Ministry of Education of the Republic of Belarus
Educational institution
Belarusian State University of
Informatics and Radioelectronics

UDC 004.056.53

DO
Manh Kiem

ENTERPRISE SECURITY MANAGEMENT SYSTEM BASED ON FORTINET

Abstract
for a Master's Degree
Specialty 7-06-0611-02 Information Security

_____

Supervisor
Belousova E.S., PhD, Associate Professor

_____

Minsk 2025

INTRODUCTION

In today's complex and ever-evolving threat landscape, securing an enterprise is no longer a simple task. Organizations face a barrage of sophisticated cyberattacks targeting their networks, applications, and data. To effectively combat these threats and maintain business continuity, a robust and comprehensive enterprise security management system (ESMS) is paramount. FortiNet provide a comprehensive functional framework for the security management system. They outline a set of policies and procedural controls implemented to protect corporate assets from risks and threats, as well as include risk assessment, compliance assurance, and consulting services for security and management. This master's thesis explores the architecture and implementation of a comprehensive ESMS leveraging the power of Fortinet's integrated security solutions, specifically focusing on the synergistic deployment of FortiGate, FortiManager, and FortiAnalyzer.

The aim of this master's thesis is to develop a virtual laboratory demonstrating a corporate network model based on FortiNet for developing practical skills in configuring network equipment and testing its functionality.

For the modeling of an enterprise network with a security management system, a corporate network layout was developed on the GNS3 platform. The layout consisted of the following devices: FortiGate 6.4.12, FortiAnalyzer 6.4.12, FortiManager 6.4.12, a PC with Windows 7 OS, and Linux.

To achieve this aim, the following tasks were solved in the dissertation:

1. To research types of security management systems.
2. To design a topology of corporate network with a security management system.
3. To develop methodology for configuring hardware and software information security tools in a corporate network.
4. To perform tests on the security management system.

This master's thesis was completed independently and checked in the “Antiplagiat” system. The originality percentage is 89,27%, which meets the standard established by the Department of Information Security. References to literary sources are indicated throughout the text of the report.

GENERAL DESCRIPTION OF WORK

Work Connection with Priority Areas of Scientific Research

The topic of the thesis corresponds to paragraph 6 Ensuring the security of humans, society and the state (means of technical and cryptographic information protection, cryptology and cybersecurity) of the list of priority areas of scientific, scientific-technical and innovative activities for 2021–2025, approved by the Decree of the President of the Republic of Belarus dated 07.05. 2020 No. 156.

The aim and tasks of the work

The aim of this master's thesis is to develop a virtual laboratory demonstrating a corporate network model based on FortiNet for developing practical skills in configuring network equipment and testing its functionality.

To achieve this aim, the following tasks were solved in the dissertation:

1. To research types of security management systems.
2. To design a topology of corporate network with a security management system.
3. To develop methodology for configuring hardware and software information security tools in a corporate network.
4. To perform tests on the security management system.

Personal contribution of the author

My specific contribution lies in developing a comprehensive Enterprise Security Management System based on Fortinet technologies. I designed and implemented a robust security architecture utilizing FortiGate next-generation firewalls, FortiManager centralized management platform, and FortiAnalyzer for security analytics. My work included configuring advanced threat protection mechanisms, establishing secure network segmentation, automating security policy deployment, and creating custom monitoring dashboards to detect and respond to security incidents in real-time.

Task setting and discussion of the results were carried out together with the supervisor *PhD, Associate Professor Belousova E.S.*

Thesis Results Approbation

The main provisions and results of the dissertation work were reported and discussed at: the XX International scientific and practical conference “Information resource management” (Minsk, 29/03/2024) and the XXIII International scientific and technical conference “Technical means of information protection” (Minsk, 08/04/2025).

Author’s publications

According to the results of the research presented in the dissertation, 2 author’s works was published, including 2 articles in proceedings of the International scientific and practical conferences.

Structure and size of the work

The dissertation work consists of introduction, general description of the work, three chapters with conclusions for each chapter, conclusion, bibliography, three appendixes.

The total amount of the thesis is 65 pages, of which 65 pages of text, 63 figures on 40 pages, 10 tables on 8 pages, a list of used bibliographic sources (17 titles on 29 pages), a list of the author's publications on the subject of the thesis (4 titles on 4 pages), 3 appendixes on 4 pages, graphic material on 9 pages.

