Integration of Software Router with Wi-Fi for Enhanced Security

Chaitra S. and Rinki Sharma
Department of Computer Engineering,
M.S. Ramaiah University of Applied Science,
Bangalore, India
chaitra2492@gmail.com and rinki.cs.et@msruas.ac.in

***Abstract* - The era of networking has moved from dedicated physical network devices to the abstraction of functional software component of those network devices. The functional software component can be run as a software image on any hardware platform. Routers are vital components in any networking environment which routes the information to different networks spread over a geographical area. VyOS is a software router developed by Vyatta, which provides the functionality of a router on generic hardware platform. It is identified that the Wi-Fi module is not integrated with Vyatta software router. Also, websites which use secured protocols, such as hypertext transfer protocol with security (HTTPS), are allowed by default.In this paper, these issues are identified and a suitable driver for Wi-Fi module is developed and implemented. Also, a control mechanism for secured protocols, to allow or block access to the website, is developed and implemented. Test cases are developed to block and allow specific websites. Results show that the websites are blocked successfully and the integration of the Wi-Fi module with the Vyatta software router functioned as expected.**

Keywords- ***VyOS; Vyatta; Software Router; Wi-Fi module integration; Firewall; HTTPS websites; Security; WPA; WPA II; WEP***

I. INTRODUCTION

Every organization has a well-established secured communication network which mainly consists of hardware routers and firewalls. The hardware routers and firewalls are two individual devices with unique features to provide secured network. There are diverse firewall connections which have different configurations of network. According to the needs of the organization, required firewall devices are purchased. But in case an organization needs to modify the functionality of the firewall, configuration on the existing firewall cannot be changed as it is a closed system i.e. source code cannot be altered [1]. Hence the firewall with the required modifications must be purchased again, which is not cost effective [1]. One of the disadvantages is that it requires high amount to be invested as the number of hardware devices increase, and hence lacks scalability. Investing on same type of devices might also not provide full-fledged functionalities such as security to confidential data, blocking websites, securing websites from hackers and proxy servers.

The work presented in this paper uses Vyatta software router which includes both router and firewall configurations to overcome the drawbacks of the hardware device. Running a firewall (hardware) on both router as well as computer can provide multiple lines of defense when it comes to dealing with attacks [1]. However, separate hardware devices for router and firewall lack security [2]. User credentials can be hacked as these details are not encrypted with security standards in Wi-Fi such as wired equivalent privacy (WEP), WEP II, and wireless access protocol (WAP), leading to loss of confidential information [2]. User credentials can be noted and encryption techniques can be identified by regular notice of data [3].

This paper presents the integration of Vyatta software router with Wi-Fi module and firewall device to attain high performance, scalability and security. Vyatta software along with the protocols, such as dynamic host configuration protocol (DHCP), network address translation (NAT), domain name server (DNS) and secure shell (SSH), are configured on a virtual machine workstation. Drivers for Wi-Fi are implemented on Vyatta using communication device class (CDC) / network control model (NCM) drivers. CDC/NCM driver is a generic device driver for Linux that creates a network interface on Vyatta. Netgear router and uniform resource locator (URL) filtering can block the hypertext transfer protocol (HTTP) traffic, but not the HTTPS traffic on Internet Explorer. For example, the website *http://www.facebook.com* is blocked by the URL filtering while the *https://www.facebook.com* cannot be blocked. Also, the existing software routers cannot block the HTTPS traffic while using private browsing on internet explorer [4]. There is a need to block HTTPS websites to secure confidential data across network. Aim of this paper is to enable the Wi-Fi module on Vyatta to block HTTPS websites, such as Facebook or YouTube, in order to secure the organization's confidential data and to avoid unauthorized access. Principal challenge is to enable Wi-Fi module in software router, which is not currently enabled in software routers by default [4]. This is achieved by implementing drivers on Vyatta software router and testing it on Linux platform. This paper presents the integration of Wi-Fi module with Vyatta and demonstrates the blocking of HTTPS websites.

Rest of this paper is organized as follows. Section II discusses the background theory and presents existing work on software routers, drivers and firewall configurations. In Section III implementation of Wi-Fi drivers with Vyatta software router is described. In Section IV, test cases are discussed. Section V discusses the results obtained from the test cases. Section VI concludes the paper and discusses future work.

