УДК 004.722:004.056

METHOD OF ORGANIZING A DISTRIBUTED FIREWALL BASED ON PROXMOX CONTAINERS FOR CORPORATE COMPUTER NETWORKS

Chepurna I.S.
e-mail: iryna.chepurna@nure.ua
Kharkiv National University of Radio Electronics, Department of the EC
Kharkiv, Ukraine

The article considers ensuring a high level of security of modern corporate networks using a distributed firewall based on the Proxmox virtualization platform. The problem of filtering and monitoring traffic of a corporate computer network using containerization is studied. The emphasis is on analyzing the effectiveness of using containerization technology in Proxmox LXC to provide dynamic control of network traffic, increase firewall performance, and flexible adaptation to changes in load. The advantages of using a distributed firewall in Proxmox containers in the context of flexible management of security policies, efficient use of computing resources, and increasing the level of protection of network infrastructure are discussed.

Modern information technologies are a key driver of the development of the information society, determining the trends of digital transformation and cybersecurity. At the same time, modern corporate networks face the challenges of building a scalable infrastructure with a high level of security under conditions of limited hardware resources. In particular, models of organizing IT ecosystems in the public and commercial sectors increasingly require ensuring reliable protection against internal and external threats, as well as maintaining high performance, taking into account the growing complexity of the network infrastructure and increasing resource costs.

The solution to this problem is possible through the use of virtualization technologies in combination with containerization [1]. This approach ensures the efficient use of available hardware resources, supports remote access to network resources and contributes to the creation of a flexible, scalable and fault-tolerant network architecture. At the same time, it allows for traffic monitoring and a high level of protection of information flows.

Modern distributed firewalls can be cloud-based, hardware-based, or software-based solutions that are used to monitor and protect both physical and virtual infrastructure. Comprehensive solutions using a distributed firewall allow for unifying traffic control in corporate networks that contain both physical and virtual segments of a multi-service corporate network (Fig. 1) [2].

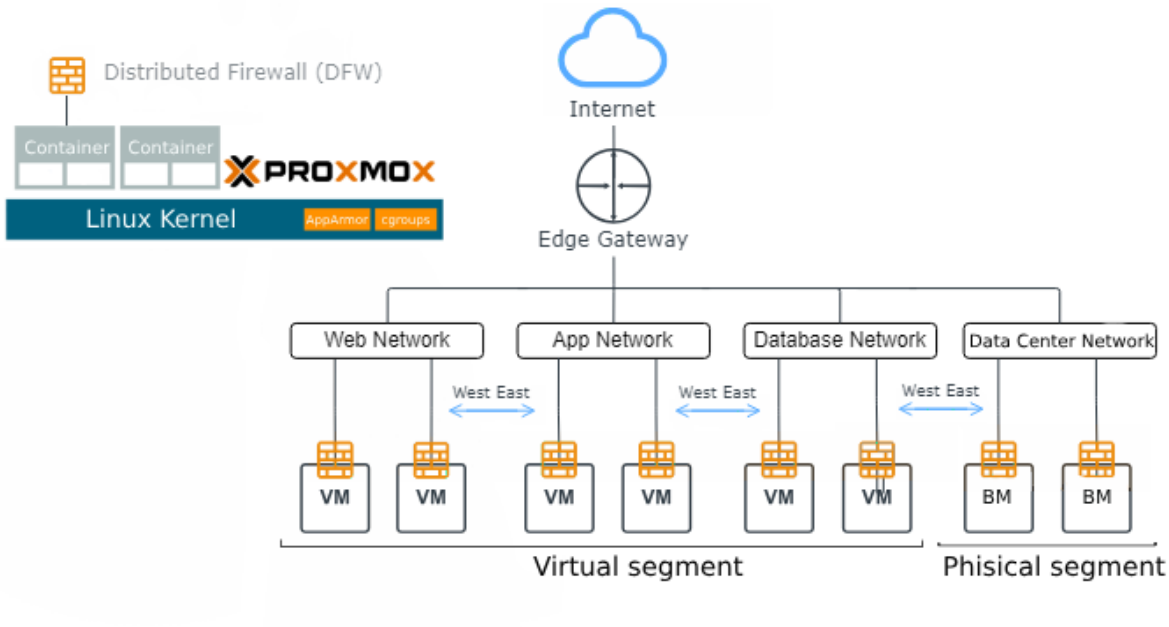

Figure 1 – Diagram of a distributed firewall based on Proxmox LXC for monitoring a multi-service corporate computer network

Despite the advantages of cloud and hardware firewalls, they also have disadvantages, including high operational and financial costs. The combination of virtualization with containerization allows you to deploy full-fledged multi-service network infrastructures that provide not only secure remote access, but also comprehensive traffic control. Such a solution can significantly reduce operational and financial costs, and is also effective in environments with limited hardware resources.

Fig. 1 shows a diagram of a distributed firewall based on Proxmox VE containers for a multi-service corporate computer network. The network architecture consists of a virtual segment, which includes virtual machines (VMs) or containers used to deploy microservices, as well as a physical segment containing physical servers (BMs) responsible for supporting the overall functionality of the network. A distributed firewall deployed in Proxmox containers is integrated with the network to control, filter, and segment traffic both between individual devices within each segment and between virtual and physical segments.

This study examines the methodology for deploying a distributed firewall based on containerization in the Proxmox VE environment. One of the containers acts as an OpenVPN server, providing secure remote access to the corporate network. Traffic filtering is implemented using iptables/nftables, which allows you to control the interaction between virtual and physical network segments. Access to the physical segment is via a virtual OpenVPN tunnel, which guarantees connection security. The VPN server functions as a secure gateway, supports certificates and private keys of common operating systems, and also implements

two-way authentication. The use of virtualization technologies allows you to effectively deploy a distributed firewall that provides access control and reduces the likelihood of unauthorized access to network resources. The use of Proxmox containers allows you to manage access to devices and resources based on defined policies, as well as scale the infrastructure by automatically adding containers in case of load growth. This approach helps reduce delays in accessing resources through defined traffic filtering rules, provides remote secure access to critical resources, rational use of hardware resources, network load balancing, and increases its fault tolerance.

The results of the research show that the use of network functions virtualization (NFV) technologies, in particular a distributed firewall, provides a high level of resource protection from external and internal threats, and also guarantees secure access to them for remote users in accordance with the requirements of reliability and information security. Further research is aimed at developing algorithms and scenarios for applying traffic monitoring and filtering policies, automating network management, and increasing the level of reliability and security in the context of multi-service corporate computer networks.

Список використаних джерел:

1. Simon, M., Huraj, L. (2023). VirtualBox and Proxmox VE in Network Management: A User-Centered Comparison for University Environments. In: Silhavy, R., Silhavy, P. (eds) Networks and Systems in Cybernetics. CSOC 2023. Lecture Notes in Networks and Systems, vol 723. Springer, Cham. https://doi.org/10.1007/978-3-031-35317-8_44

2. Arzo, Sisay Tadesse, et al. "A theoretical discussion and survey of network automation for IoT: Challenges and opportunity." IEEE Internet of Things Journal 8.15 (2021): 12021-12045.

3. Vazhynskyi, B., and V. Tkachov. "Problematyka bezpeky ta kryterii khnadiinosti multykhmarnykh seredovyshch." Systemy upravlinnia, navihatsii ta zviazku. Zbirnyk naukovykh prats 3.73 (2023): 75-78.

4. Kuchuk, N., Kovalenko, A., Tkachov, V., Rosinskiy, D., & Kuchuk, H. (2021). Predicting traffic anomalies in container virtualization. Computer And Information Systems And Technologies.