Int. j. adv. multidisc. res. stud. 2025; 5(2):889-893

Received: 01-02-2025
Accepted: 11-03-2025

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Investigate the Vulnerabilities of Internet Security Systems and find one of the Cheapest Internet Security Methods used in the Industry and how to Set it up for use by an Educational Institution

HGP Chinthaka
Assistant Lecturer, Department of Information Technology, Advanced Technological Institute, Ampara Hardy, Sri Lanka

Corresponding Author: **HGP Chinthaka**

Abstract
In the evolving landscape of cyber security, educational institutions are increasingly prioritizing the establishment of robust internet security systems to safeguard their networks and sensitive data. This paper explores the implementation of pfSense, a leading open-source firewall solution, as a cost-effective and efficient means for small educational institutions in Sri Lanka to create a comprehensive internet security framework. By leveraging pfSense's versatile features—including caching server configurations, SQUID proxy integration, IP mapping, Network Address Translation (NAT), port monitoring, and web filtering—institutions can enhance their network security and manage internet access with greater control. This study highlights the practical benefits of deploying pfSense on standard computer hardware, demonstrating its capability to meet the specific security needs of educational environments. The findings advocate for the adoption of pfSense as a vital component in the network security strategy of small educational organizations, ensuring both protection against external threats and compliance with institutional internet usage policies.

Keywords: Internet Security Systems, pfSense, Network Address Translation (NAT), Sri Lanka

1. Introduction

1.) Background and justification

The increasing dependence on internet facilities in educational institutions has created a critical need for efficient management systems to provide these resources at a low cost. This proposal outlines how to develop a robust system that enables educational institutions to administer internet facilities effectively, ensuring accessibility while minimizing expenses.

Many educational institutions have encountered significant challenges in effectively leveraging network facilities due to inadequate access to essential computer equipment and a lack of technical expertise in network administration. Despite investing in network infrastructure, the absence of the necessary hardware and skilled personnel has hindered their ability to fully utilize and manage these resources. This gap not only restricts the potential for enhancing educational experiences and facilitating digital learning but also impacts the institution's overall operational efficiency. Addressing these issues through targeted investments in technology and training can help institutions optimize their network capabilities and better support the educational needs of their students and staff.

2.) Problem statement/ study problem

Development of a Low-Cost Internet Administration Platform.

3.) Research objectives

1. Cost Efficiency
2. User Autonomy
3. Scalability
4. Security and Reliability

5. Community-Centric

2. Review of Literature

National scenario in the proposes area of research

Sri Lanka Computer Emergency readiness Team | The Coordination Center conducts policy formulation and studies on IT security and cyber security in Sri Lanka. Conducts research on cyber threats and research on potential threats. It also coordinates research on cyber security. It also provides information to government agencies in Sri Lanka on the introduction of polices on cyber security and the study and information on domain that poses a threat to cyber security.

International scenario in the proposes area of research

The most pressing issue in the IT industry nationally and internationally is how to maintain cyber security. Therefore, organizations are established internationally and introduce stand and polices regarding cyber security. The National Institute of Standards and Technology (NIST) regularly conduct tests and introduce stand-ins and polices related to cyber security. The Information Technology Laboratory (ITL), established by NIST, is constantly testing cyber security and developing new security strategies.

Also, computer virus protection companies are constantly introducing new security strategies for their software. Therefore, they are also constantly conducting research on cyber security. However, with the change of technology day by day, the threat of various types of cyber hackers is increasing. Internationally, the world today has turned into a cyber war. Therefore, many experts in the world are engaged in various studies to counter the cyber war. Due to this, new discoveries are being introduced to the world day by day.

3. Literature Review

1.) Open source security System

Open source software is a rapidly growing market because every user has access to the respective programming code, can audit what the code's functionality does and can edit the code to fit specific requirements. Open source cyber security software is in high demand in the market. But many open source security tools do not provide all the capabilities of the respective paid version in the free open-source software. Small to Mid-size enterprises will often use a combination of free and paid open source tools to improve their organization's cyber security and modify the solution to protect their digital assets and networks according to their unique business operation needs.

