Techno Science
International Scientific
Journal of Technical
Sciences

Firewall for the sake of software protection

HAMZA SUŠIĆ, ALJO DELIĆ

FACULTY OF TECHNICAL STUDIES, UNIVERSITY OF TRAVNIK, BOSNIA AND HERZEGOVINA

ABSTRACT

Nowadays, firewall systems are necessary for every network that is in any way connected to the Internet. Due to a large number of computers and the inability to completely control Internet communication, it is only a matter of time before an unauthorised intrusion into private networks lacking a firewall protection system takes place. By placing a firewall device between two or more network segments, one can also control the access rights of certain users in specific parts of the network. In such a case, firewall is designed to allow access to valid requests and block all others. Firewall also represents an ideal solution for creating a Virtual Private Network since it creates a virtual tunnel for encrypted data. You might even say that firewall is a service (typically consisting of a firewall device security protocol) enabling the user to filter certain types of network traffic with the goal to increase security and provide a certain level of intrusion protection. If a system has firewall, it implies that the decision on what is allowed and what is not has already been made. The basic function of Firewall lies in examining IP packets travelling between the client and the server, whereby establishing control over the information flow for each service, by IP address and port in both directions.

Keywords: software, protection, firewall

Firewall ("A protective wall")?

Firewall is a security element placed between a local and a public network (the Internet), which is designed to protect classified, corporative and user data from unauthorised users (by blocking and denying traffic according to the rules defined by the adopted security policy).

Firewalls are generally classified as network-based or host-based. Network-based firewalls are placed on network computers, WANs and the Intranet. They are either software devices operating on general-purpose hardware or intrusion protection hardware devices. Intrusion protection hardware devices can also offer another functionality to the internal network they are protecting such as DHCP (protocol) or VPN (Virtual Private Network) server for the network.
Host-based firewalls are placed on the network node itself and they control network traffic to and from the machines. Each one has its advantages and disadvantages. However, each plays a part in layered security. Firewalls also vary depending on where the communication is taking place, where the communication is intercepted and the state that is being traced.

Thereby, there can be two types of firewalls, namely, hardware and software. This presentation will deal with software firewall.

Hardware firewall

Firewall, as a part of hardware within the computer network, has the ability to prevent an irregular data transfer through the network which is restricted by the security policy. Firewall is in charge of controlling the data flow between different zones in a computer network. Usually, the Internet zone is considered insecure, while the Local Area Network is deemed relatively secure.

The most important goal is to establish a normal relationship between the two zones so that one does not harm the other. Most frequently, firewall makes sure that a harmful code (virus, worm, etc.) does not enter into the computer through the global network - the Internet. In layman's terms, firewall prevents viruses from entering a computer, but it cannot cure, i.e. remove them.

Firewall cannot work on its own and, most frequently, it requires a more experienced user who will allow or deny access to a network activity. Firewall is the fundamental component constituting a secure computer network which is a requirement for normal operations.