978-1-5090-1560-3/17 $31.00 © 2017 IEEE
DOI 10.1109/IACC.2017.14

II. Related Work

Authors in [1] have identified the limitations of firewall. Transmission control protocol (TCP) relay and internet protocol (IP) address spoofing is used to hijack a browser. A visitor who types in the URL of a legitimate site is taken to a fraudulent web page created by the hijacker. The request packets from the visitor do not reach the legitimate website as a result of IP spoofing. Firewall provides protection from IP spoofing. IP spoofing can be avoided by TCP gateway for low level applications such as point-to-point communication. However, the firewall does not provide protection for IP spoofing for high level applications such as distributed communication. Different software routers, such as Bloom Bird, eXtensible Open Router Platform (XORP) and Click are discussed in [2, 3]. The authors in [2, 3] also discuss the performance metrics of open source routers. The authors in [4] discuss about how an error in a firewall policy creates security loophole that allows malicious traffic to sneak into a private network and block the legitimate traffic. The authors in [4] have observed that purchase of multiple firewalls leads to an increase in the cost and space required. Configuring multiple firewalls for only one project is not cost effective and it is more complex to analyze the performance in hardware devices. Therefore there is a need to analyze multiple firewalls and integrate the policies implemented on multiple firewalls on one software router. Required firewall policies from the integrated software router can be selected according to the need of the project. Authors in paper [5] focus on how wireless interface can be shared using virtualization technologies to host multiple virtual wireless networks on a software platform. Virtualization is used to create a new virtual system for software router Vyatta. Authors in paper [6] focus on providing hands on networking and practical experience on virtualization platform by integrating traditional physical device and virtual device. VMware server that contains all the virtual routers and virtual switches is connected to Cisco router using virtual local area network (VLAN) protocol. It is observed that integration of physical and virtual device source code cannot be altered according to user requirements as hardware routers are closed systems. From this paper it is inferred that open software router should be used to change source code in order to configure firewall policy and implement Wi-Fi module. Paper [7] conveys that using closed devices does not give security as the source code cannot be changed. Regular notice of closed system configurations allows hackers to access confidential data. Hence integration should be completely virtualized. Enhancement of security using protocols such as WPA, WPA II and WEP is discussed in [8]. Comparison of WEP, WPA, WPA II protocols and their modified versions from the application settings is based on key management [8].The authors in paper [9, 10] discuss about hardware and software routers. It is observed that software routers have twice the performance in terms of resource sharing when compared to hardware routers.

III. Design and Development

In this paper, an integrated Wi-Fi module with Vyatta software router is developed on a virtual machine workstation. This paper also analyzes whether the driver for Wi-Fi module is integrated and access on Vyatta to block the secured and non-secured websites is enabled. Design of the Vyatta software router is based on the Vyatta configurations for the DHCP, DNS, NAT and SSH protocol. The design of the Vyatta software router used in this paper is shown in Figure 1. The system is implemented using the latest version of VyOS [11] on an Intel platform with core i5 5th Generation processor, 512 MB of Random Access Memory (RAM) and 2 GB of storage.

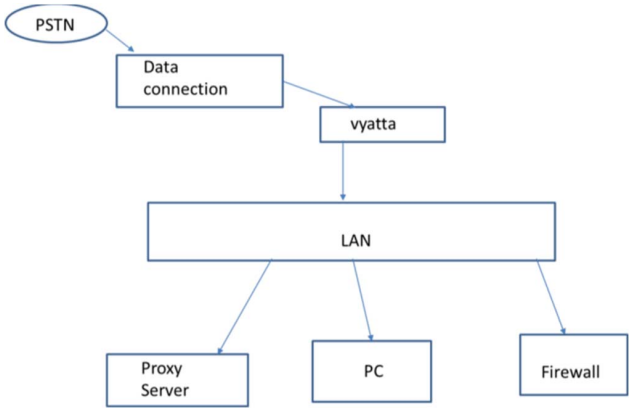

Figure 1: Design of Software Router Vyatta

Figure 1 shows Vyatta software router implemented between data connection and local area network (LAN). Public switched telephone network (PSTN) provides data connection to the routers, which is Vyatta software router in this case. There are three different devices, firewall, personal computer (PC), and a proxy server, on LAN. All these three devices are integrated with Vyatta and configured. The management of these three devices is software based and hence they can be modified according to the requirement. In Vyatta software router, all the protocols such as DHCP, NAT, SSH and DNS are configured, along with the firewall policies. Wi-Fi module drivers are implemented and integrated on Vyatta using C++ platform. DHCP dynamically assigns reusable IP address. This reduces cost and configuration effort. DNS converts domain name to IP address which goes to device and vice versa. NAT converts private and public address and vice versa. In this paper HTTPS websites are in public network while Vyatta is in private network, and thus NAT is configured. Vyatta is integrated with Linux based platform, running Debian Jessie operating system [12], in order to test the WiFi module.

Vyatta is implemented using image-based installation method. It does not alter files while booting the operating system. Each Vyatta release is self-contained within a directory on the selected storage device. It allows multiple images to be installed on the same system, such as firewall,

providing a predictable environment upon boot, and allows for a quick upgrade to a new release of Vyatta software router.