There are many types of free open source software available, many of which can be used for academic purposes. To study cyber security open source software can be introduced on Linux, KeePass, Metasploit Framework, Nikto, Nmap, OpenVAS, OSSEC, Security Onion, VeraCrypt and Wireshark.

2.) CISCO Network Acadamy

CISCO network academy is one of the largest computer networking knowledge providers in the world. It is a leading provider of advanced computer networking, cyber security software development and related activities. They educate their users through various courses and their products have good security features. They say that cyber security studies must work in an environment with such configurations. Then we will desperately study the security issues and the solutions to them. Their products are updated day by day, and new configurations of new products are included as a result of the studies they perform.

3.) Unified threat Management

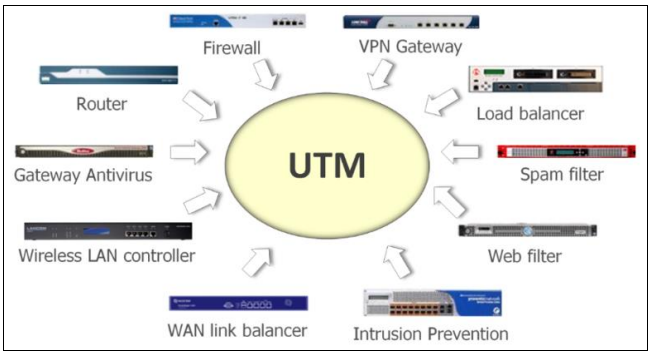

Fig 1: UTM Application Functions

IT teams are constantly faced with the challenge of protecting their companies' productivity and digital assets against evolving and sophisticated threats, including spam and phishing attacks, viruses, Trojans and spyware infected files, unapproved website access, and unapproved content. They have to address these challenges with limited budgets and resources. Having multiple separate devices, each designed to perform a specialized function such as spam filtering, web content filtering, or antivirus protection does not make this task easier. Rather, it adds to the cost and complexity of managing multiple boxes and multiple operating systems.

UTM is a single system that provides the answer to all of these challenges and more: It secures the network from viruses, malware, or malicious attachments by scanning the incoming data using Deep Packet Inspection.It prevents attacks before they enter the network by inspecting the packet headers. It prevents access to unwanted websites by installing enhanced web filtering. It provides ability to update automatically with the latest security updates, anti-virus definitions, and new features so that minimal manual intervention is required beyond initial set-up.It enables administrators to manage a wide range of security functions with a single management console.

4. Methodology

1.) Place and time period

Table 1: Place and Time

Place	Time period
In Sri Lanka	March of 2022 to February of 2025

2.) Materials

1. Two computers
2. Open source Firewall Software
3. Simulation Software
4. internet connection
5. Network Items

3.) Experimental methods

This study is structured into two distinct phases. In the initial phase, a comprehensive investigation will be carried out to assess and identify the most effective freely available

firewalls currently utilized within the industry. This evaluation will involve a systematic comparison of various firewall solutions based on key performance metrics such as security features, ease of use, and overall effectiveness in protecting systems from potential threats. Through this analysis, the study aims to provide valuable insights into the capabilities and reliability of these firewalls, ultimately guiding organizations in their selection of the most suitable security solutions.

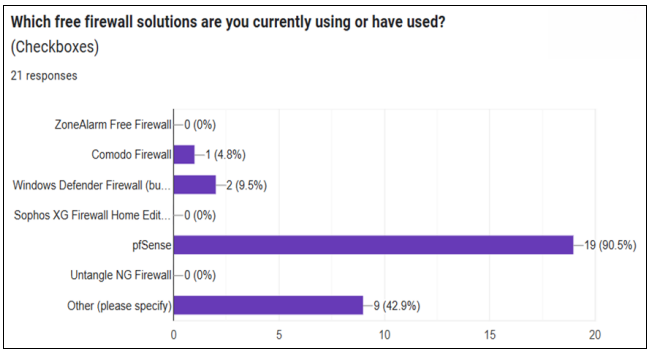

Fig 2: Pie Chart One

The data presented in Pie Chart One encapsulates a comprehensive summary derived from a recent survey focusing on the utilization of free firewalls within various sectors of the industry. The chart highlights the most commonly used free firewall solutions among respondents, providing valuable insights into current trends and preferences.

