ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

UDC 004.77/.72 DOI: https://doi.org/10.30837/2522-9818.2025.3.180

I. CHEPURNA, D. FROLOV

A METHOD FOR INCREASING THE PRODUCTIVITY OF A DISTRIBUTED FIREWALL BASED ON PROXMOX IN CORPORATE COMPUTER NETWORKS

The subject of the study in the article is a method for increasing the performance of a distributed firewall based on LXC containers of the Proxmox VE environment for corporate computer networks. The goal of the work is to develop approaches to ensure a high level of efficiency of a distributed firewall for monitoring and managing traffic in corporate networks and virtualized networks, enabling the minimization of delays during traffic filtering and ensuring reliable operation of the corporate network under conditions of limited hardware resources. To solve the problem, the following research methods were applied: theoretical analysis of literature sources; analysis of the features of the application of containerization technology for implementing dynamic network traffic control, study of methods to improve computational resource utilization efficiency in environments with limited hardware resources, analysis of the advantages of distributed firewall regarding minimizing data transmission delays, increasing system throughput, and reducing unauthorized access risks; experimental validation of the functionality and efficiency of the distributed firewall. The results obtained indicate that the proposed method allows minimizing delays during traffic filtering and provides automatic scaling of the firewall`s functionality while maintaining the integrity of the network security system. The proposed approach provides a high level of CCM protection by segmenting the network with the assignment of a separate LXC container to serve each local subnet, which allows for targeted traffic filtering and flexible access policy management. Conclusions: the paper proposes a configuration of a distributed firewall in the Proxmox environment, including setting up a basic set of filtering rules to ensure the effective operation of a corporate computer network. The scientific novelty of the method lies in improvement of security mechanisms in scalable environments with limited hardware resources, enabling a high level of protection against external and internal threats, while maintaining fault tolerance and reliability of the network infrastructure. Experimental validation of the method's functionality and efficiency confirmed the feasibility of its implementation to ensure stable and controlled access to the corporate computer network's resources.

Keywords: method; distributed firewall; container; Proxmox; virtualization; delay; traffic filtering.

Introduction

Under the conditions of rapid development of information technologies and growth of network infrastructure, the issue of ensuring security in corporate computer networks becomes particularly relevant [1]. Modern network infrastructure is becoming increasingly scalable, which increases the risk of unauthorized access to nodes and services that require effective and continuous protection from internal and external threats.

A distributed firewall provides network traffic control, detection, and blocking of potential threats, making it an effective tool for protecting distributed infrastructure. However, the complexity and number of filtering rules directly affect network performance, security system response time, and service stability.

The use of virtualization technologies enables the creation of a flexible and scalable network infrastructure. In particular, the use of the Proxmox platform with containerization support helps to implement a managed distributed protection system, which allows this approach to be applied in conditions of limited hardware resources and high performance and security requirements.

At the same time, the growth in network load, incoming traffic volumes, threat complexity, and the number of filtering rules significantly reduces the effectiveness of traditional approaches to IT infrastructure protection [2]. This can lead to delays in information transfer and a decrease in overall system performance. Therefore, the search for practical solutions that ensure an adequate level of protection system performance in real time is a pressing task.

The use of effective optimization methods and the implementation of a distributed firewall help to achieve a balance between the level of protection, traffic processing speed, and rational use of server environment resources. Thus, improving firewall mechanisms is a key step toward increasing the reliability and stability of server infrastructure in the context of growing demands for corporate computer network protection.

Problem statement

The main directions of development the modern information society are formed in the context of dynamic IT development, which is a key factor in digital

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33) ISSN 2524-2296 (online)

transformation and the basis for the formation of effective cybersecurity systems. At the same time, corporate networks are facing the problem of creating a scalable infrastructure with a high level of information security in the case of limited computing resources [3]. IT ecosystems in the public and commercial sectors increasingly require reliable protection against internal and external threats, as well as support for high performance, given the complexity of network architecture and rising hardware costs.

The deployment and use of firewalls in modern IT environments is accompanied by a number of problems that make it difficult to ensure an adequate level of cybersecurity. In distributed environments, security policy management must be centralized, flexible, and adaptive, but the increasing complexity of corporate networks and the use of network virtualization technologies complicate traditional methods of manual security rule configuration, which can lead to errors, vulnerabilities, and lengthy configuration times [4, 5].

The growing number of IoT devices, particularly in healthcare networks, increases the risk of cyberattacks as these networks become more open and vulnerable [6]. This increases the load on traditional firewalls, which may not be able to effectively control traffic at all levels of the architecture. In addition, the use of packet filtering firewalls leads to exponential growth in the size of policy rules, which increases the likelihood of anomalies in their execution and makes it difficult to maintain a continuous level of security [7].

