**East African Scholars Journal of Engineering and Computer Sciences**
*Abbreviated Key Title: East African Scholars J Eng Comput Sci*
ISSN: 2617-4480 (Print) & ISSN: 2663-0346 (Online)
Published By East African Scholars Publisher, Kenya
Volume-4 | Issue-4 | May-2021 | DOI: 10.36349/easjecs.2021.v04i04.002

OPEN ACCESS

**Original Research Article**

# Portable Firewall for Data Security toward Secured Communication

Kalukhe Siddhesh Vikas Susmita[1], Kailas[2], Devasis Pradhan (IEEE Member)[3*]
[1,2]B.E Final Year Students, [3]Assistant Professor, Department of Electronics & Communication Engineering, Acharya Institute of Technology, Dr. Sarvepalli RadhaKrishnan Road, Soladevanahalli, Bengaluru -560107, India

**Article History**
Received: 06.04.2021
Accepted: 10.05.2021
Published: 16.05.2021

**Journal homepage:**
https://www.easpublisher.com

**Quick Response Code**

**Abstract:** As networked communications continue to expand and grow in complexity, the network has increasingly moved to include more forms of communication. Due to the COVID-19 outbreak an uptick in sophisticated phishing email schemes by cybercriminals has emerged. Malicious actors are posing as the Center for Disease Control and Prevention (CDC) or World Health Organization representatives. This year has seen a 600% raise in cyber-crime due to the pandemic. The fourth industrial revolution is creating an environment in which everything will be interconnected and intelligent. Internet of Things is the cornerstone of this new era. With the advent of the internet of things, privacy and security of sensitive data has become a major concern. As the tools used for an attack become more sophisticated with the use of Artificial Intelligence and Machine Learning. According to Threat post, this year has seen a 100 percent surge in IoT infections observed over wireless networks. IoT devices are now responsible for 32.72 percent of all infections observed in mobile and Wi-Fi networks – up from 64.68 percent in 2021.

**Keywords:** Fire wall; Security; IDS; Honeypot; Network; NIDS.



## INTRODUCTION

A Firewall is a Hardware and/or Software that monitors incoming and outgoing network traffic and decides whether to ALLOW OR DENY specific traffic based on the set of SECURITY RULES. Firewall have been the line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal network (INTRANET) and the untrusted outside networks. Firewall examines all the messages entering or leaving the INTRANET and block those that do not meet the specified security criteria.

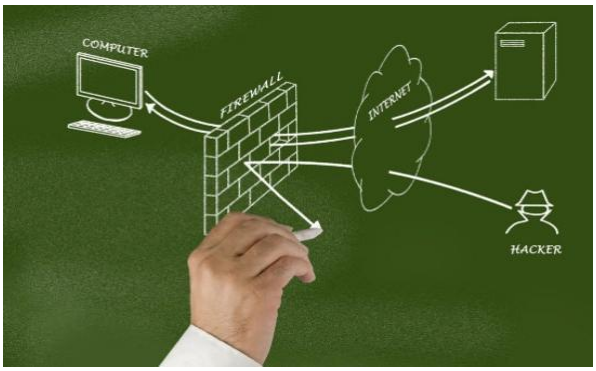


**Fig-1: Traditional Firewall**

An INTRUSION DETECTION SYSTEM (IDS) is a security software or hardware which inspects all inbound and out bound network traffic for suspicious patterns that may indicate a network or system security breach. The IDS checks traffic for that match the known intrusion patterns, and signals an alarm for when found [1-2].

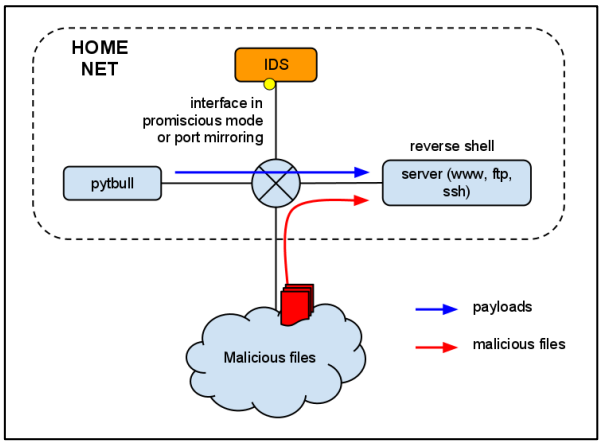


**Fig-2: Intrusion Detection System**

A HONEYPOT is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network. It has no authorized activity, does not have any production value. Any traffic to it is a probe, attack or compromise [3].