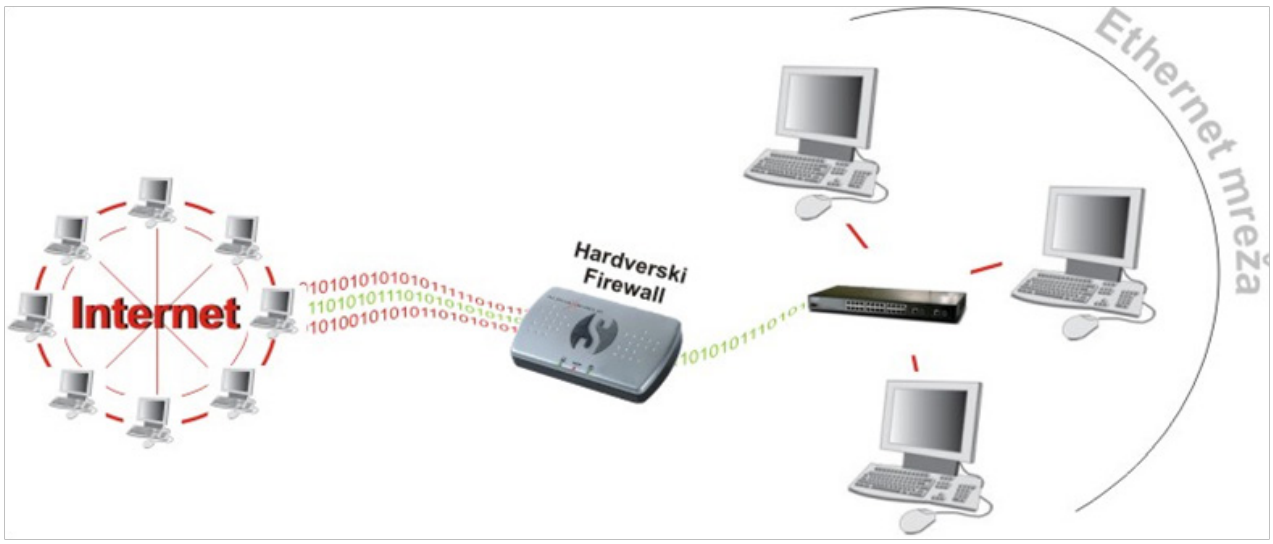

Image 1: An illustration of an operating hardware firewall

Software firewall

Traditionally, software or personal firewall is a type of software installed on the end user's computer which controls network traffic to and from a computer, permitting or denying communication based on a security policy. A personal firewall differs from a conventional firewall due to the fact that there is no hardware difference between the firewall software and user applications. A personal firewall will usually protect only the computer on which it is installed, with the exception when other computers share the Internet connection from the protected computer.

Softwere fairwall problems and weaknesses

- Instead of decreasing network services, a personal firewall is an additional service using system resources, and can also be a target of an attack
- If the system has been compromised by malware or similar unwanted software, these programmes can also manipulate the firewall, because both are running on the same system. Security experts have demonstrated that there may be numerous ways to bypass or even completely shut down personal firewalls
- For home users, shutting down all network services and installing latest updates is usually sufficient to protect against external attacks
- Since they are installed on the system they protect, attacks on the firewall itself may affect the system and vice versa
- They frequently alert the user about an attack when there is no need to do so, e.g. when attempting to connect to a closed port, or they inaccurately interpret network traffic as an attack

Regardless of the above stated, as well as the opinions of some experts that personal firewall only provides a false sense of security, Internet activities on a Windows-based system without a form of firewall are nowadays extremely risky.

Types of external attacks and protection against them

Firewalls lacking a sound and strong protection, a certain policy (rule) for incoming packets and data, are susceptible to various types of attacks.
If a firewall does not support the creation of Virtual Private Networks (VPNs), and the organisation wants to allow access from certain IP addresses to the Local Area Network, it is possible to configure the firewall to allow passage to the packets and data with precisely determined source IP addresses. However, such a setup has numerous disadvantages. For example, an attacker can get hold of the packets and discover the logical address which is allowed to connect to the Local Area Network. Subsequently, the attacker can create packets assigning them the logical address of the computer allowed to connect as the source address, and so, through specifically customised packets, inflict damage to the Local Area Network. It is necessary to configure the firewall so that it prevents various existing attacks. The majority of today's firewall producers proudly emphasise the attacks their firewalls are immune to, but new types of attacks are developed every day, and they are more complicated and complex. Nevertheless, each firewall should be immune to the familiar attacks such as:

Port-Scanner

A Port-Scanner attack is founded on discovering open TCP and UDP ports by sending SYN or FIN packets to the targeted ports and waiting for an RST response. It is necessary to limit the number of such scans.

Ping-of-Death

A Ping-of-Death attack can cause an operating system crash if a large number of ICMP echo requests are directed towards the computer. The best solution is to forbid echo request packets, and the alternative solution is to restrict the number of ICMP echo requests.

Address Spoofing

An Address Spoofing attack enables the packet to be forwarded from an external environment to an internal computer if an attacker uses one of the addresses within the Local Area Network as the source address. In this case, firewall is perhaps configured to allow the packet to pass and so, the target computer can receive the specifically customised packet. In order to prevent this type of an attack, it is necessary to forbid forwarding packets which have one of the local addresses as a source address, and the environment connected to the Internet as an input environment.

SYN-Flood

A SYN-flood attack is based on the attacker's transmission of a large number of connection TCP packets with a SYN flag set and ignoring the TCP response with the SYN and ACK flags set. Thereby, the resources of the target computer are occupied by answering the packets.In order to prevent such a form of attack, it is necessary to restrict the number of incoming TCP packets in the firewall.

Smurf

A Smurf attack belongs to the group of attacks whose goal is to prevent certain servers and computers from operating, the so-called DoS (Denial-of-Service) attack. An attacker sends an ICMP echo request packet to the broadcast address of the entire Local Area Network. This addresses all computers within a Local Area Network. The target computer that is sought to be disabled through a large number of responses is stated as the destination.
To defend against this type of an attack, it is sufficient to disable the broadcast packet in the firewall configuration file.