The economic aspects of cybersecurity also play a key role in the implementation of firewalls, as the costs of their proper configuration, management, and updating are constantly increasing. For example, financial losses from cyberattacks in the UK increased by 31% in one year, highlighting the critical need for effective protection mechanisms [8]. At the same time, environmental aspects are becoming increasingly relevant, in particular the increased energy consumption caused by the high computational complexity of manual firewall policy administration, which is particularly relevant for distributed systems [9].

Therefore, the implementation of firewalls in corporate networks requires a comprehensive approach that takes into account a number of important factors: determining the nature of potential threats, requirements for network infrastructure architecture, integration of centralized security policy management mechanisms, and ensuring the necessary level of automation for deploying and configuring firewall settings. Achieving an adequate level of corporate network protection using firewalls is possible with the implementation of automated and centralized solutions that guarantee high performance and ensure network resilience to external and internal threats.

Analysis of recent studies and publications

Current research in the field of computer networks, particularly virtualized ones, is largely focused on analyzing aspects of firewall deployment and their role in ensuring the security of such environments. Particular attention is paid to the effectiveness of network traffic filtering, security policy optimization, and research into the impact of firewalls on the performance of high-speed networks. The solutions discussed in the scientific literature draw attention to the need to increase the performance of firewalls, which can be achieved by automating the configuration of security rules, minimizing delays in the processing of network traffic, and implementing methods for dynamically scaling the network infrastructure. The importance of adapting protection mechanisms to traffic changes and increasing the number of devices in virtualized environments is emphasized separately.

According to the authors of [10], traditional firewalls play a key role in ensuring the security of modern networks, but their configuration is still mostly done manually. This creates a risk of errors, which can lead to security breaches and significant time spent on reconfiguration. In virtualization-based networks, this problem becomes even more relevant due to the increasing complexity and dynamism of the infrastructure, which makes manual administration of security rules difficult.

In addition, traditional firewalls are typically implemented as separate dedicated devices that sequentially apply security policies to each incoming packet. The authors of [11] argue that processing filtering rules can create a significantly greater load on the system than normal routing. This problem becomes particularly relevant in the context of increasing network traffic speeds, which requires constant optimization of packet filtering mechanisms. Effective configuration of security policies is critical to ensuring the performance and security of high-speed networks, especially in the context of dynamically changing threats.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

In study [12], the authors also emphasize that firewalls can become a bottleneck for network performance and a primary target for attacks, particularly denial-of-service attacks. The firewall filtering mechanism is based on checking each incoming packet against a defined set of rules to decide whether to block or forward it. The performance of such a check depends on the average number of rules that need to be processed before a decision is made. When the firewall is under heavy load, such as during peak traffic periods or DoS attacks, processing delays can increase, leading to packet loss and network performance degradation.

The introduction of virtualization and containerization technologies [13] is an effective approach to solving the problem of network infrastructure scalability. Recent research in the field of virtualization and containerization is aimed at improving the efficiency and reliability of distributed firewalls in containerized environments, such as Proxmox, in order to ensure secure access to corporate networks [14]. *Proxmox*, in particular, offers built-in tools for managing network resources, including server clustering and live migration of virtual machines [15]. This allows network infrastructure to be scaled without the need for additional investment in new equipment, which is important for small and medium-sized businesses. However, issues related to traffic processing performance and optimal resource utilization remain relevant and require new approaches.

The paper [16] analyzes the performance of architectures using one and several virtual servers on the *Proxmox VE* platform. The results of the study show that the architecture with multiple virtual servers demonstrates higher availability, specifically 80.25% with 100 concurrent users, compared to the single-server architecture, where availability is 78.4% with 80 users. The results confirm the feasibility of using scalable containerization-based solutions for the effective deployment of distributed firewalls.

Thus, an analysis of recent studies and publications [10–16] shows that scientific developments in the field of virtualized computer networks are aimed at improving security mechanisms, particularly in the context of distributed firewalls. The main problems associated with the deployment and use of firewalls are aimed at improving traffic filtering efficiency, automating security rule settings, and adapting to changing network conditions. Traditional firewalls, while playing a key role in network protection, have limitations in terms of traffic processing speed and configuration flexibility, which can lead to delays and increased system load. Virtualization and containerization technologies, such as the *Proxmox VE* platform, offer effective solutions for dynamically scaling network infrastructure and optimizing resource utilization. They contribute to increased fault tolerance, network management flexibility, and security in corporate environments. However, the issue of performance in network traffic processing remains relevant and requires further research and improvement of automated optimization methods.