In a recent survey evaluating the popularity of various firewall solutions, six prominent options were considered: ZoneAlarm Free Firewall, Comodo Firewall, Windows Defender Firewall (integrated), Sophos XG Firewall Home Edition, pfSense, and Untangle NG Firewall. The results indicated a significant preference for pfSense, with an impressive 90.5% of respondents identifying it as their firewall of choice.

However, it's noteworthy that approximately 42.9% of users expressed concerns regarding the adequacy of pfSense as a standalone solution for safeguarding their computer networks. This indicates a prevalent belief among users that additional firewall measures are necessary to ensure comprehensive security.

These findings indicate that while pfSense is widely respected within the user community, there is an ongoing critical conversation regarding the necessity of implementing multiple layers of security to safeguard digital infrastructures effectively. Although pfSense offers robust features, it is important to note that it may not provide comprehensive protection for sensitive processes, especially those involving SSL transactions. Consequently, organizations that engage in financial transactions or manage web server communications should consider deploying additional specialized firewalls. Such multi-layered security strategies are essential to enhance overall network protection and mitigate potential vulnerabilities.

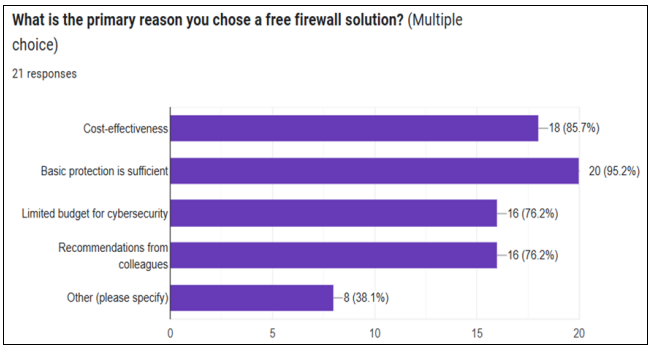

Fig 3: Pie Chart two

The tester sought a firewall solution that was both free and highly effective. To identify the most cost-effective option, several key factors were taken into consideration:

Cost-Effectiveness: The need for a budget-friendly solution was paramount, ensuring that essential cybersecurity functions could be maintained without incurring additional expenses.

Basic Protection Sufficiency: The firewall's ability to provide adequate protection for typical network threats was a critical criterion, as many organizations require only fundamental security measures.

Limited Cybersecurity Budget: Given the constraints of a limited budget for cybersecurity measures, the solution had to deliver robust functionality without financial strain.

Colleague Recommendations: Input and endorsements from peers in the industry played a significant role in the decision-making process, lending credibility to the chosen solution based on collective experiences.

Other Considerations: This category allowed for additional factors to be explored that may not have been captured in the primary criteria.

In evaluating these factors, pfSense emerged as the clear favorite, receiving over 75% positive responses across all primary criteria, indicating strong support for its effectiveness and cost efficiency as a firewall solution. However, the responses to the "Other" category were varied and less definitive, suggesting that additional unique considerations may exist that warrant further exploration.

Overall, pfSense stands out as a highly recommended firewall for organizations seeking reliable and cost-effective cyber security strategies.

4.) Sampling techniques
Non-probability sampling methods.

