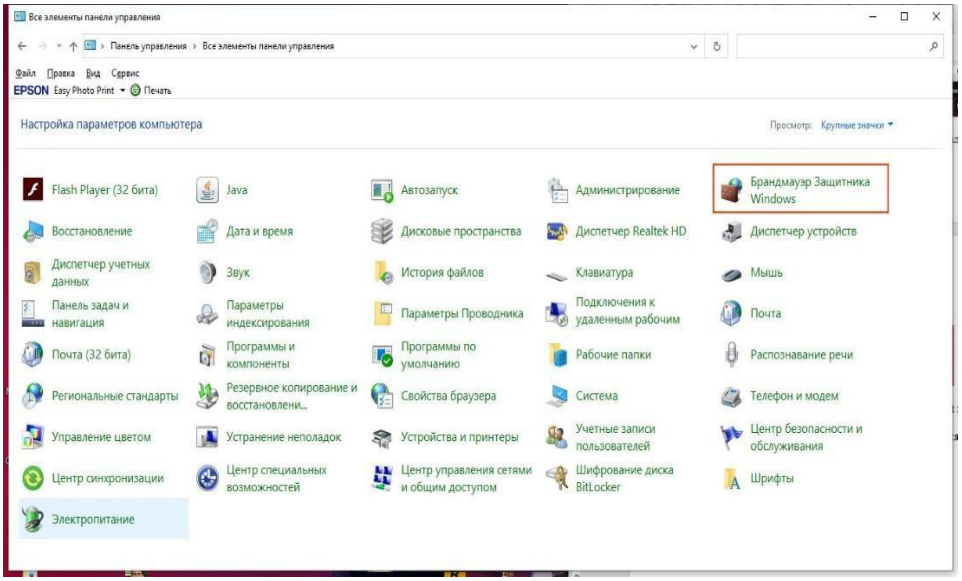

Figure 3. Control panel window. Windows Defender Firewall highlighted in red.

Figure 4. Selecting a network profile

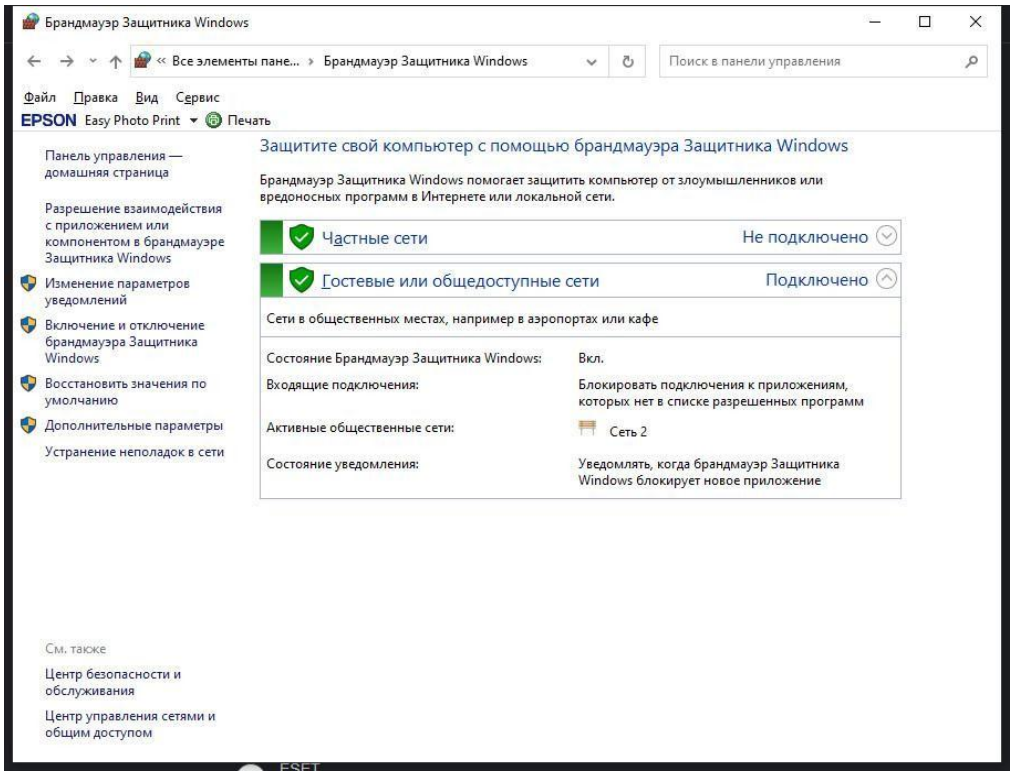

Figure 5. Firewall window

To configure the firewall, follow the links on the left (Fig. 5). The first two links with the image of a shield, namely “Change notification settings” and “Turn Windows Defender Firewall on or off” lead to the same window (Fig. 6), so that there is not much difference in which of them to go.