Main research material

Algorithmic provision

The proposed method for improving the performance of a distributed firewall, aimed at ensuring effective monitoring and management of network traffic in corporate and virtualized networks, is based on the integration of modern virtualization technologies with mechanisms for dynamic distribution of network resources. The scientific novelty of the approach lies in the use of virtualization to build a multi-level network infrastructure with flexible segmentation and controlled access to resources, which provides an increased level of security. The implementation of continuous traffic monitoring, support for adaptive data flow management, and the ability to apply differential access policies contribute to the growth of overall network performance and ensure an adequate level of security in accordance with the requirements of modern corporate environments.

The method involves a series of sequential steps, each of which is aimed at implementing a structured and scalable approach to building a distributed traffic filtering system. Let's take a look at these steps.

1. Analyze the existing infrastructure for logical network segmentation based on the functional purpose of the nodes and the criticality of the data. This allows you to optimally determine the required initial number and placement of distributed firewall containers.

2. Deploy containers and configure routing to ensure proper interaction between segments and with the external network.

3. Configure traffic filtering policies to form a set of filtering rules, including restricting access to critical resources, allowing specific protocols and ports, and detecting anomalies.

4. Testing the distributed firewall with the initial configuration to analyze the status of the distributed firewall, delays, and evaluate resource usage for further

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

optimization or configuration adjustments to ensure the required level of throughput and system stability.

The proposed method is appropriate for use in the following conditions:

– the need for centralized security coordination and unification of access policies at all levels of the corporate network;

– increased requirements for the protection of critical corporate network resources to ensure their integrity and confidentiality;

– limited hardware resources, requiring optimization of the use of available infrastructure in view of reliability and efficiency requirements.

Thus, the implementation of the proposed method makes it possible not only to optimize the use of network resources and ensure a high level of protection, but also to create a flexible environment capable of adapting to changes in the topology of the corporate network and increased requirements for its stability.

Assessment of the developed method's effectiveness

The overall effectiveness of a distributed firewall in a corporate network is determined by its ability to minimize the number of unwanted connections, i.e., those considered potentially dangerous, as well as by reducing delays in network traffic processing. At the same time, with the increasing load on the network infrastructure, it is critical to be able to scale the firewall with minimal deployment and configuration costs.

Thus, the optimization task of organizing a distributed firewall can be formalized as the task of selecting the optimal set of configuration parameters that minimize the total traffic processing time while achieving a high level of security and scalability of the system. Formally, this task can be expressed as follows:

$$\min_{P} C(R), \tag{1}$$

where $R = \{r_1, r_2, ..., r_n\}$ – a set of filtering rules applied in a distributed firewall;

$C(R)$ – target function that reproduces the generalized costs of traffic processing, taking into account security and scalability requirements.

Accordingly, the effectiveness $E(R)$ of a distributed firewall can be presented as a function inversely proportional to the value of the target function $C(R)$:

$$E(R) = \frac{1}{\omega_1 \cdot C(R) + \omega_2 \cdot U_{CPU} + \omega_3 \cdot U_{RAM} + \omega_4 \cdot S + \omega_5 \cdot M}, \tag{2}$$

where ω_1, ω_2, ω_3, ω_4, ω_5 – weight coefficients that determine the priorities of criteria formed from the requirements and needs in the application of a distributed firewall;

U_{CPU} – level of containers' processor resources usage in the environment *Proxmox*;

U_{RAM} – RAM usage level;

S – assessment of security level, which can be defined as the number of blocked (potentially harmful) network packets;

M – scaling efficiency coefficient, which indicates the system's ability to adapt to increased load (for example, the number of successfully scaled containers without loss of performance).

The components of the optimization problem of organizing a distributed firewall (2) are presented below.

1. The total traffic processing time by the firewall $C(R)$ is a target function that reproduces the generalized traffic processing costs. Minimizing packet processing time can be achieved by automating the deployment of rules for new containers and distributing traffic across segments, which allows you to clearly build traffic filtering rules and reduce the time it takes to redirect packets to their destination. In this case, traffic processing time will be presented as

$$C(R) = T_f + T_r, \tag{3}$$

where T_f – average processing time for one packet in the firewall container, ms;

T_r – average time to redirect a packet to its destination after filtering, ms.