5.) Research design

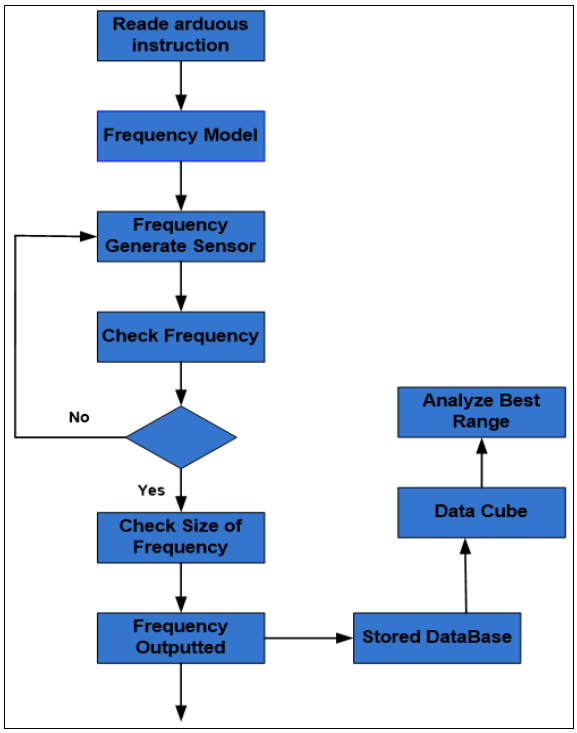

Fig 4

6.) Methods of data collection
1. Obtaining information from 21 IT workers of the industry of Sri Lanka through a Google forum.
2. Observing the results obtained by the prepared technical equipment and recording those observations.

7.) Description of data analysis
The information provided by the Google from is analyzed by a pie chart, leading to conclusions. Analyze the information obtained from the interviews, enter the information into a Microsoft excel sheet, and analyze the data. The same information can be obtained from the pie chart.'
All the information obtained from the test results is tabulated and entered into the Microsoft Excel sheets and then the mean value and standard deviation values of the data are obtained using R Studio software.

5. Result & Discussion
Result
PfSense Firewall.

Discussion
In today's digital age, safeguarding network security while managing bandwidth and content accessibility is imperative for educational institutions. Among the array of available firewall solutions, **pfSense** stands out as an exceptional choice for small educational institutions due to its robust features, cost-effectiveness, and ease of use.

6. Key Features and Benefits of pfSense
1. **Bandwidth Management:** pfSense offers comprehensive tools for bandwidth management, ensuring that the institution can efficiently allocate network resources. This capability is particularly essential in educational environments where multiple users may be accessing the internet simultaneously.
2. **Video Streaming Optimization:** With its caching configuration, pfSense allows institutions to manage video streaming effectively. By caching popular content, it minimizes latency and enhances the user experience, making it ideal for institutions offering online courses or multimedia content.
3. **Content Filtering with Squid:** pfSense integrates seamlessly with the Squid proxy server, enabling institutions to block unwanted websites and manage web access. This feature is crucial for maintaining a safe and focused learning environment, as it helps restrict access to inappropriate or distracting online content.
4. **IP Mapping:** The ability to map real IP addresses to local IP addresses facilitates easier management of network devices and services. This capability simplifies network administration and enhances the overall organization of the institution's IT infrastructure.
5. **Web Server Hosting:** pfSense can also function as a web server, allowing educational institutions to host their own websites and applications. This feature provides schools with the flexibility to develop digital resources tailored to their specific needs.
6. **Global Server Utilization:** Institutions can leverage pfSense to connect and utilize other servers globally, expanding their access to resources and services beyond their local network.
7. **Cost Considerations:** One of the most compelling advantages of pfSense is its cost-effectiveness. As an open-source solution, pfSense incurs no licensing fees. The primary investment required is in the hardware, specifically a computer and monitor capable of running the software. This presents an accessible option for small educational institutions operating on limited budgets.

7. Conclusions, Recommendations & Limitations
In conclusion, pfSense presents an impressive array of features tailored to the needs of small educational institutions. Its capabilities in bandwidth management, content filtering, video streaming management, and server hosting make it an invaluable asset. Additionally, the absence of licensing costs ensures that even institutions with modest financial resources can implement a comprehensive and effective network security solution. By choosing pfSense, educational institutions can enhance their operational efficiency while providing a secure and focused learning environment for students.

8. References
1. https://www.cisco.com. https://www.cisco.com/site/us/en/products/security/firewalls/index.html. https://www.cisco.com/site/us/en/products/security/firewalls/index.html. [Online] Cisco. [Cited: 6 12 2023.]
2. Santos Omar. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. USA: Cisco Press, 2020. 978-0135971970.

3. Electric Sheep Fencing, LLC. All Rights Reserved. pfsense.org/. https://www.pfsense.org/. [Online] Electric Sheep Fencing, LLC. All Rights Reserved., 2 1 2024. [Cited: 12 2 2024.]
4. Blokdyk Gerardus. Unified Threat Management UTM A Complete Guide, November 25, 2021. 978-0655166702.