Plagiarism

An examination of the dissertation “Enterprise security management system based on FortiNet” by *Do Manh Kiem* was carried out for the correctness of the use of borrowed materials using the network resource “Antiplagiat” (access address: https://antiplagiat.ru) in the online mode 02.05.2025. As a result of the verification, the correctness of the use of borrowed materials was established (the originality of the thesis is 89,27%).

SUMMARY OF WORK

The **introduction** addresses the problems of securing enterprises in today's complex and evolving threat landscape, highlighting the necessity of a robust and comprehensive enterprise security management system (ESMS) to combat sophisticated cyberattacks and maintain business continuity. Fortinet is presented as providing a comprehensive functional framework for such a system, encompassing policies, procedural controls, risk assessment, and compliance. The general description of the work shows that the aim of this master's thesis is to develop a virtual laboratory demonstrating a corporate network model based on Fortinet solutions (specifically FortiGate, FortiManager and FortiAnalyzer) to develop practical skills in network equipment configuration and testing its functionality.

The **general description of work** shows the connection between the work and the priority areas of scientific research, the aim and tasks of the research, the personal contribution of the applicant for a scientific degree, the approbation of the dissertation results.

In the first chapter, the research on types of security management systems is presented. Various methods for corporate network security management are described, including Firewalls, VPNs, Identification and Authentication, Data Encryption, Security Monitoring and Auditing, Security Policies, Physical Security, Intrusion Detection and Prevention Systems (IDS/IPS), and Proxy Servers. The chapter analyzes the concept of an Information Security Management System (ISMS) and its core functions (Identification, Protection, Detection, Response, Recovery) within a cybersecurity framework. An overview of the security management systems market is provided, highlighting key players like FortiNet, Cisco Systems, Check Point Software Technologies, among others, with a focus on FortiNet's leadership in integrated threat management. Fortinet's approach to information security management, leveraging FortiGate for protection, FortiClient for endpoints, and FortiManager/FortiAnalyzer for centralized management, monitoring, and analysis, is detailed. The conclusion of the chapter establishes the decision to focus on firewall systems, selecting FortiNet due to its comprehensive framework and market leadership.

In the second chapter, the design of a corporate network with a security management system is described, along with the configuration methodologies. The selection process for the key components is explained: FortiGate-VM64 as the firewall, FortiManager as the centralized management system, and FortiAnalyzer as the Security Information and Event Management (SIEM) platform. The

corporate network topology modeled on GNS3, including LAN1, DMZ, LAN2 (representing an attacker segment), FortiGate, FortiManager, FortiAnalyzer, Windows 7 PC, and Kali Linux, is presented in figure 1 [1–A, 2–A].

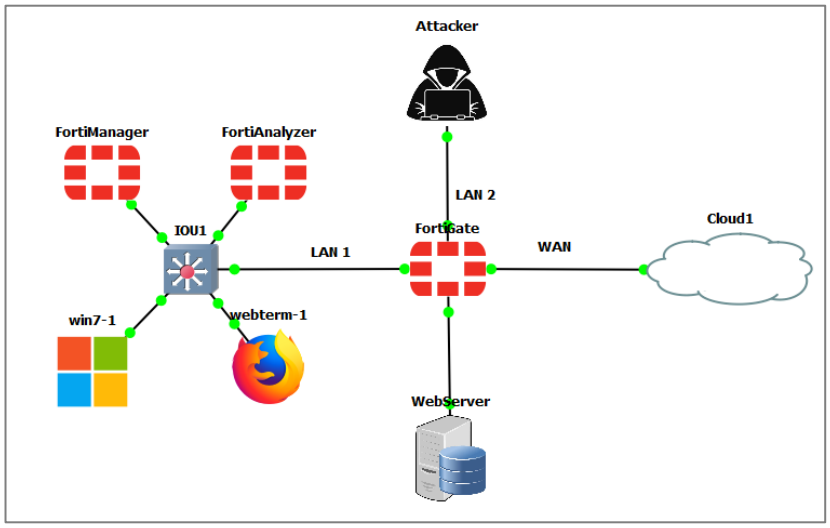

Figure 1 – Corporate network topology

Methodologies for configuring the FortiGate firewall are developed, covering access via CLI/GUI, DNS/DHCP setup, routing and security policies, establishing a Demilitarized Zone (DMZ), and implementing user. Configuration methodologies are also developed for FortiAnalyzer (connecting CLI/GUI, connecting FortiGate, setting up logging) and FortiManager (connecting CLI/GUI, connecting FortiGate, managing FortiGate policies, and synchronizing policies). Figure 2 shows the successful connection between the FortiGate and FortiManager.