***Corresponding Author:** Devasis Pradhan

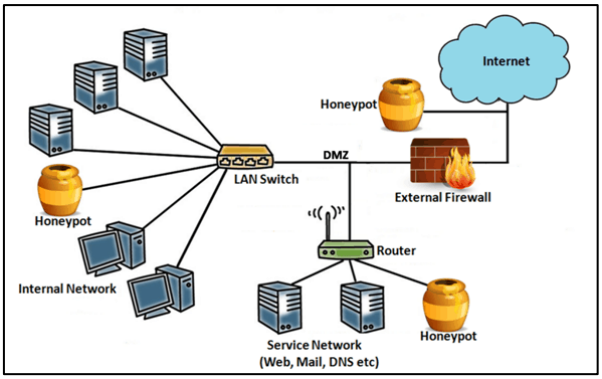


**Fig-3: Honeypot**

**Why Firewalling?**

As our networks evolve to accommodate new ways of doing business, so too must our network security. In the current world of distributed IT assets, the firewall is still central to a robust security posture. However, firewall requirements have increased significantly to protect the wide array of network infrastructures, connected devices, and operating systems from advanced threats. Consequently, our "traditional" firewall devices are being augmented by a mixture of physical and virtual appliances—some are embedded into the network while others are delivered as a service, are host-based, or are included within public cloud environments. Some are even taking on new form factors, such as clustered appliances that scale to large traffic requirements, software that runs on personal devices, SD-WAN routers, and secure Internet gateways [4-5].

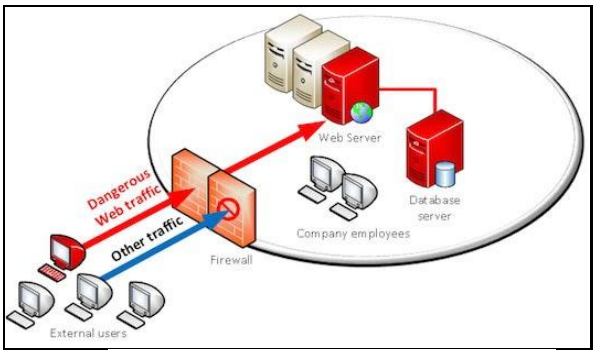


**Fig-4: Traditional network firewall approach**

The activity of sharing threat intelligence across all these disparate firewall devices, regardless of their location, is vital for uniform threat visibility and a strong security posture. To make the full shift and better secure today's networks, businesses must move away from the traditional "perimeter" approach. Instead they've got to establish strategic enforcement points across the entire network fabric, closer to the information or applications that need to be protected [6-10].

**What is Firewalling?**

Firewalling can provide an agile and integrated approach for centralizing policies, advanced security functionality, and consistent enforcement across your increasingly complex, heterogeneous networks [12-15].

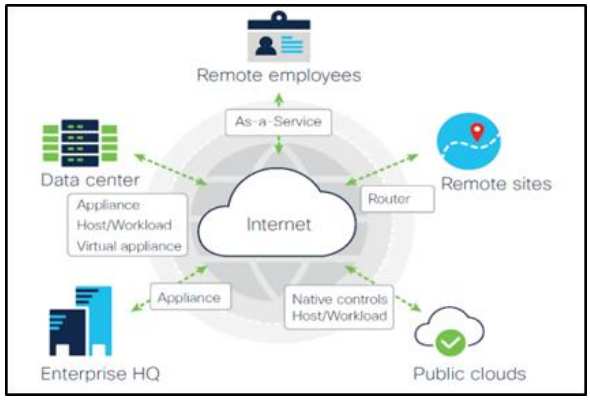


**Fig-5: The core tenants of firewalling as a means to address the security challenges of modern networks**

It should deliver comprehensive protections, visibility, policy harmonization, and stronger user and device authentication. Firewalling should also benefit from the sharing of threat intelligence across all control points to establish uniform threat visibility and control—dramatically cutting the time and effort needed to detect, investigate, and remediate threats. Enforcement points are everywhere across today's heterogeneous networks [6]. Figure 5 shows Firewalling is delivering consistent threat prevention functionality with consistent policy and threat visibility so you can prevent, detect, and stop attacks faster and more accurately, everywhere.