2. The use of processor resources U_{CPU} determines the likelihood of firewall container overload, which leads to increased packet processing time, process scheduling queues, and traffic loss during peak loads, as well as increased power consumption in conditions of limited resources. U_{CPU} is the inverse of the number of firewall containers and can be defined as follows:

$$U_{CPU} = \frac{1}{n} \sum_{i=1}^{n} \frac{P_i}{P_{\max}}, \tag{4}$$

where n – number of firewall containers;

P_i – actual processor load in the i-th container;

$P_{\max}$ – maximum allowable processor load specified by hardware resources.

3. The use of RAM U_{RAM} determines the effective management of the firewall's traffic filtering rules.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

The level of RAM usage also affects container stability and scalability. In case of insufficient memory, this can lead to containers crashing, the inability to add new filtering rules, or the refusal to deploy new firewall containers. The level of RAM usage can be calculated as

$$U_{RAM} = \frac{1}{n}\sum_{i=1}^{n}\frac{M_i}{M_{\max}}, \quad (5)$$

where n – number of firewall containers;

M_i – amount of RAM used in the i-th container;

$M_{\max}$ – maximum available memory size in the system.

4. The security S level assessment will depend on the analysis of attacks, their complexity, and the effectiveness of traffic filtering rules. The security S level assessment will be calculated as

$$S = 1 - \sum_{i=1}^{k}(p_i / c_i), \quad (6)$$

where k – number of protection levels provided by a distributed firewall;

p_i – probability of a successful attack at the i-th level;

c_i – computational complexity of conducting an attack at the i-th level.

5. The efficiency of firewall container scaling M can be estimated over a period of time for deploying a firewall container and adding a set of filtering rules to it, and can be expressed as

$$M = \frac{1}{T_d + T_c}, \quad (7)$$

where T_d – average time to deploy a new container;

T_c – average time to add a set of filtering rules to it.

The proposed approach provides a comprehensive assessment of the effectiveness of a distributed firewall implementation, taking into account security and scalability requirements. This approach is key to determining the optimal architecture and operating parameters of a distributed firewall under variable load and limited resources.

Setting up the experiment

At the initial stage, the hardware requirements for the test environment were analyzed. It showed that for productive operation of a distributed firewall, a processor with at least four cores and a maximum frequency of 2.9 GHz can be used. The amount of RAM depends on the number of connected devices and data flow. From a practical point of view, 16 GB of RAM allows you to effectively serve three containers used to deploy a distributed firewall and serve up to three segments of a corporate network that are built as separate local subnets. The availability of such hardware resources ensures the deployment of a distributed firewall in corporate networks of small and medium-sized businesses with the ability to scale segments, as well as scale distributed firewall containers. The communication channel bandwidth must be at least 1 Gbit/s. To service a distributed firewall, you need to have two network interfaces that will be used to control the firewall and traffic to corporate network segments, which is sufficient to serve users of an experimental corporate network. The hard drive where the *Proxmox* virtualization platform with a distributed firewall is deployed must have at least 500 GB of free space.

Within the experiment, all functions of the distributed firewall have been implemented, and the possibility of scaling firewall containers as the load on the corporate network increases has been provided. Figure 1 shows a generalized diagram of a distributed firewall based on LXC containers of the *Proxmox VE* virtualized environment.

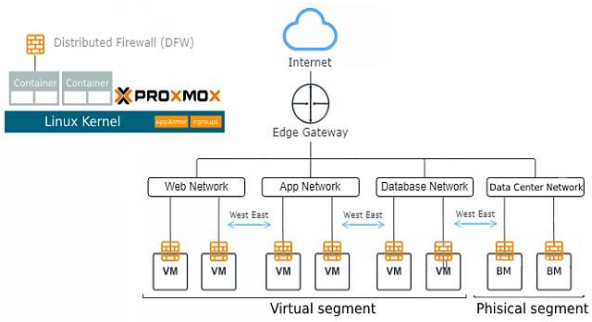

Fig. 1. Generalized diagram of a distributed firewall for a corporate network

At the initial stage, an isolated virtualized environment was created using LXC container technology within the *Proxmox VE* platform. Each container acts as a separate distributed firewall node with predefined network traffic filtering rules. Ubuntu 20.04 is installed as the base operating system in each container, providing a stable foundation for further configuration of access control policies.

The distributed firewall architecture involves the use of two types of network interfaces. The external interface with the IP address 192.168.31.50/24 provides a connection to the global Internet and is the access

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

interface to the *Proxmox VE* platform. Internal interfaces (vmbr1, vmbr2, and vmbr3) were configured for distributed firewall containers, each of which has its own IP address: 192.168.31.101/24, 192.168.31. 102/24, and 192.168.31.103/24.

