Research and Deployment of pfSense Firewall for Enterprises

Nguyễn Tuấn Anh
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student656@ictu.edu.vn

***Abstract*—This undergraduate thesis investigates the feasibility and practical deployment of the open-source pfSense firewall in enterprise environments, with a focus on small and medium-sized enterprises (SMEs). It begins by outlining the evolving threat landscape and the role of firewalls in mitigating network risks. The study then details the selection of pfSense, highlighting its modular architecture, NAT, DHCP, VPN, IDS/IPS (Suricata), and traffic-shaping capabilities. A virtualized testbed built on VMware is used to configure and evaluate a multi-segment network, including VPN client-to-site, alias groups, bandwidth limits, and rule sets for departmental access. The report illustrates configured rules and test screens, but it does not establish comprehensive protection or measured enterprise performance. The author notes limited data and restricts the proposed model to smaller organizations. The work concludes with recommendations for scaling the solution to larger enterprises and for future research on performance optimization.**

***Index Terms*—pfSense, firewall, network security, small and medium enterprises, VPN, IDS/IPS**

I. Introduction

Network security has become a critical concern for modern enterprises, as cyber-attacks grow in frequency and sophistication. Firewalls serve as the first line of defense, filtering traffic and enforcing access policies. This thesis examines pfSense, an open-source firewall platform, as a cost-effective alternative for SMEs. The objectives are to (1) review the theoretical foundations of network security and firewall architecture, (2) justify the choice of pfSense based on its feature set, and (3) demonstrate a practical deployment that addresses typical SME requirements such as VPN connectivity, intrusion detection, and bandwidth management [1]. Earlier ICTU student work on related designs is included here for context [2], [3], [4], [5], [6], [7], [8]. Published technical books provide background for the methods discussed in this summary [9], [10], [11]. These contextual works were selected for this English summary; they are not asserted to appear in the original thesis bibliography.

II. Methods

A VMware-based virtual environment was provisioned to emulate an enterprise network comprising multiple subnets (e.g., 192.168.100.0/24, 192.168.10.0/24, 192.168.200.0/24). pfSense was installed on a virtual machine and configured with NAT, DHCP servers, and a VPN client-to-site tunnel. Alias groups were created for IT and social-media traffic, and firewall rules were applied to enforce departmental access and block unwanted destinations. The Suricata IDS/IPS package was installed to monitor traffic, and traffic-shaping limits were set to control download/upload rates per subnet. The implementation chapter records configuration screens and examples of connection, access-blocking, and bandwidth checks in the virtual topology [1].

Supervisor: Trịnh Minh Đức, Thai Nguyen University of Information and Communication Technology (tmduc@ictu.edu.vn).

III. Results

The report shows the virtual firewall configuration, VPN connection screen, departmental access rules, Suricata settings, and bandwidth limiter examples. It includes screenshots of allowed and blocked connectivity and an alert example. These are demonstrations within the testbed, not evidence of deployment inside a real enterprise network. However, the project encountered obstacles related to the limited availability of real-world traffic data and the steep learning curve associated with pfSense's advanced features. Overall, the implementation confirmed pfSense's suitability for SME environments, though scalability considerations remain [1].

IV. Discussion

The study highlights pfSense's strengths: open-source licensing, modularity, and a rich set of features that align with SME security needs. Its ability to integrate VPN, IDS/IPS, and traffic shaping within a single appliance can consolidate configuration within one virtual appliance. The thesis does not compare costs or administrative effort empirically. Nonetheless, the solution's effectiveness is bounded by the scale of the network; larger enterprises may require additional redundancy, high-availability clustering, and more granular policy enforcement. The lack of extensive performance data also limits the ability to predict behavior under heavy load, underscoring the need for further empirical evaluation [1].

V. Conclusion

The thesis demonstrates that pfSense can be configured for a small-enterprise network model in a virtual testbed. The practical experience gained in configuring NAT, DHCP, VPN, IDS/IPS, and bandwidth limits provides a solid foundation for future work. Subsequent research should focus on optimizing pfSense performance in larger, more complex networks,

exploring high-availability configurations, and developing automated deployment scripts to streamline scaling. The project also enhanced the author's independent problem-solving and time-management skills, preparing them for advanced roles in network security [1].

References

[1] Nguyễn Tuấn Anh, "Research and Deployment of pfSense Firewall for Enterprises," internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2024.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Hoàng Đăng Huy, "A Study on Virtual Private Network and the Construction of a Site-to-Site VPN System for Thành Đạt Joint Stock Company," internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[7] 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.

[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] D. Zientara, Learn pfSense 2.4. Packt Publishing, 2018. ISBN 9781789343113.

[10] D. Zientara, Mastering pfSense, 2nd ed. Packt Publishing, 2018. ISBN 9781788993173.

[11] J. M. Stewart and D. Kinsey, Network Security, Firewalls, and VPNs, 3rd ed. Jones & Bartlett Learning, 2020. ISBN 9781284183696.