Conference name – X International scientific and practical conference «Computer integrated technologies of automation of technological processes», November 05-08, 2024, Hamburg, Germany

Section name – TECHNICAL SCIENCES

ARCHITECTURE OF ENTERPRISE SECURITY NETWORKS BASED ON SDN

Dolgova Natalya
Ph.D., Associate Professor
Department Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics
Nauki ave., 9-A, Kharkov, Ukraine, 61166
natalya.dolgova@hneu.net

Chen Zhaoxian
Master's student
Department of Information Systems
Simon Kuznets Kharkiv National University of Economics
Nauki ave., 9-A, Kharkov, Ukraine, 61166
1549813513@qq.com

Software-defined networking (SDN) is a modern network architecture that separates the control plane from the data plane, creating a centralized network management system. This system, often called a 'controller, 'is a single point of control for the entire network, managing and directing traffic and defining the rules for interaction between network devices such as switches and routers. The basic principle of SDN is that this logically centralized controller manages the network, allowing for more flexible and programmable network management and making the network adaptable to changes and business requirements. SDN offers standardized interfaces that enable the integration of various applications and security features, making it easier to monitor, automate, and modernize the network in real-time. This architecture significantly improves the visibility of network processes and enables faster incident response through global control of the entire network [1].

Modern enterprises face increasing security threats due to the widespread adoption of cloud, big data, and the Internet of Things (IoT). These technologies create dynamic and scalable networks, where the volume and variety of data, as well as the number of connected devices, can change rapidly. Traditional security measures can no longer cope with these demands. The move to SDN technologies offers centralized management that provides flexibility and adaptability, making these technologies an essential direction for enterprises [1].

One of the critical aspects is data integrity. In SDN architecture, centralized data management reduces the risks of data tampering, but maintaining security requires

robust mechanisms such as encryption and digital signatures [2]. These measures minimize threats and impose additional obligations to protect the communication channels between the control and data layers.

An important aspect is access control. Traditional networks rely on physical hardware for access control, which reduces flexibility and scalability. SDN, on the other hand, provides centralized and more precise tools to manage access rights using approaches such as role-based management (RBAC) and attribute-based management (ABAC), which allow networks to adapt to business requirements and secure critical resources.

The benefits of SDN are also related to the ability to integrate advanced threat detection systems. With a centralized SDN architecture, it is possible to monitor network activity in real-time, integrate deep packet inspection, and use machine learning techniques for anomaly analysis [1]. This enables faster detection and response to threats while minimizing human intervention.

Scalability and flexibility are essential advantages of SDN. In traditional networks, adding new devices requires significant effort, while SDN, due to its centralized management and programmability, can adapt security policies in real time. However, such changes require continuous monitoring and updating of security policies to avoid potential vulnerabilities [2].

To demonstrate a practical application, consider Company A, a large financial services provider implementing SDN to protect its data centers. Previously, the company faced challenges with scaling and rapid incident response. After implementing SDN, the architecture was centralized, allowing Company A to redirect traffic and isolate suspicious devices automatically. In one SDN case, the system automatically detected abnormal activity on one of the servers and immediately isolated it, preventing a potential data leak. This reduced the incident response time from hours to minutes and minimized potential losses.

Compliance with regulatory requirements such as GDPR and HIPAA is easier with SDN, which enables centralized management of security policies and automates data encryption and auditing processes. This simplifies regulatory compliance and reduces the risk of non-compliance penalties.

Incident response also becomes faster with the automation that is possible in SDN. Traditional networks rely on manual intervention, which increases response time to threats. SDN enables real-time isolation of infected devices and redirection of traffic to minimize damage.

Software-defined networking (SDN) has become a crucial tool for securing enterprise networks due to its ability to manage resources and flexibly control network traffic centrally.

SDN architecture for enterprise security consists of three main layers: the application, control, and data plane layers. Each layer plays a significant role in network management and interacts through standardized interfaces (e.g., OpenFlow) to ensure system flexibility and scalability [3].

Application Layer is responsible for monitoring, automatic configuration, and security policy management. It interacts with the control layer through the northbound interface (NBI), allowing the network behavior to be dynamically

adapted according to business and security requirements. This layer includes network monitoring modules and traffic management applications, such as IDS/IPS, which ensure network security.

Control Layer is the core of the SDN system. The primary component of this layer is the SDN controller, which manages and monitors network devices, providing a global view and distributing network resources. The controller interacts with both the application layer and the data plane, optimizing network performance and implementing security policies issued by the upper layer [4].

Data Plane Layer consists of physical devices (routers, switches, firewalls) that execute instructions from the controller. These devices process data flows based on rules formulated by the controller, ensuring a high degree of security and stability in data transmission.