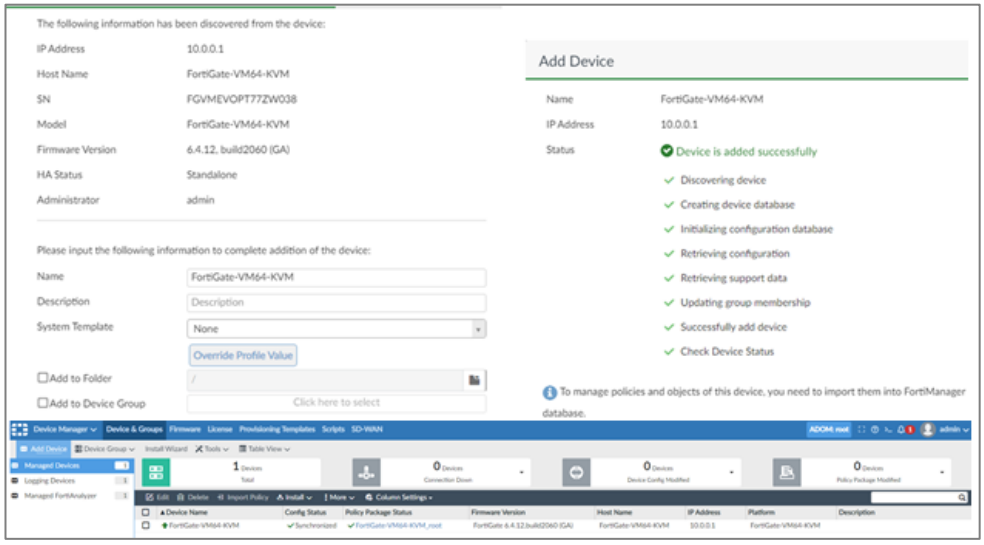

Figure 2 – Successful connection

Policy management via FortiManager includes implementing time-based restrictions, defining restrictions for websites/applications, configuring antivirus scanning, setting download size limits, configuring DLP, IPS, and DoS/DDoS protection profiles (figure 3). The conclusion highlights that the integration of these Fortinet components forms a comprehensive centralized solution and confirms the development of the necessary configuration methodologies.

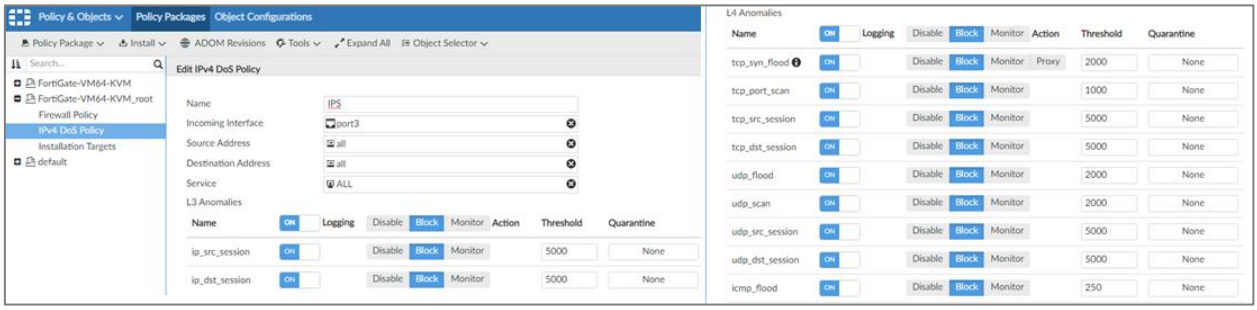

Figure 3 – IPv4 DoS Policy Configuration

In the third chapter, the testing of the security management system is presented. Tests were conducted in the developed virtual laboratory to validate the configured security policies on FortiGate 6.4.12. These tests included: attempting to access web resources during restricted times, verifying user access restrictions to websites and applications by attempting to access Facebook, attempting to download a malicious file (EICAR), attempting to download a large file (20 MB), attempting to download a PNG file blocked by the File-Filter, modeling a DoS attack (ICMP flood) using hping3, and simulating an unauthorized remote RDP connection attempt using Metasploit (figure 4). Results are presented, showing successful blocking of unauthorized access, malicious files, large files, and specific file types, as well as demonstrating protection against DoS attacks and RDP exploitation. Log entries from FortiGate and FortiAnalyzer confirming these blocked events are shown (figures 5).