Conclusion

In today's world where Internet is an important and necessary resource in all organisations, it is highly important to pay particular attention to computer security. Thereby, firewall plays an important role since it protects organisations from numerous malicious Internet users. They are the first barrier an attacker has to pass so as to come to the desired goal - protected computers.
Choosing an appropriate firewall is getting more difficult since there is an increasing number of firewalls on offer. Such firewalls can be commercial or free. Commercial firewalls usually offer easier configurations and a larger number of options. Free firewalls are usually useless without an expert to configure and maintain them.
Apart from the classification to commercial and free ones, firewalls can be divided into those intended for Windows operating systems, as well as firewalls intended for Unix/Linux operating systems. Their performance and options are basically the same, and some firewall producers make firewalls that work on both operating systems.

Depending on the users' needs, it is possible to configure a firewall that protects the Local Area Network from unauthorised and malicious users in different ways. Thereby, it is possible to use different solutions, either configurational or software.Malicious software develops alongside the development of computers. That which mostly stimulated the development and spread of such programmes is the computer network. Before the appearance of networked computers, the only way of transferring malicious software was through an infected floppy disk, and such programmes had incomparably lower chances for spreading further. With the appearance of the Internet and services like electronic mail, the possibilities of transferring malicious software drastically rose. They have soon started to spread at a much higher speed and used more sophisticated ways of transference.
As the number of computers with Internet access grew, and the Internet increasingly started becoming a global network, so the infections became more serious and most frequently happened at a global scale. New types of malicious software emerged, with their primary goal no longer being an infliction of damage to other users, but collecting or stealing their information. Using Internet to perform financial transactions leads to the appearance of a new form of crime - electronic crime.

References

1. Rolf Oppliger: "Internet Security: firewalls and beyond", 1997 (Accessed 10th September 2018)
2. James F. Kurose, Keith W. Ross, "Computer Networking: A Top-Down Approach Featuring the Internet", 2001 (Accessed 10th September 2018)
3. Rob Pickering, Internet Firewall Tutorial, 2009 (Accessed 11th September 2018)
4. Peter Szor, The Art of Computer Virus Research and Defense, Addison Wesley, 2006 (Accessed 10th September 2018)
5. Tetsu Iwata Masakatsu Nishigaki, "Advances in Information and Computer Security", 2011 (Accessed 11th September 2018)
6. https://www.netiq.com/documentation/netiqaccessmanager4/target_installation/data/b651hwh.html (Accessed 10th September 2018)
7. https://www.microsoft.com/en-us/windows/comprehensive-security (Accessed 11th September 2018)

Firewall u cilju zaštite softvera

SAŽETAK
Firewall sistemi su danas neophodni u svakoj mreži koja je na bilo koji način povezana sa Internetom. Zbog ogromnog broja računara i nemogućnosti potpune kontrole komunikacije koji se Internetom odvija, pitanje je kada će doći do neovlaštenog upada u privatne mreže koje nisu pod zaštitom firewall sistema. Postavljanjem Firewall uređaja između dva ili više mrežnih segmenata može se kontrolisati i prava pristupa pojedinih korisnika u pojedinim dijelovima mreže. U takvom slučaju Firewall je dizajniran da dopušta pristup valjanim zahtjevima, a blokira sve ostale. Firewall ujedno predstavlja idealno rješenje za kreiranje Virtualne Privatne mreže jer stvarajući virtualni tunel kroz koji putuju kriptirani podaci. Moglo bi se reći da je firewall servis (koji se tipično sastoji od firewall uređaja pravilnika o zaštiti) koji omogućuje korisniku filtriranje određenih tipova mrežnog prometa sa ciljem da poveća sigurnost i pruži određeni nivo zaštite od provale. Ako sistem raspolaže Firewall-om, to znači da je odluka o tome šta je dozvoljeno, a šta nije već donijeta. Osnova rada Firewall-a je u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i portu u oba smjera.

Ključne riječi: rizik, akcident, upravljanje, prevencija, informacioni sistem, životna sredina, zaštita, bezbjednost, kvalitet života, organizaciono-funkcionalni model

Received: February 08, 2018 / Accepted: February 18, 2018
Correspondence to: Hamza Sušić, University of Travnik, Faculty of Technical Studies, Travnik, Bosnia and Herzegovina
E-mail: hamza_susic@hotmail.com