A Next-Generation Firewall Security Design for SmartSoft Vietnam

Ngô Văn Quyết
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student541@ictu.edu.vn

***Abstract*—This undergraduate thesis investigates network-security controls for SmartSoft Vietnam using a next-generation firewall. A company network needs explicit controls for traffic between local segments and external services. The author describes a simulated company network and configures FortiGate firewall functions together with port security, DHCP snooping, and Dynamic ARP Inspection. The report documents addressing, network segments, and configuration steps. The thesis presents a network model and security configuration for the chosen environment. Its conclusion treats the configuration as a useful foundation. It does not report a measured reduction in company incidents or an independently audited production rollout. Simulation and configuration evidence cannot by themselves establish resistance to all attacks. Rule maintenance, endpoint posture, monitoring, and recovery procedures would be necessary in a live enterprise. The contribution is a documented student study or prototype whose stated scope can guide further testing.**

***Index Terms*—FortiGate, firewall, network security, DHCP snooping**

I. Introduction

A company network needs explicit controls for traffic between local segments and external services. This thesis investigates network-security controls for SmartSoft Vietnam using a next-generation firewall. It begins from a practical engineering need and explains the technologies and workflow chosen for the case. The objective is to document a student implementation or comparative investigation, together with the evidence available in the manuscript. Broader operational or economic effects require separate measurements and are not assumed from the existence of a prototype [1]. Earlier ICTU student work on related designs is included here for context [2], [3], [4], [5], [6], [7], [8], [9], [10]. These contextual works were selected for this English summary; they are not asserted to appear in the original thesis bibliography.

II. Methods

The author describes a simulated company network and configures FortiGate firewall functions together with port security, DHCP snooping, and Dynamic ARP Inspection. The report documents addressing, network segments, and configuration steps. The source is summarized through its stated design, implementation material, examples, and conclusion. Features shown in the manuscript are distinguished from proposals for later development. This review does not add a new experiment, fill missing measurements with estimates, or treat a planned capability as an observed result. The source thesis remains the provenance for the reported work [1].

Supervisor: Mai Văn Hoàn, Thai Nguyen University of Information and Communication Technology (mvhoan@ictu.edu.vn).

III. Results

The thesis presents a network model and security configuration for the chosen environment. Its conclusion treats the configuration as a useful foundation. It does not report a measured reduction in company incidents or an independently audited production rollout. The report's screens, configurations, examples, or measurements constitute the evidence for this summary. A capability described only as a design intention is not counted as a validated operational outcome. No additional performance, adoption, financial, or safety figure has been introduced here. The result is interpreted within the scope of the student's documented setup [1].

IV. Discussion

Simulation and configuration evidence cannot by themselves establish resistance to all attacks. Rule maintenance, endpoint posture, monitoring, and recovery procedures would be necessary in a live enterprise. A later evaluation could test authorized and blocked traffic, log handling, rule changes, recovery, and security outcomes in a controlled operational pilot. These limitations affect how the evidence should be read. The current manuscript can support understanding of the design and reported demonstration, while independent tests would be needed for stronger claims. Any later deployment should document its environment and separate observed outcomes from intended benefits [1].

V. Conclusion

The thesis documents network-security controls for SmartSoft Vietnam using a next-generation firewall. The thesis presents a network model and security configuration for the chosen environment. Its conclusion treats the configuration as a useful foundation. It does not report a measured reduction in company incidents or an independently audited production rollout. Simulation and configuration evidence cannot by themselves establish resistance to all attacks. Rule maintenance, endpoint posture, monitoring, and recovery procedures would be necessary in a live enterprise. A later evaluation could test authorized and blocked traffic, log handling, rule

changes, recovery, and security outcomes in a controlled operational pilot. Accordingly, the present contribution is a source-grounded account of the student work and its tested or illustrated scope. Claims about broader effectiveness should be assessed in later work using explicit evaluation conditions [1].

References

[1] Ngô Văn Quyết, ”A Next-Generation Firewall Security Design for SmartSoft Vietnam,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2024.

[2] ICTU Student 129, ”Construction of a Network Security System for the Commercial Bank of Vietnam Hanoi Branch,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[3] ICTU Student 130, ”Construction of a Network Security System for a College of Education in Thai Nguyen,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[4] ICTU Student 120, ”Development of a Simulation Program for Static Packet Filtering Firewall Technology,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[5] ICTU Student 106, ”Design and Security of Wi-Fi Networks for the Tai Nguyen Software Technology Center,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[6] ICTU Student 105, ”Design of a Secure Network Using Cisco PIX Firewall for a Technical College,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[7] ICTU Student 189, ”Application of Routing and Access Control Lists in Designing a Hierarchical Network Model for the Department of Information Technology - Thai Nguyen University,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2010.

[8] ICTU Student 142, ”Construction of a Remote Access VPN System on PIX/ASA Devices for Âu Lạc Joint Stock Company,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[9] ICTU Student 98, ”Research and Development of a Virtual Private Network (VPN) System for Kraal Enterprise Co., Ltd.,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[10] ICTU Student 54, ”Design of LAN and WAN Systems for the Information and Communication Department of Phu Tho,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2008.