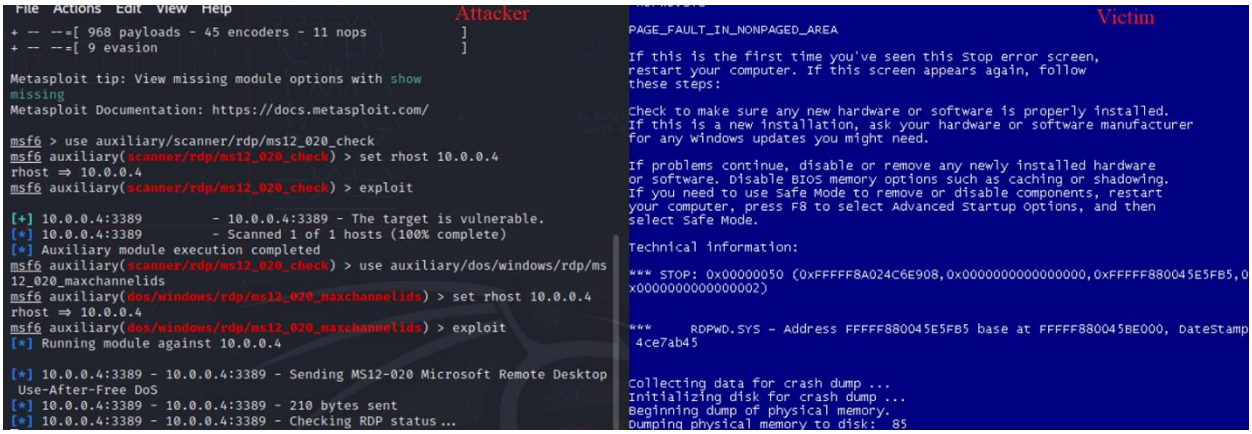

Figure 4 – Unauthorized remote connection via RDP protocol and its result

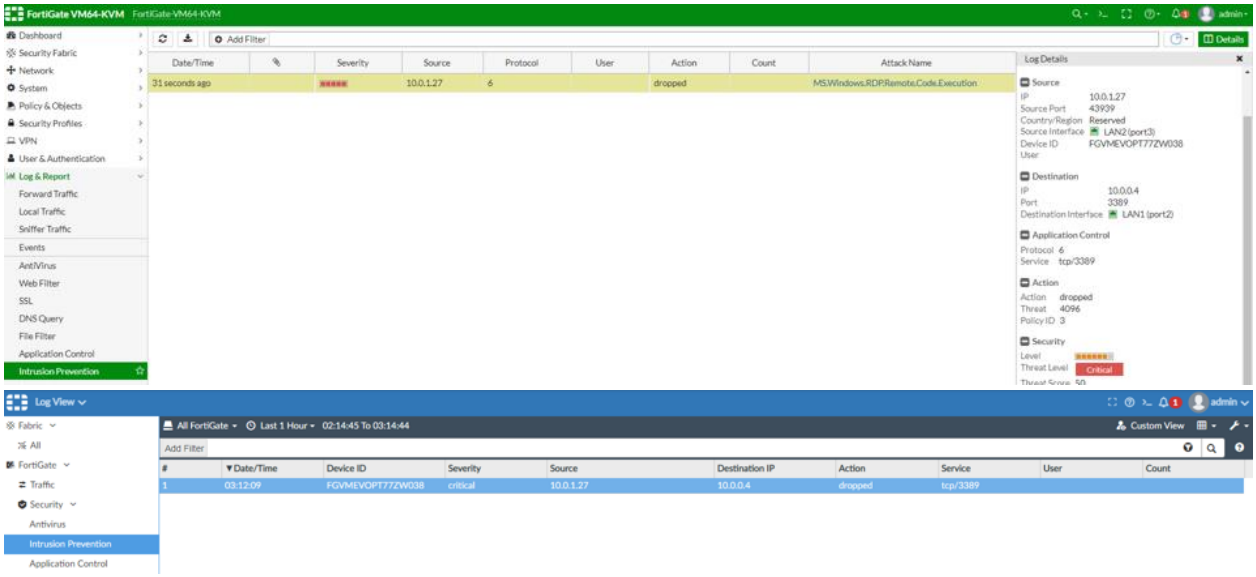

Figure 5 – Intrusion Prevention Log

The conclusion of the chapter establishes that the tests confirmed the correct functionality and effectiveness of the configured FortiGate security policies and the overall security management system. It was determined that FortiGate provides a full range of security capabilities and that the virtual laboratory effectively demonstrates this, serving as a valuable tool for practical skill development in network traffic filtering and security management.

CONCLUSION

As a result of reviewing and studying security management methods in corporate networks, it was decided to use firewall systems for managing the security of the corporate network. Based on the analysis of the global firewall market, it was found that FortiNet is one of the leaders. FortiNet products provide a comprehensive functional framework for the security management system. They outline a set of policies and procedural controls implemented to protect corporate assets from risks and threats, as well as include risk assessment, compliance assurance, and consulting services for security and management.

Based on the review and study of corporate network security management system planning methods, it can be asserted that the integration of FortiGate, FortiManager, and FortiAnalyzer into a corporate network security management system forms a comprehensive, centralized event management solution and ensures a high level of security and reliability. They are easily deployed and provide a high degree of security and reliability. Descriptions have been developed for the baseline FortiGate configuration methodology, the FortiGate policy management configuration methodology by using FortiManager, and the methodology for collecting, analyzing, and processing information security events in FortiAnalyzer. The described advantages of FortiManager and FortiAnalyzer allow to recommend them for building a corporate network security management system, both in training scenarios and in practical applications.