**Packet Filter Firewall**

Packet filtering applies a set of rules to each packet and based on outcome, decides to either forward or discard the packet. A packet filtering router should be able to filter IP packets based on information included source IP address, destination IP address, TCP/UDP source port and TCP/UDP destination port. It is used to block connections from specific hosts or networks, block connections to specific hosts or networks, block connections to specific ports and block connections from specific ports [7]. In Packet filtering IP packets are either forwarded or discarded without checking their contents. Figure 6 shows the brief idea behind the packet filtering firewall [13-16].

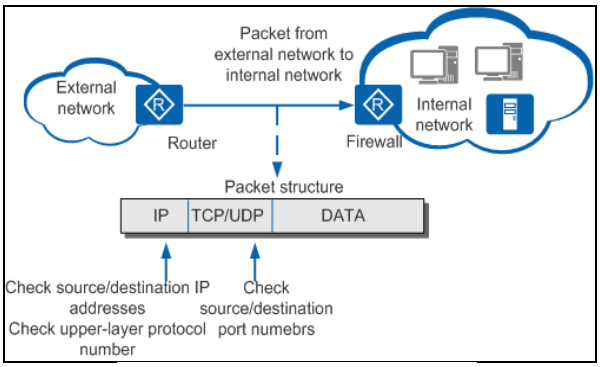


**Fig-6: Packet Filtering Firewall**.

This type of firewall allows all traffic between "trusted" hosts. All the packets that are incoming to the networks will be checked in detail by the packet filtering firewall. The firewall system checks basic information that resides in the packet such as source and destination address, source and destination port numbers, protocol and others that are related. Then, a comparison will be made between information on the packets with the rules, which had been configured on the firewall system [7-9].

**Network-Based intrusion Detection Systems (NIDS)**

These mechanisms typically consist of Black Box that is placed on the network in a promiscuous mode, listing for patterns indicative of an intrusion monitors the entire network for suspicious traffic by analysing protocol activity [8-10].

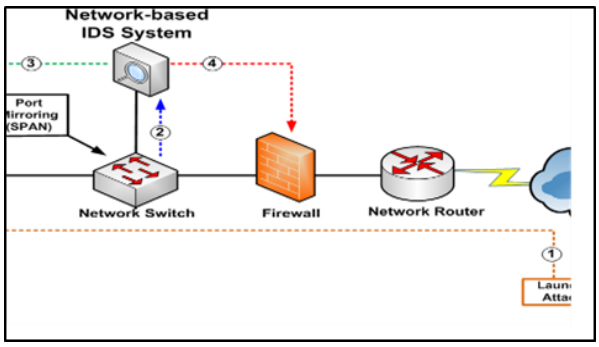


**Fig-7: Network-Based intrusion Detection Systems**

**Proposed System**

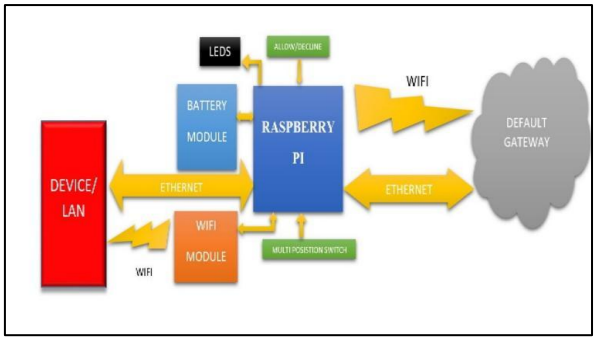


**Fig-8: Overview of Raspberry Pi based Portable Firewall**

This device has a 3000 mAh battery, Ethernet port, WIFI. It has a micro USB type-b connector for charging

The device has three configurations.

1. WIFI-WIFI
2. WIFI-ETHERNET
3. ETHERNET-WIFI

A Multi Position Switch is used to select the configuration modes.