Debian Jessie Linux operating system is installed on virtual work station. Vyatta router is integrated with Debian operating system and is checked for the functionality. Vyatta supports all its packages only on Debian Squeeze version. Hence the installed Debian Jessie is downgraded manually to Squeeze version using Cow builder which is a base image. Base image is an old stable Squeeze distribution which runs in the background.

IV. Test Cases

This section discusses the unit testing of the developed and implemented Vyatta software router. The testing is carried out on the integrated Wi-Fi module with Vyatta on debian Jessie, with the aid of test cases developed. The obtained test outcomes are studied and compared with the expected results. The test cases are developed based on the following motives:

- Testing if Vyatta software router is able to enable USB and exchange data.
- Testing if Vyatta is able to block sites.
- Testing if Vyatta is able to block sites using keywords.

Test case 1 - Testing drivers implemented on Vyatta:
To test if USB is enabled on Vyatta and the Wi-Fi module drivers are implemented successfully. The outcome of test case 1 is shown in Figure 2.

Test case 2 - Integration of Vyatta and OS Debian Jessie:
To check whether the data is enabled on Linux based Debian Jessie in order to access websites and also to test for blocking the websites.

Test case 3 - Denying access using keywords and block category:
To test whether websites are blocked based on the keyword. If any keyword is added to the blocked list then the website with that keyword in the URL will be blocked. For example, in Figure 4, 'Yahoo' keyword is blocked, due to which 'Yahoo' based news and 'Yahoo' account are blocked as shown in Figure 6. In block category, job search is blocked, due to which all job search related websites like *naukri.com*, *shine.com* etc. are blocked.

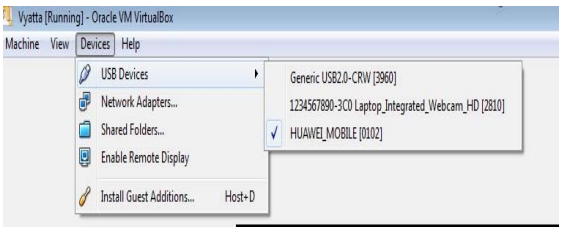

Figure 2: Enabling of USB

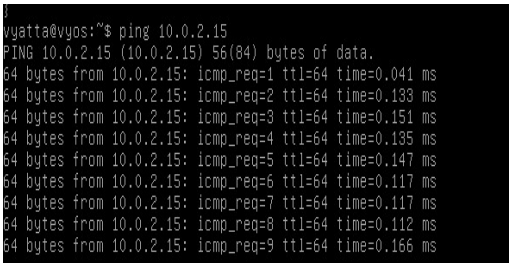

Figure 3: Driver is implemented and pinging to IP 10.0.2.15

Figure 2 shows the results of Test case 1 where drivers are implemented successfully, due to which USB named as HUAWEI_MOBILE (0102) is enabled, and in turn the internet can be accessed. The connectivity is checked by using the ping command on driver's IP address which is 10.10.2.15. Figure 3 shows the result of the ping command which is successful.

V. Results and Discussions

The Wi-Fi module is successfully integrated with Vyatta, and the functionality of the same is verified. The websites are successfully blocked and the connectivity to the websites is tested before and after enabling the block code on Vyatta. Figure 4 shows the code to blocked websites based on category, secured websites and keyword.

```
        cache-size 100
        default-port 3128
        listen-address 10.0.2.15 {
            disable-transparent
            port 3128
        }
        url-filtering {
            squidguard {
                allow-ipaddr-url
                auto-update {
                    update-hour 0
                }
                block-category adult
                block-category audio-video
                block-category jobsearch
                block-category shopping
                default-action allow
                local-block facebook.com
                local-block yahoo.in
                local-block oneindia.in
                local-block rediff.com
                local-block news.yahoo.com
                local-block yahoo.com
                local-block-keyword in.yahoo.com
```

Figure 4: Code to Block Websites

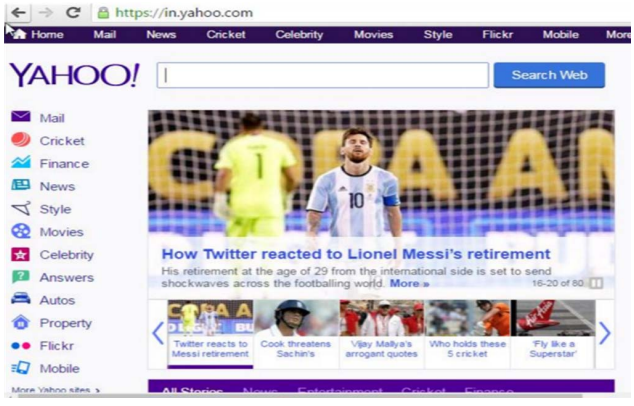

Figure 5: Before Blocking

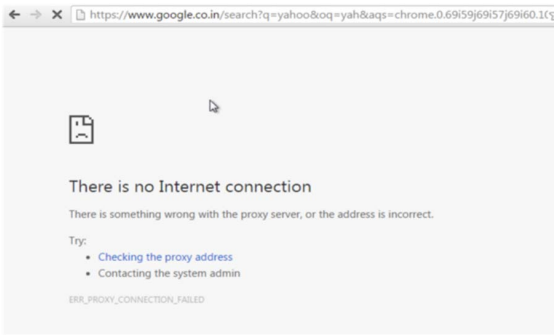

Figure 6: After Blocking

Figures 5 and 6 show the connectivity to the website before and after adding the website to the blocked list. The test cases developed using Vyatta software router satisfy the design specifications and the outcome of the test cases is on par with the expected results.