In a designed virtual laboratory, the security policies configured on FortiGate 6.4.12 were tested for correct functionality by: attempting to access web resources during restricted times; restricting user access to specific web resources and applications; attempting to download a malicious file; attempting to download a PNG file blocked by the File-Filter; and simulating cyberattacks such as DoS, DDoS, and unauthorized remote RDP connections. It was determined that the FortiGate firewall provides a full range of functionality (firewalling, malware protection, user authentication, web filtering, IPS/DLP, etc.). These capabilities allow it to detect attacks, malware, and other threats, as well as enable the FortiGate firewalls to block these threats. Therefore, a virtual laboratory representing a network topology segmented into LAN, DMZ, by using FortiGate, FortiManager, and FortiAnalyzer, was modeled. This virtual laboratory will allow students to improve their practical skills and knowledge in the course “Traffic Filtering in Corporate Networks”.

LIST OF OWN PUBLICATIONS

1–А. До, М.К. Обоснование выбора эмулятора GNS3 для изучения принципов построения локальных сетей с межсетевым экранированием / М.К. До, Е.С. Беллоусова // 59-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 17-21 апреля 2023 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2023. – С. 41-43.

2–А. До, М.К. Методика конфигурации и тестирования защиты от DDoS-атак на межсетевом экране FortiGate / М.К. До // Технические средства защиты информации : тезисы докладов XXI Белорусско-российской научно-технической конференции, Минск, 6 июня 2023 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол.: Т. В. Борботько [и др.]. – Минск, 2023. – С. 33.

3–А. До, М.К. Интеграция FortiManager и FortiAnalyzer в систему управления безопасностью корпоративной сети / М.К. До, Е.С. Белоусова // Управление информационными ресурсами: тезисы докладов XX Международной научно-практической конференции, Минск, 29 марта 2024 г. / Академия управления при Президенте Республики Беларусь; – Минск, 2024. – С. 260-261.

4–А. До, М.К. Система предотвращения вторжений FortiGate / М.К. До, В.К. Фунг // XXIII Международная научно-техническая конференция «Технические средства защиты информации», Минск, 8 апреля 2025 г. / Белорусский государственный университет информатики и радиоэлектроники; – Минск, 2025. – С. 141-145.