To ensure isolation and increase the security level of network traffic in the corporate network, access to a separate local network served by the corresponding firewall node was configured:

– subnet 172.16.16.0/24 is served by container 101;
– subnet 172.16.17.0/24 is served by container 102;
– subnet 172.16.18.0/24 is served by container 103.

Thus, each container processes network traffic coming to the corresponding subnet, implementing the distribution and segmentation of access control policies (Fig. 2).

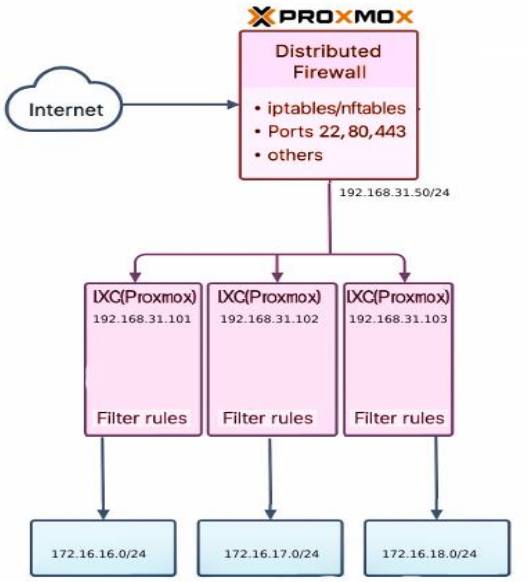

Fig. 2. Distributed firewall diagram for an experimental corporate network

In the second stage, network traffic filtering mechanisms are configured in each container using the iptables utility in accordance with defined security policies. The basic configuration of rules provides for opening ports 22/TCP (SSH), 80/TCP (HTTP), and 443/TCP (HTTPS), as well as allowing ICMP packet processing, which provides remote administrative access and supports the functioning of web services.

Filtering rules are configured using the following utility *iptables* commands:

iptables -A FORWARD -p icmp -j ACCEPT
iptables -A FORWARD -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp --dport 443 -j ACCEPT

Containerization enables rapid system scaling in case of increased request volume or more complex filtering policies, particularly when expanding the range of open ports, implementing VPN connections, or processing special network protocols. This approach allows creating additional containers without changing the underlying system architecture. In addition, it is possible to integrate automation and orchestration tools for the distributed firewall container cluster using the built-in *Proxmox VE* API.

After completing the deployment of the distributed firewall, a comprehensive check of its functionality was performed. At the initial stage of testing, ICMP diagnostics were performed from the test container to the services of the local network served by the distributed firewall, in particular to the deployed *nginx* web server. For additional diagnostics of network service availability, the *mtr* utility was used, which provides route verification and analysis of loss and delay statistics in real time (Fig. 3). Successful completion of these tests confirmed the correct configuration of the distributed firewall, the correct implementation of filtering rules, the compliance of network routes, and the availability of Internet access from each individual container. This, in turn, confirmed the reliability of the access control system in accordance with the specified security architecture.

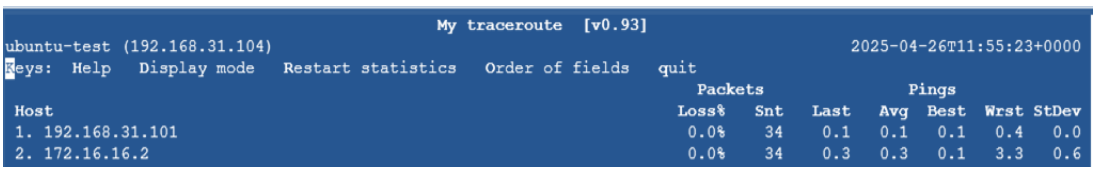

Fig. 3. Firewall test results using route checking with the utility *mtr*

Within the scope of this work, the *M/M/n* queuing model and Jackson's open network model [17] were used to model the performance of a distributed firewall. The use of these models is due to the need for quantitative analysis of the performance of the distributed firewall infrastructure in the event of increased load and complexity of traffic filtering policies.

The *M/M/n* model allows us to correctly describe the behavior of a queuing system in which incoming traffic filtering requests are sent to a limited number

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

of firewall containers that function as independent processors. Taking into account parameters such as input flow intensity, average request processing time, and the number of parallel service channels allows us to evaluate system properties such as average delay, load level, and the probability of queues. This helps to determine the minimum number of containers required to achieve a given level of performance under varying loads.