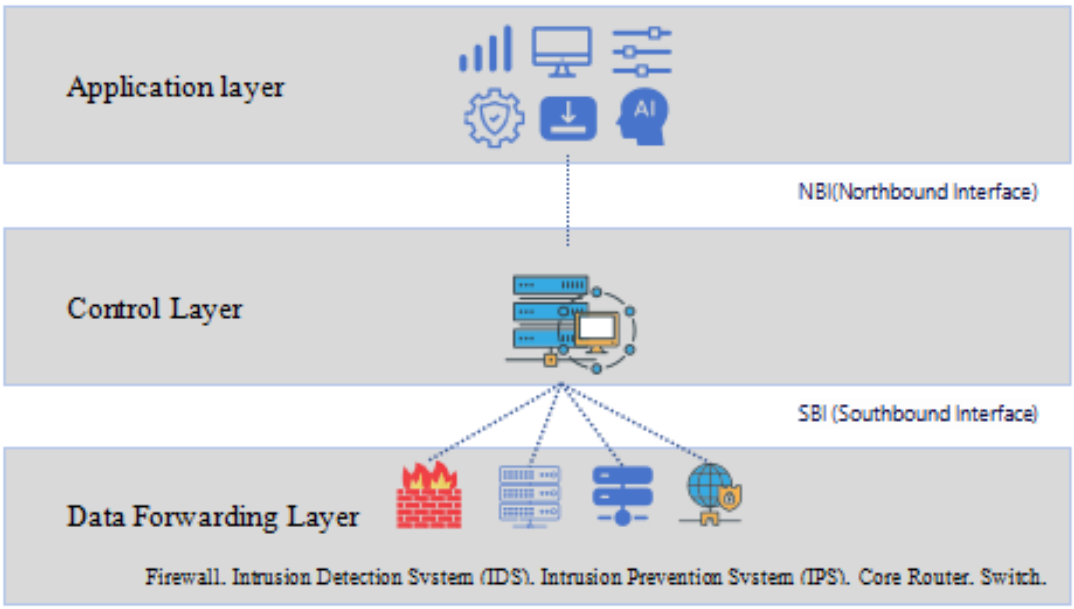

Figure 1. High-level model.

Network virtualization, a core feature of SDN, allows creating multiple isolated virtual networks on a single physical infrastructure. This significantly improves manageability and security within enterprise networks, ensuring the independence and continuity of various business processes. For instance, networks can be segmented into parts: one for external services and another for internal corporate applications. Such isolation minimizes risks, reducing the potential impact of threats on critical systems.

Security policies in SDN networks include access control, firewalls, and traffic isolation, contributing to developing a resilient and flexible security perimeter. Access control is critical in restricting interaction with network resources to authorized users and devices only. Using Role-Based Access Control (RBAC), administrators can flexibly manage permissions based on user roles and privileges.

Firewalls in SDN architecture are integrated at the controller level, enabling centralized management of traffic filtering rules and their real-time adaptation to

changing conditions and threats. Traffic isolation is achieved by segmenting data flows at the virtual network level, preventing internal interaction between different parts of the network, and protecting against threats such as DDoS attacks and ARP spoofing.

One of the critical features of SDN networks is the ability to detect and respond to threats in real-time. Integrating IDS/IPS systems with the SDN controller allows rapid threat identification and mitigation. The controller collects and analyzes data on traffic, topology, and security events, providing administrators with a global view of the network and the ability to respond immediately when threats are detected.

Threat response involves automatic policy adjustment to isolate threats and minimize damage. Thanks to centralized management and a global network view, SDN systems can effectively coordinate responses across different network segments, which would be complex and costly in traditional networks [3].

Choosing the appropriate controller is critical when designing an SDN system for enterprise security. This article examines two popular controllers: OpenDaylight and ONOS. OpenDaylight, being a fully open-source solution, offers a flexible API and a developed ecosystem, making it suitable for organizations requiring customizable and adaptable solutions. ONOS, on the other hand, focuses on modularity and supports hardware compatibility, making it advantageous for applications requiring high performance.

The choice of controller depends on the specific needs and features of an organization’s network, as well as compatibility with existing infrastructure. Consider using OpenDaylight, given its flexibility and community support, making it suitable for building a scalable and adaptable network.

An essential feature of SDN is network virtualization, which allows the creation of several logically isolated virtual networks on a single physical network infrastructure.

Each virtual network can have its own dedicated resources, policies and services, allowing flexible allocation and management of network resources while enhancing network security. The flexibility and scalability of network virtualization allow administrators to define and manage virtual networks according to specific business needs and security policies.

To meet the diverse requirements of different corporate networks, this model will create two virtual network segments: one for external service applications and one for internal corporate office applications. With the virtualization capabilities of the SDN network, these segments can be logically isolated, allowing the respective resources and security policies to operate independently without interference. As shown in Figure 2, the external service application segment and the internal corporate office application segment can be deployed on separate virtual networks. This ensures that even if enterprise service systems are compromised, the normal operation of internal enterprise applications remains unaffected. This design not only enhances system security, but also ensures the independence and continuity of each business module.

