Data protection by means of firewalls of new generation

Olexander Terentyev[1], Ievgenii Gorbatyuk[2]

Kyiv National University of Construction and Architecture
Povitroflotsky Prospect 31 Kyiv, Ukraine, 03037
[1] terentyev79@ukr.net, orcid.org/0000-0001-6995-1419
[2] gek_gor@i.ua, orcid.org/0000-0002-8148-5323

ENTRY

With every year volume the internet of traffic and devices interconnect grows. Accordingly, and a necessity grows for network safety both personal devices and large the ramified informative networks. Firewall it one of basic instruments that is used for protecting of networks from the unauthorized attempts of access. However, the firewalls of present generation already are not able independently (without the additional and permanent tuning) to provide sufficient strength security [1].

A computer network consists of two or more computers that is connected to the exchange resources, such as printers, scintiscanner, databases, files, programs. Computers in a computer network can be connected by means of coaxial cables, twisted pair, fiber optics, companions or infra-red rays of light. When a computer network is connected to the Internet, even a separate computer can become the aim of hackers and harmful software. A firewall can provide sufficient safety that will allow to avoid threats or mother facilities for a fight against network attacks. A firewall is an obstacle or guarantee that is intended for defense your the personal computer, plane-table or telephone from ill-intentioned software that exists in the Internet. A firewall must guarantee that only the authorized user has an access to the operating system or to the computer interconnect, protecting private information and protecting the users of computers from the thefts of person. In most cases firewalls block an unauthorized division about that the users of computers do not know [2]. Data interchange between your computer and servers and routers in a network, and knots that are between networks watch these data (what sent in packages), to check, or safe they or not.

A firewall is the important component of architecture of safety of computer network. A firewall is software or vehicle device that filters information (packages) that comes over the Internet to your personal computer or computer network. Firewalls can decide or allow or block network traffic between devices on the basis of the rules preliminary adjusted or set by the administrator of firewall.

AIM OF THE ARTICLE

The aim of active research consists in that, to generalize the evolution of traditional firewall, as a result of what drawn conclusion that a traditional firewall has certain limitations. Features and advantages of firewalls of new generation are examined in the real article.

DATA PROTECTION BY MEANS OF FIREWALLS OF NEW GENERATION

A firewall protects the computer (decorate a pattern) of user from an unauthorized remote division. He can block reports that allude to undesirable content, and watches and controls network traffic into a network. In accordance with certain politician of safety, firewall – a vehicle or programmatic device allows to the enormous amount of networks to communicate inter se. A firewall is used, when a requirement is in the networks of different level of power for a commonunication from each other. Firewall software works on host, that is connected both to reliable and unreliable networks. Host-Operating system is responsible for implementation of functions of routing that is able to execute many operating-rooms of the systems. Operating system host must be maximally protected to establishment of firewall software [2].

Firewalls can be classified on three types:

1. *Filters of packages:* Set of rules is used on the basis of accordance of the fields in the title of IP or TCP to every entrance package of IP, decides and then, to send or cast aside him.

2. *Sluices of level of additions:* He is also named proxy server that operates as retransmitting of traffic at the level of additions. Using the sluices of contacts of program users, a query gets only to the authentic users. A sluice of additions is specific services, such as FTP, TELNET, SMTP or HTTP.

3. *Sluices of level of chain:* a sluice of level of chain can be separate or by the dedicated system. A sluice sets two TCP-connections, as he does not allow to the end of TCP-connection. After establishment of connections of TCP a sluice retransmits the segments of TCP from one connection to other without the study of content. The function of defence determines, what connections will be settled, and that is forbidden.

Without regard to that a firewall provides safety for users, all above-mentioned types of firewall have certain limitations, as remembered below:

- A firewall can not scan every entrance package on content of virus. Thus, he can not protect an intranet from a viral threat.
- Firewall does not provide the system of exposure of encroachments (IDS).
- Firewall can not effectively (quickly) process an Internet-traffic.
- Firewall can not protect from any attacks that walk around a firewall.
- Accordingly, it does not protect from internal threats from within (man - in - the - middle attack).
- Firewalls can not protect from to the tunnel most program protocols.

The firewall of new generation must contain:

- Are Standard possibilities of firewall, such as a state complete inspection.
- It is the Complex prophylaxis of encroachments.
- It is program Awareness and control needed, to define and block the risky programs.
- Are the Renewed ways for including of future informative channels.
- Are Methods of decision of problems of informative threats that develop only [1, 3].