At the same time, Jackson's open network model is used to model the more complex interaction between the components of a distributed firewall. It provides the probability of describing the system as a set of nodes between which requests can circulate, replicating the structure of a real firewall with multiple modules or levels of protection, such as traffic inspection, authorization verification, threat analysis, etc. Taking into account internal traffic between containers allows us to evaluate the impact of complex multi-level security policies on overall system performance.

The combined use of the *M/M/n* and Jackson models helped to compare centralized and distributed firewall architectures and to establish optimal configurations for the container infrastructure. The simulation results showed that scaling the number of containers reduces the average request processing delay. This directly improves the efficiency of the traffic filtering system.

Thus, the dependence of firewall efficiency on the number of filtering rules, as well as on the level of scalability in conditions of increasing load and security requirements, is confirmed (Figs. 4, 5).

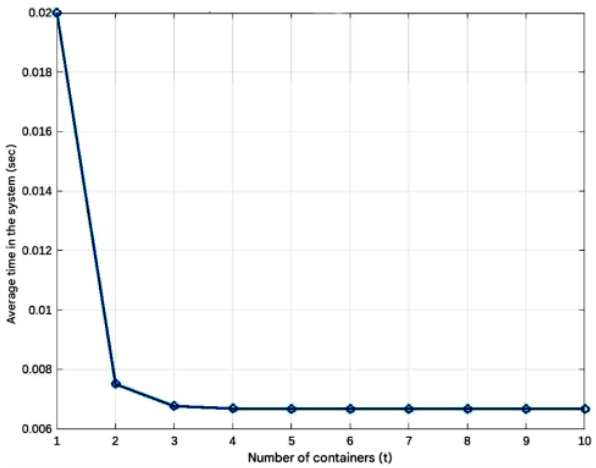

Fig. 4. Graph showing the dependence of distributed firewall efficiency on the number of containers for the open Jackson model

The experiment was conducted at the laboratory of computing systems and network technologies of the Department of Electronic Computers at Kharkiv National University of Radio Electronics.

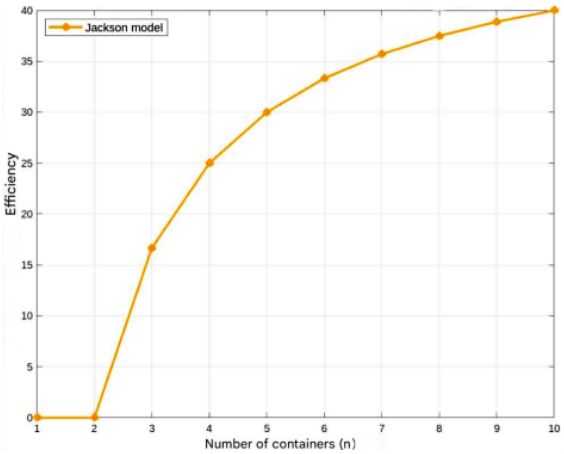

Fig. 5. Graph showing the dependence of distributed firewall efficiency on the number of containers for the *M/M/n* model

Conclusions

The article proposes and analyzes in detail a method for improving the performance of a distributed firewall in order to ensure a high level of security in virtualized environments or computer networks with scalable infrastructure. The proposed approach minimizes delays during traffic filtering and enables automatic scaling of firewall functionality while maintaining a comprehensive network security system.

The scientific novelty of the method lies in the improvement of security mechanisms in scalable environments in the case of limited hardware resources, which contributes to achieving a high level of protection against external and internal threats, while maintaining the fault tolerance and reliability of the protective infrastructure.

The results of the effectiveness analysis showed that when scaling the infrastructure, it is critically important to consider the deployment time of the protection system, as this stage can be potentially vulnerable. However, reducing delays in the scaling process allows for continuous protection, and the even distribution of the load on active infrastructure elements helps maintain its stability and efficiency.

Practical implementation of the method involves taking into account the characteristics of the transmitted information, the level of protection required, available resources, as well as filtering parameters and the number of security rules applied. The proposed approach is suitable for small and medium-sized businesses that seek

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

to ensure reliable network protection in environments with remote access and limited resource capacity, while maintaining the ability to scale and use automated configuration mechanisms.

Further research should focus on optimizing the proposed method by integrating intelligent monitoring and event processing systems, such as Prometheus and Grafana. The use of these tools will enable effective metric collection, information visualization, and rapid anomaly detection, which will help increase the response speed of the distributed firewall to potential threats.