VI. Conclusion and Future Work

Cloning of Vyatta on Debian Jessie and integration of Wi-Fi module with Vyatta is carried out successfully. The security of Vyatta is enhanced, on both wired and wireless networks, by enabling the feature of blocking websites based on keywords. It reduces the cost since it is an open source system software router. Multiple websites can be blocked simultaneously, and hence it is scalable. From the test cases and the results, it is evident that the developed Vyatta software router performs better than the other hardware routers. Allowing users to change the required firewall policies and block the websites can lead to better results. In future, elaborate testing can be carried out to study energy efficiency of the router.

VII. Acknowledgement

Authors thank Mr. Shravan Tateneni from Skylux Telelink Pvt. Ltd., Bangalore for their suggestions and support in successful completion of this work.

References

[1] Deb, S.S. and Munro, A., (2007) October. Closing the Loop for Dynamic IP QoS Provisioning: A Case Study. In *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on* (pp. 368-375). IEEE.

[2] Digikey.com, (2011). Security Issues with WiFi Bluetooth and ZigBeeDigiKey.

[3] Guillen, E., Sossa, A.M. and Estupiñán, E.P., (2012) Performance Analysis over Software Router vs. Hardware Router: A Practical Approach. In *Proceedings of the World Congress on Engineering and Computer Science* (Vol. 2, pp. 24-26).

[4] Liu, A.X. and Gouda, M.G., (2008) Diverse firewall design. *Parallel and Distributed Systems, IEEE Transactions on*, *19*(9), pp.1237-1251

[5] Lee, B. and Jeon, J. (2006). An Embedded Router for Internet Communication Among Private Networks. *2006 IEEE International Conference on Industrial Technology*

[6] Peng, H., (2012) April. WIFI network Information security analysis research. In 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet, April (pp. 21-23)

[7] Ukil, A., Sen, J. and Koilakonda, S. (2011). Embedded security for Internet of Things. *2011 2nd National Conference on Emerging Trends and Applications in Computer Science*

[8] Zhong, H. and Xiao, J., 2014, June. Design for integrated WiFi defence strategy in mordern enterprise context. In *Software Engineering and Service Science (ICSESS), 2014 5th IEEE International Conference on* (pp. 748-753). IEEE

[9] Aljabari, G. and Eren, E., (2011) Virtual WLAN: extension of wireless networking into virtualized environments. *International Journal of Computing*,*10*(4), pp.322-329.

[10] Babar, S., Stango, A., Prasad, N., Sen, J. and Prasad, R. (2011). Proposed embedded security framework for Internet of Things (IoT). *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronic Systems Technology (Wireless VITAE)*.

[11] *Index of /software/vyos/iso/release/1.1.7*. (2016). *Mirror.vyos.net*. Retrieved 10 August 2016, from http://mirror.vyos.net/iso/release/1.1.7

[12] *Ftp.debian.org*. Retrieved 8 August 2016, from http://ftp.debian.org/debian/dists/jessie/main/installeramd64/current/images/netboot/mini.iso

[13] Bahrambeigy, B., Ahmadi, M. and Fazlali, M., (2014) May. BloomBird: A scalable open source router based on Bloom filter. In *Electrical Engineering (ICEE), 2014 22nd Iranian Conference on* (pp. 980-985). IEEE.

[14] Chan, K.C. and Martin, M., 2012, July. An integrated virtual and physical network infrastructure for a networking laboratory. In *Computer Science & Education (ICCSE), 2012 7th International Conference on* (pp. 1433-1436). IEEE.

[15] Yu, R., Xue, G., Kilari, V. T., & Zhang, X. (2015). Network function virtualization in the multi-tenant cloud. *IEEE Network*, *29*(3), 42-47.

[16] Riggio, R., Rasheed, T., & Narayanan, R. (2015, May). Virtual network functions orchestration in enterprise wlans. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 1220-1225). IEEE.

[17] Han, B., Gopalakrishnan, V., Ji, L., & Lee, S. (2015). Network function virtualization: Challenges and opportunities for innovations. *IEEE Communications Magazine*, *53*(2), 90-97.