ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Developed Secure Network Model Using Radius Server

John Samuel Ndueso, Ndujuiba Charles, Okonigene Robert, Udensi Amaogechukwu Nwamara
Department of Electrical and Information Engineering, Covenant University, Ota, Ogun State, Nigeria
Department of Electrical and Information Engineering, Covenant University, Ota, Ogun State, Nigeria
Department of Electrical and Electronics Engineering, Ambrose Alli University, Ekpoma, Edo State, Nigeria
Department of Electrical and Information Engineering, Covenant University, Ota, Ogun State, Nigeria

Abstract: ***History of networks dates back to the early 1970's and due to the emerging ding demands placed on networks by administrators and users, securing the network becomes a necessity. In this research work we studied the various existing methods employed in securing private networks and came up with using radius server as a backbone to network security. A dedicated network was designed and the administrative and client networks on virtual LAN (VLAN) basis configured. This ultimately authenticates a valid user and rejects an invalid user from gaining access into the network using the method of authentication, authorization and accounting (AAA), while monitoring the valid user and keeping record of activities on the network.***

***Index Terms*—Accounting Authentication Authorization, Radius Server, Network Monitoring, Network Security.**

I. INTRODUCTION

Network security is all about creating an environment where users of a particular network or the internet are able to exchange and retrieve secured data. With the introduction of internet, security has been a major challenge and therefore highlighting its history is very essential to give a better understanding of networks and means of securing them. Interest in network security was driven by the crime committed by Kevin Mitnick in the USA. It was recorded as the largest computer related crime in the history of USA. After then, more focus was placed on securing a network either private or public. Public networks are mostly used in the transfer of information. Therefore due to evolving need for information privacy necessitated the need for advance security [1]. Internet protocols in the past were built with less security, thereby keeping them open to attacks. For instance, the TCP/IP stack has no security measures or protocols implemented in them. But in recent times, it was observed that developments in computer architecture has provided for security protocols given rise to the emergence of the next generation network (IPsec) with embedded security. We studied network security and observed that the internet was a driving force for the improvement of data security. Most network-based applications and services stand out as security risks to both individual and corporate bodies. The desire to get connected to the internet comes with the need to adequately secure the network [2]. Network security is the process by which information is protected and its main goal is to provide confidentiality, maintain integrity, and assure availability of data. Hence, it is essential that all networks should be protected from vulnerabilities and threats in order for a business to achieve its full potential. These vulnerabilities can arise from wrongly configured hardware or software, poor network design, technology weakness or user carelessness. Careful management and monitoring of network can help prevent attack, decrease network threats and aid in the analysis of suspected security breaches [3].

II. NETWORK SECURITY AND PROTECTION

The main target of developing security is to protect. Hence, every administrator tends to be focused on the protection of data within the network. As e-business and internet applications increases, finding the balance between being isolated and open becomes necessary. With increased number of LANS, and personal computers, the internet creates a lot of security risks giving rise to the advent of firewalls to prevent and isolate computer systems from intruders. These devices are hardware or software that enforce and access control policy between two or more networks. Firewall finally gave businesses a balance between security and simple outbound access to the internet. Network security is the most essential component in information security because it is

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

responsible for securing all information passed through computers in any network [4, 5]. Real-world security involves prevention, detection and response. Without detection and response, preventive mechanisms would be limited in value. On the internet, it can be said to be monitoring. In protecting a network, there are many preventive techniques to secure networks against threats. Protecting a network first begins with the physical layer of the network to ensure that all connections are adequately and appropriately placed with the correct wiring [6, 7]. In network security, we discuss in details, threats, attacks and vulnerability of networks and how to effectively overcome them. The weaknesses can be traced to devices such as routers, switches, desktops, servers and any hardware involved in the network process. Weaknesses may arise from the technology, configuration applied or security-policy in use [8, 9]. Though in ensuring appropriate security, it must be observed and noted that no network is 100% secure or cannot be absolutely safe from hackers or network surfer spooler.