In the WIFI-WIFI configuration, both the default gateway and the user device/LAN will be connected wirelessly. Any number of devices can be connected to the firewall in this configuration on the receiving end.

In the WIFI-ETHERNET configuration, the default gateway is connected through a wire and the client device/LAN are connected wirelessly.

In the ETHERNET-WIFI configuration, the default gateway is connected wirelessly and the client device is connected through a wire. Only one device can be connected in this configuration.

When in WIFI-WIFI and WIFI-ETHERNET configuration only way to accesses the firewall will be and rolling password generated randomly and the main administrator of the network has to manually allow each user connecting. This feature can be disabled.

## RESULTS AND DISCUSSION

This firewall is a Network-Based Firewall which will be a software appliance running on the Administrator can manually set the policies which block the other users from accessing restricted websites [17-18]. Additional to this, The Device has a pre-written rule which will block the user accessing website without a SSL certificate the device has a Network-Based Intrusion Detection System (IDS), which detects malicious activities such as DoS attacks, Port Scanning, etc. The device also has an USB port which can be connected to an external storage device which can act as a BLACK BOX.

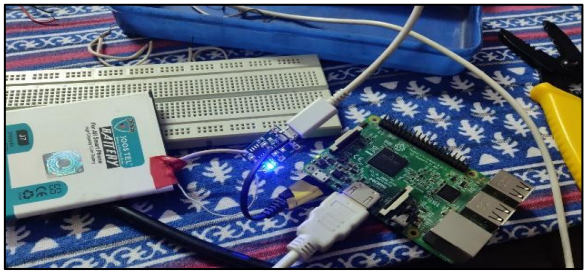

**Fig-9: Prototype of the device without the cabinet**

Intrusion Detection Tool used is SNORT. Snort uses the popular libpcap library (for UNIX/Linux) or winpcap (for Windows), the same library that tcpdump uses to perform packet sniffing. Snort's Packet Logger feature is used for debugging network traffic. Snort generates alerts according to the rules defined in configuration file.

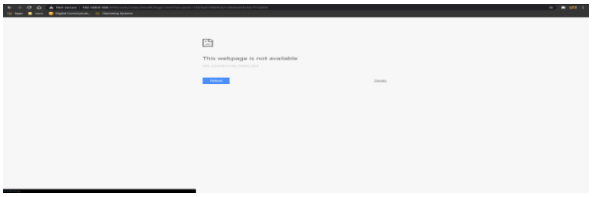

**Fig-10: Screenshot of the device trying to access insecure webpage**

An option of connecting a Honeypot to this firewall is also given. Additional to this SPECTER is also installed. SPECTOR is a smart honeypot-based IDS that offers common Internet services such as SMTP, FTP, POP3, HTTP, and TELNET. So this firewall can also act as a Honeypot in other networks. With the help of this device we can secure PAN, LAN and WLAN. Without the Firewall the user device shows up on the net discovery.

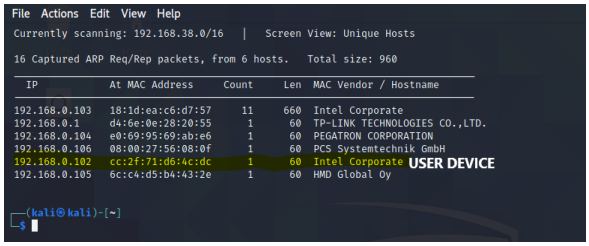


**Fig-11: User Device shows up on Net discovery**

With the Firewall the use device is hidden.