References

1. Vazhynskyi, V. B., Tkachov, V. M. (2023), "Problematyka bezpeky ta kryterii khnadiinosti multykhmarnykh seredovyshch. Natsionalnyi universytet “Poltavska politekhnika imeni Yuriia Kondratiuka". *National University "Yuri Kondratyuk Poltava Polytechnic*", 75 p. available at: http://repositsc.nuczu.edu.ua/bitstream/123456789/19451/1/issue-galley-73%20%281%29.pdf
2. Swati, Roy, S., Singh, J., Mathew, J. (2025), "Securing IIoT systems against DDoS attacks with adaptive moving target defense strategies". *Scientific Reports*, 15(1), 9558 p. DOI: https://doi.org/10.1038/s41598-025-93138-7
3. Bytsiv, M. M. (2021), "Znachennia informatsiinykh tekhnolohii yak chynnyka innovatsii u diialnosti maloho ta serednoho biznesu", *Biznes, innovatsii, menedzhment: problemy ta perspektyvy: zbirnyk tez dopovidei II Mizhnarodnoi nauk.-prakt. konferentsii*, Natsionalnyi tekhnichnyi universytet Ukrainy «Kyivskyi politekhnichnyi instytut imeni Ihoria Sikorskoho», P. 206–207. available at: https://confmanagement-proc.kpi.ua/article/view/231790
4. Bringhenti, D., Marchetto, G., Sisto, R., Valenza, F., Yusupov, J. "Automated Firewall Configuration in Virtual Networks", *in IEEE Transactions on Dependable and Secure Computing,* Vol. 20, No. 2, P. 1559–1576, DOI: 10.1109/TDSC.2022.3160293
5. Zhurylo, O. Liashenko, O. (2024), "Arkhitektura ta systemy bezpeky IoT na osnovi tumannykh obchyslen", *Innovative Technologies and Scientific Solutions for Industries*, (1(27), P. 54–66. DOI: 10.30837/ITSSI.2024.27.054
6. Anwar, R. W., Abdullah, T., Pastore, F. (2021), "Firewall Best Practices for Securing Smart Healthcare Environment: A Review". *Applied Sciences*, 11(19), 9183 p. DOI: https://doi.org/10.3390/app11199183
7. Togay, C., Kasif, A., Catal, C., Tekinerdogan, B. (2022), "A Firewall Policy Anomaly Detection Framework for Reliable Network Security", *in IEEE Transactions on Reliability* , Vol. 71, P. 339–347, DOI: 10.1109/TR.2021.3089511
8. Kaur, H., Atif, M., Chauhan, R. (2020), "An Internet of Healthcare Things (IoHT)-Based Healthcare Monitoring System". *In Advances in Intelligent Computing and Communication; Springer*: Berlin, Germany, P. 475–482.
9. Bringhenti, D., Valenza, F. (2024), "GreenShield: Optimizing Firewall Configuration for Sustainable Networks", *in IEEE Transactions on Network and Service Management,* Vol. 21, No. 6, P. 6909–6923, DOI: 10.1109/TNSM.2024.3452150
10. Bringhenti, D., Marchetto, G., Sisto, R., Valenza, F. Yusupov, J. (2023), "Automated Firewall Configuration in Virtual Networks", *in IEEE Transactions on Dependable and Secure Computing* , Vol. 20, № 2, P. 1559–1576, DOI: 10.1109/TDSC.2022.3160293
11. Tiwari, Aman, Sivani, Papini, Hemamalini, V. (2022), "An enhanced optimization of parallel firewalls filtering rules for scalable high-speed networks". *Materials Today: Proceedings* № 62, P. 4800–4805. DOI:10.1016/j.matpr.2022.03.346
12. Sinha, M., Bera, P., Satpathy, M. (2021), "An Anomaly Free Distributed Firewall System for SDN", *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland, P. 1–8, DOI: 10.1109/CyberSA52016.2021.9478256
13. Novorodovskyi, V. (2020), "Informatsiina bezpeka Ukrainy v umovakh rosiiskoi ahresii. Society". *Document. Communication.* № 9. P. 150–179. DOI: https://doi.org/10.31470/2518-7600-2020-9-150-1179
14. Tkachov, V. M., Chepurna, I. S., Fesenko, T. H. (2024), "Metod multyrivnevoho vpn-tuneliuvannia dlia zabezpechennia viddalenoho dostupu do vuzliv ekstranet-merezhi", *Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu*. №. 3 (90). P. 299–308. DOI: https://doi.org/10.35546/kntu2078-4481.2024.3.37
15. "Proxmox VE. Proxmox VE." (2025), URL: https://pve.proxmox.com/mediawiki/index.php?title=Main_Page&oldid=12223 (last accessed: 26.04.2025)
16. Ariyanto, Y. (2023), "Single server-side and multiple virtual server-side architectures: Performance analysis on Proxmox VE for e-learning systems". *ITEGAM-JETIA*, №9(44), P. 25–34. DOI: https://doi.org/10.5935/jetia.v9i44.903
17. Ghandour, O., El Kafhali, S., Hanini, M. (2024), "Adaptive workload management in cloud computing for service level agreements compliance and resource optimization". *Computers and Electrical Engineering,* № 120, 109712 p. DOI:10.1016/j.compeleceng.2024.109712