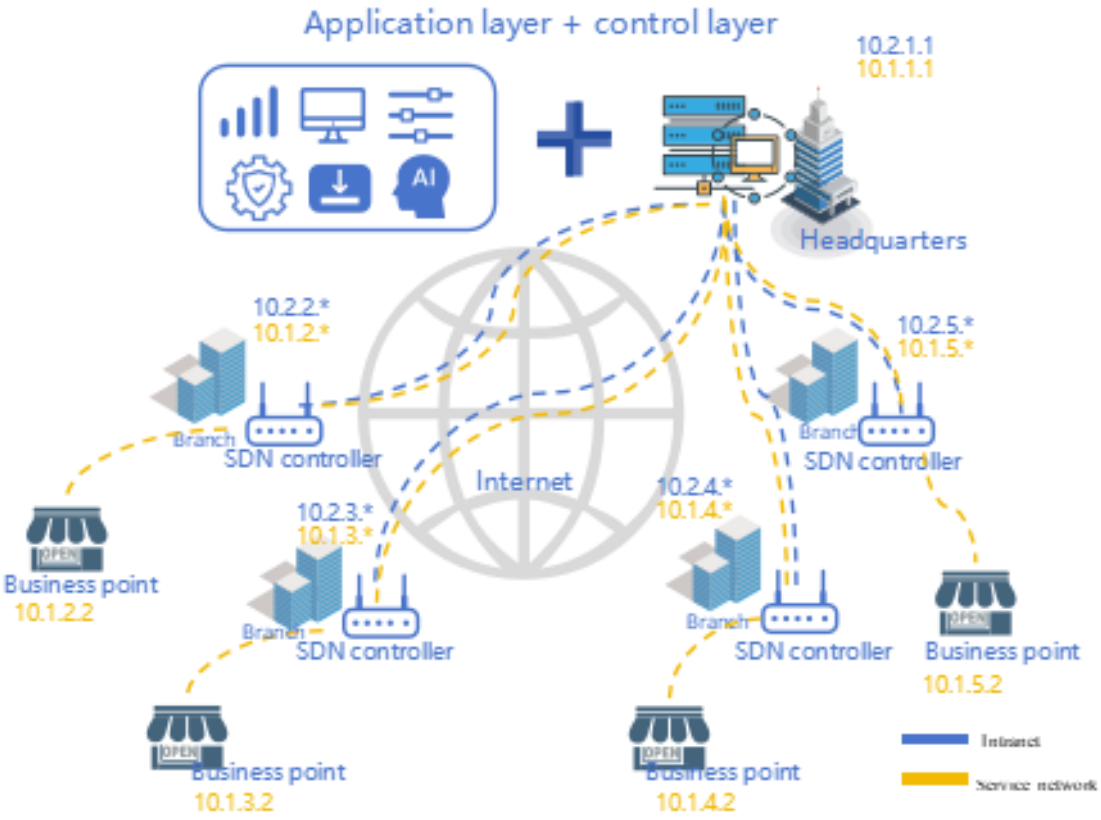

Figure 2. Virtual Network Model.

Software-defined networking technology represents a powerful tool for building flexible and reliable enterprise network security systems. SDN architecture enables the integration of modern threat detection and security management solutions, ensuring data protection and business continuity. Centralized management, real-time policy implementation, and network segmentation capabilities make SDN an indispensable tool for organizations seeking to enhance their cybersecurity posture and protect critical information systems.

References:

1. Farooq, M.S.; Riaz, S.; Alvi, A. Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review. Electronics 2023, 12, 3077. https:// doi.org/10.3390/electronics12143077

2. Derler, D., Krenn, S., Slamanig, D. Signer-Anonymous Designated-Verifier Redactable Signatures for Cloud-Based Data Sharing. In: Foresti, S., Persiano, G. (eds) Cryptology and Network Security. CANS 2016. Lecture Notes in Computer Science(), vol 10052. Springer, Cham. https://doi.org/10.1007/978-3-319-48965-0_13

3. S. Farahmandian and D. B. Hoang, "A Policy-based Interaction Protocol between Software Defined Security Controller and Virtual Security Functions," 2020 4th Cyber Security in Networking Conference (CSNet), Lausanne, Switzerland, 2020, pp. 1-8, doi: 10.1109/CSNet50428.2020.9265460

4. Abbas Javan Jafari, Abbas Rasoolzadegan, Security patterns: A systematic mapping study, Journal of Computer Languages, Volume 56, 2020, 100938, ISSN 2590-1184, https://doi.org/10.1016/j.cola.2019.100938