DEVELOPMENT OF TRADITIONAL FIREWALL IS TO THE FIREWALL OF NEW GENERATION

1. *Firewall of only management threats* (UTM).

The firewall of UTM – it only a firewall that inserts the face of user in accordance to the criteria of firewall, allowing to the enterprises to influence politicians and to identify users directly after the user name, but not through IP-address. It is a powerful vehicle firewall that provides the stationary and deep review of packages, protecting enterprises the same from the attacks of imitation of IP, access, authentication users, defense of network and level of additions control. In this work development of criteria, functions of UTM will be studied and it is shown, as far as UTM better comparatively with an ordinary firewall and VPN [3].

The firewalls of UTM bring front-rank technologies of network safety for small and midsize businesses and remote offices / of branches. Traditional firewalls can block / to accept a traffic only on the basis of IP-addresses and ports and provide small defense out of it. This approach quickly becomes antiquated in the today's Internet, where many additions send / get traffic through ports that is usually settled by traditional firewalls.

Features of UMTS:

- It is the Only instrument room platform.
- It is the Compatible interface of management.
- Contract One agreement / contact of supplier.
- It is Decline of area of DPC.
- It is Decline of consumption of electric power.
- It is the Minimized point of refuse / of delay.
- It is Simplified architecture of network safety.
- It is the Mixed protecting from a threat.
- Advantages of UTM:
- It is Diminished complication.
- It is Lightness of development Integration.
- It is the Easy survey of defects.

2. *Firewall of new generation* (NGFW).

NGFW combines in itself the functions of traditional firewalls, such as filtration of packages, translation of network addresses (NAT), blocking of URL-addresses and virtual private networks (VPN). He answers the functional of quality of service (QoS) also. Features include prevention of encroachments, verification of SSL and SSH, deep verification of packages and exposure of the harmful programs on the basis of reputation, and also awareness with additions. NGFW use more careful style of verification, checking up the actual loads of packages and co-coordinating signatures on harmful actions, such as on-the-road attacks and ill-intentioned software. His aim – to include glowed the more model of OSI.

Features:

- It is Awareness of additions.
- It is the State inspection.
- In three-throw system of protecting from interference (IPS).
- It is Awareness in relation to an identity (user and control group).
- Are bridges or routed modes.
- It is Possibility of the use of outsourcing.

Advantages:

- NGFW combines the traditional functions of firewall with the prophylaxis of encroachments, anti-virus and protocol filtration.
- Possible for monitoring and updating from one cantilever.
- NGFW scans content for prevention of source of data and stop of threats by the detailed verification of motion real-time.
- It is diminishes the amount of necessary devices of safety.

3. NGFW, oriented to the threat.

These firewalls include all possibilities of traditional NGFW, and also provide the extended exposure and removal of threats.

Features:

- Guided by visibility (analysis of threats).
- Focused on threats.
- Set at once on a platform.

Advantages:

- It understands of that, what assets risk most.
- It is the rapid reacting on attacks.
- Better find out evasive or suspicious activity.
- It is considerably more short time of cycle of exposure-reaction.
- It is lightness of introduction and reduction to complication.

CONCLUSIONS

In this article the short analysis of firewall of new generation is given in comparison a traditional firewall. After a short study we came to the conclusion, that the firewall of new generation combines in itself the features of traditional firewall and has the features. It is the system of network safety, based on the vehicle and programmatic providing, for an exposure and blocking of difficult attacks, applying politics of safety by means of the simplified management and reduces the total worth of the use and defence of the informative systems.

Keywords: firewall, UTM, filtration of packages, network safety, firewall of new generation.

REFERENCES

1. **Geier E., 2011.** Intro to Next Generation Firewalls. EsecurityPlanet. URL: https://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html (access: 17.06.2019).
2. **Gralla P., 1999**. How the Internet Works. Indianapolis: Que Pub, 340.
3. **Imran M., 2015**. Role of firewall Technology in Network Security. International Journal of Innovations & Advancement in Computer Science, Vol.4, No.12.
4. **Microsoft** Corporation. Improving Web Application Security, **2010**. Threats and Countermeasures. Docs Microsoft.. URL: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649432(v=pandp.10) (access: 18.06.2019).
5. **Stavroulakis P., Stamp M., 2010**. Phishing attacks and countermeasures. Crete: Springer Science & Business Media, 867.
6. **Kondratenko V., 2019**. On creation of the universal mathematical management decision making theory. Underwater Technologies, Vol.09, 3-12.