Надійшла (Received) 25.05.2025

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

Відомості про авторів / About the Authors

Chepurna Iryna – Kharkiv National University of Radio Electronics, Assistant Lecturer at the Department of Electronic Computers, Kharkiv, Ukraine; e-mail: iryna.chepurna@nure.ua; ORCID ID: https://orcid.org/0009-0008-2442-6221
Frolov Dmytro – Postgraduate Student, Kharkiv National University of Radio Electronics, Department of Informatics, Leading Engineer at the IOC, Kharkiv, Ukraine; e-mail: dmytro.frolov@nure.ua; ORCID ID: https://orcid.org/0009-0009-3291-3561

Чепурна Ірина Сергіївна – Харківський національний університет радіоелектроніки, асистентка кафедри електронних обчислювальних машин, Харків, Україна.
Фролов Дмитро Євгенович – аспірант, Харківський національний університет радіоелектроніки, кафедра інформатики, провідний інженер ІОЦ, Харків, Україна.

МЕТОД ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ РОЗПОДІЛЕНОГО БРАНДМАУЕРА НА БАЗІ *PROXMOX* У КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Предметом дослідження в статті є метод підвищення продуктивності розподіленого брандмауера на базі LXC-контейнерів у середовищі *Proxmox VE* для корпоративних комп'ютерних мереж. **Мета роботи** – розроблення підходів до забезпечення високого рівня ефективності розподіленого брандмауера для моніторингу та управління трафіком у корпоративних і віртуалізованих мережах, що дає змогу мінімізувати затримки під час фільтрації трафіка та забезпечити надійне функціювання корпоративної мережі в умовах обмежених апаратних ресурсів. Для розв'язання завдань упроваджено такі **методи дослідження:** теоретичний аналіз літературних джерел; аналіз особливостей застосування технології контейнеризації для реалізації динамічного контролю мережного трафіка; вивчення методів підвищення ефективності застосування обчислювальних ресурсів у середовищах з обмеженими апаратними ресурсами; аналіз переваг розподіленої архітектури брандмауера щодо мінімізації затримок під час передачі інформації, підвищення пропускної здатності системи та зниження ризиків несанкційного доступу; експериментальна перевірка працездатності та ефективності розподіленого брандмауера. **Досягнуті результати.** Запропонований метод дає змогу мінімізувати затримки під час фільтрації трафіка та забезпечити автоматичне масштабування функційності брандмауера в умовах збереження цілісної системи безпеки мережі. Розроблений підхід забезпечує високий рівень захисту ККМ способом сегментації мережі з призначенням окремого контейнера LXC для обслуговування кожної локальної мережі, що допомагає здійснювати цілеспрямовану фільтрацію трафіка та гнучке управління політиками доступу. **Висновки.** У роботі запропоновано конфігурацію розподіленого брандмауера в середовищі *Proxmox* разом із налаштуванням базового набору правил фільтрації для забезпечення ефективного функціювання корпоративної комп'ютерної мережі. Наукова новизна методу полягає в удосконаленні механізмів забезпечення безпеки в масштабованих середовищах за умов обмеженості апаратних ресурсів, що дає змогу досягти захисту високого рівня від зовнішніх і внутрішніх загроз, зберігаючи водночас відмовостійкість і надійність мережної інфраструктури. Експериментальна перевірка працездатності та ефективності методу підтвердила доцільність його впровадження для забезпечення стабільного й контрольованого доступу до мережних ресурсів ККМ.

Ключові слова: метод; розподілений брандмауер; контейнер; Proxmox; віртуалізація; затримка; фільтрація трафіка.

Бібліографічні описи / Bibliographic descriptions

Чепурна І. С., Фролов Д. Є. Метод підвищення продуктивності розподіленого брандмауера на базі *Proxmox* у корпоративних комп'ютерних мережах. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 3 (33). С. 180–188. DOI: https://doi.org/10.30837/2522-9818.2025.3.180

Chepurna, I., Frolov, D. (2025), "A method for increasing the productivity of a distributed firewall based on Proxmox in corporate computer networks", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (33), P. 180–188. DOI: https://doi.org/10.30837/2522-9818.2025.3.180