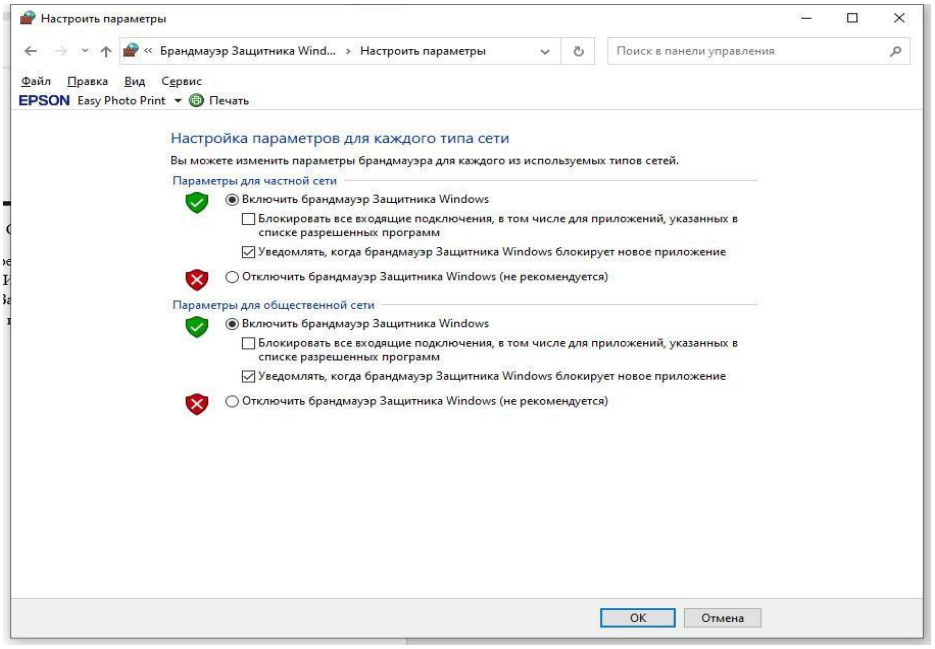

Figure 6. Firewall settings window

Figure 6 clearly shows that the settings can changed for different network profiles. When setting up, it is advisable to have a check mark where they are in Figure 6. With this setup, every time the firewall blocks something, it opens notifications, as in Figure 7. This is a one-time action, since after receiving a notification, we can either allow access or deny it (in this case, the notification will come again when the application requests access to the network, unless it is permanently deleted).