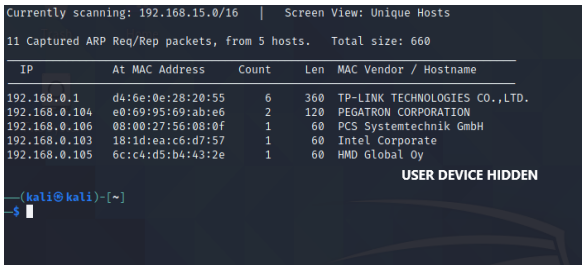


**Fig-12: User Hidden**

The device does not even show up on WIRESHARK

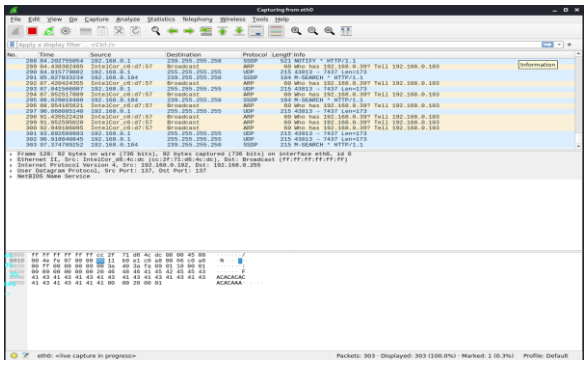

**Fig-13: WIRESHARK Snapshot**

With the rolling password feature increases security which is given only to admin of the network. The Admin can also configure a VPN on the firewall.

## CONCLUSION

Networks are very tools, they can be misused. Firewalls, though not perfect, provide a strong measure of protection for computers connected to networks. There are a number of firewall technologies to choose from, each with its own advantages. Regardless of which is selected, careful configuration is necessary. But if one have a good security policy, and a correct implementation of it, one can enjoy most of the benefits of networking, while minimizing the risks.

## REFERENCE


1. Anklesaria, F., McCahill, M., Lindner, P., Johnson, D., Torrey, D., & Albert, B. (1993). RFC1436: The Internet Gopher Protocol (a distributed document search and retrieval protocol).
2. Bellovin, S. M. (1990). Pseudo-network drivers and virtual networks. In USENIX Conf. Proc. pp. 229- 244
3. Abie, H. (2000). CORBA firewall security: increasing the security of CORBA applications. Telektronikk, 96(3), 53-64.
4. Chapman, D. B., & Zwicky, E. D. (1995). Building Internet Firewalls. O'Reilley & Associates. Inc. Sebastopol, CA.
5. Bryant, B. (1988). Designing an authentication system: a dialogue in four scenes. MIT, Project Athena.
6. Cook, D. J., Youngblood, M., Heierman, E. O., Gopalratnam, K., Rao, S., Litvin, A., & Khawaja, F. (2003, March). MavHome: An agent-based smart home. In Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.(PerCom 2003). (pp. 521-524). IEEE.
7. King, N. (2003). Smart home–a definition. Intertek Research and Testing Center, 1-6. [Online]. Available: https://goo.gl/89rRIa
8. Warroom Study.(1996). Security in Cyberspace Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate, 104th Congress, 2nd Session. ISBN 0-16-053913-7.
9. August and Xfinity. (2016). "The Safe and Smart Home: Security in the Smart Home Era. [Online] Available: http://goo.gl/UGWb5Z
10. V. Srinivasan et al. (2008). "Protecting your daily in-home activity information from a wireless snooping attack," 10th international conference on Ubiquitous computing, pp. 202-211
11. B. Ur et al. (2013). "The current state of access control for smart devices in homes," Workshop on Home Usable Privacy and Security.
12. S. Notra et al. (2014). "An experimental study of security and privacy risks with emerging household appliances," IEEE Conference on Communications and Network Security, pp. 79-84
13. V. Sivaraman et al. (2015). "Network-level security and privacy control for smart-home IoT devices," Wireless and Mobile Computing, 6 Networking and Communications, pp. 163-167.
14. T. D. P. Mendes et al. (2015). "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources," Energies, vol. 8, no. 7, pp. 7279-7311.
15. C. Debes et al. (2016). "Monitoring Activities of Daily Living in Smart Homes: Understanding human behavior," IEEE Signal Processing Magazine, vol. 33, no. 2, pp. 81-94 .

16. C. Lee et al. (2014). "Securing smart home: Technologies, security challenges, and security requirements," IEEE Conference on Communications and Network Security, pp. 67-72.
17. K. Islam et al. (2012). "Security and privacy considerations for wireless sensor networks in smart home environments," Computer Supported Cooperative Work in Design, IEEE 16th International Conference on, pp. 626- 633,
18. Bellovin, S. M., & Cheswick, W. R. (1994). Network firewalls. IEEE communications magazine, 32(9), 50-57.

**Cite This Article:** Kalukhe Siddhesh Vikas Susmita *et al* (2021). Portable Firewall for Data Security toward Secured Communication. *East African Scholars J Eng Comput Sci*, *4*(4), 41-45.