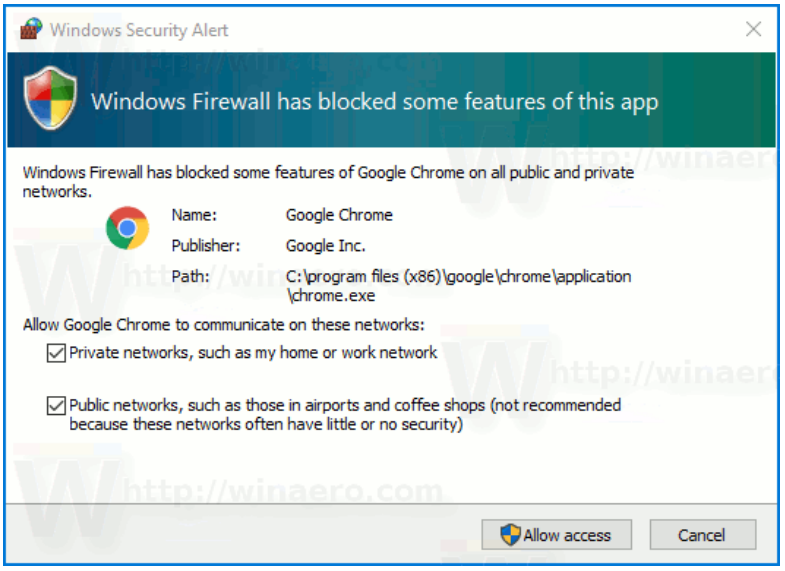

Figure 7. Firewall Alert

The very first checkbox (Fig. 6) makes it clear that any incoming connections will be blocked. This is very important if you suspect that you have been attacked, and this feature will help you if:
Your network is local and does not require remote access
Threat of bot-net teams or miners
Safe system diagnostics required
The third point, as the text says, is not recommended to be used. Under no circumstances should you disable the firewall unless you know what you are doing. You should not risk your safety for the sake of access, because... In rare cases, the firewall itself may block a secure application, but a non-advanced user cannot know this, accordingly, without proper knowledge, you should not deviate from the recommended parameters. In addition to the parameters, there is also a more extensive list, this is a list of rules. To access it, among the links in Figure 5, you need to select the “Advanced parameters” item. In this window we are interested in the rules for incoming and outgoing connections (Fig. 8 and 9).

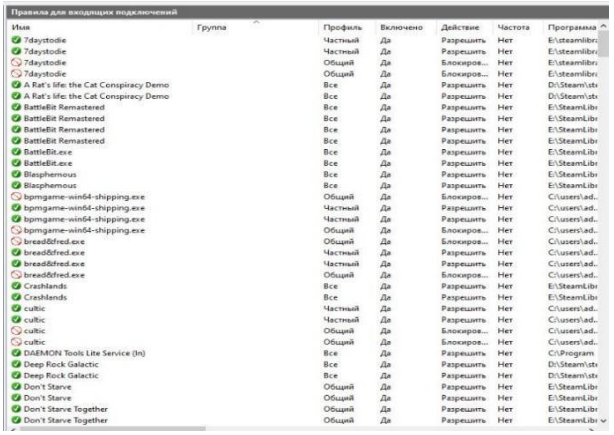

Figure 8. Rules for incoming connections

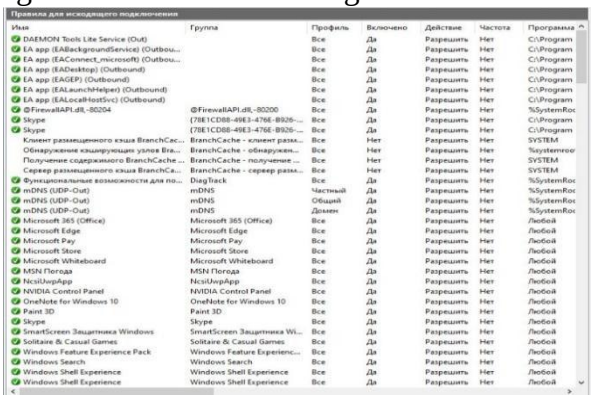

Figure 9. Rules for outgoing connection

Here we see two large lists. Once a process registered on the network, we can manually regulate access through the firewall. In the end, it is worth checking our safety. There are online services for this, in particular we will take Shield Up. This firewall test site will attempt to connect to us directly using upnp (Universal Plug and Play) technology. The result shown in Figure 10.

Figure 10. Probing result

As can be seen from the results, the probing attempt was unsuccessful and even the site itself tells us that this is good news. To check your own safety, you can read it yourself using the link given above.

Conclusion

Installing and testing a firewall is an important step in ensuring network security. In this review, we discussed the firewall system in detail, reviewed its key features, including legal and security measures, and tested its effectiveness in preventing attacks and protecting the network. Using a firewall effectively requires an understanding of network threats and network needs. The configuration must be tailored to specific scenarios and security requirements to provide optimal protection. During testing it was demonstrated that a properly configured firewall can successfully block unwanted traffic and prevent a variety of attacks. Based on the results of our research, we can conclude that installing a firewall is an important step in ensuring network security and protecting critical resources. It allows you to restrict access to the network, reducing the risk of data leaks and potential attacks. This work provides a resource that can be used to improve network security and ensure information integrity.

References

[1] https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/best-practices-configuring
[2] https://en.wikipedia.org/wiki/Windows_Firewall
[3] https://en.wikipedia.org/wiki/Firewall_(computing)
[4] https://www.grc.com/x/ne.dll?Bh0bkyd2