III. MATERIALS AND METHODS

Ubuntu is a computer operating system based on Linux distribution and used as free open source software with its own desktop environment. In this work, the server edition of the operating system was used. Fig 1 shows the flow diagram for the authentication process. To adequately secure the network, the dedicated Ubuntu server was setup using two network interface cards (NIC) to support the client and administrator (admin) networks separately. Cisco catalyst 2950 switch was used to manage all Ethernet ports and VLANS within the network and server. A wireless router (TP link) was also used to route the wireless network for clients willing to connect via wireless. The radius server used was microtik hotspot with embedded Linux, Apache, MySQL and PHP (LAMP). It houses the authentication, authorization and accounting (AAA) aspect of the security. Also a firewall (PFSense) was used to filter, monitor and protect the network from internet prone attacks; this gives the permission of various security options and backup plans such as LAN/WAN failover, load balancing etc. The idea was to create a secured network with minimal cost implication, and based on this, the firewall and the radius server were virtually installed on the server using VMware Vsphere Client. The network interface card 1 (eth0) is the admin interface while network interface card 2 (eth1) stands as the client interface. This was done in a way as to prevent the client from easy access to the work of the admin. The hardware cabling was implemented using RJ45, Ethernet straight through cables, as shown in Fig 2. The connections were made from server to switch and router and host (admin) system.

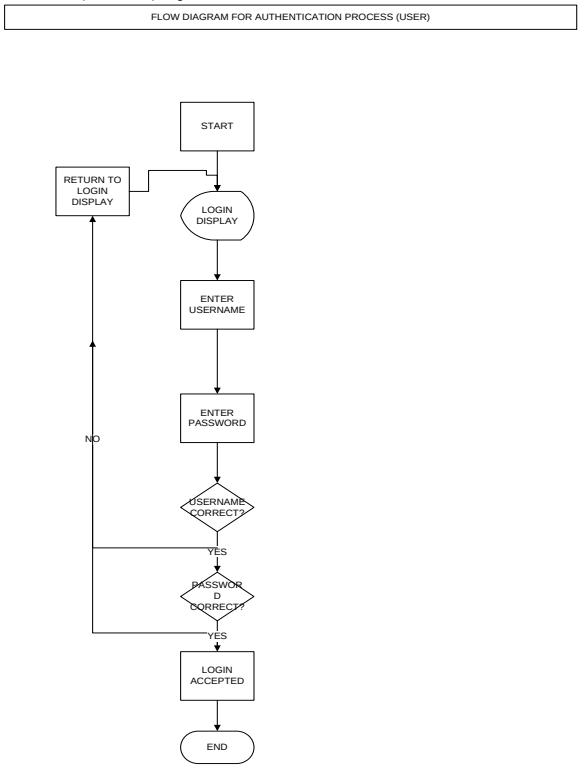

Fig 1 shows the flowchart of the user process in the network authentication

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

IV. TESTING AND ANALYSIS OF RESULTS

The results obtained were the authentications of a valid user into the network and the rejections of an invalid user. We also observed the simultaneous monitoring and filtering capabilities by the admin on the network with respect to the user. Generally, we observed that the results obtained during an event of a secured network mostly depend on the type of security protocol used in implementation. Two protocols mostly in used in security are the Radius and Tacacs. In this work, the radius protocol was used to configure security on the network. The radius server uses the AAA; this required a frame format that supports UDP, a client and a server for its implementation. The implementation of network security on this model were firstly, the cabling of the hardware components implemented using RJ45 straight through cables and with each cabling handling a different part of the model. The network interface card (NIC1) goes through the port to the switch on fa0/9 serving as the server switch port; the other network interface card (NIC2) goes through the port to the switch on fa0/3, serves as the management switch port. Fa0/2 on the switch was connected to the admin/host system port to manage the server and switch interoperability. Fa0/5 was used as WAN port and connected to the router to route information along network from the internet. The fast Ethernet ports (fa0/2- fa0/5) are output ports on the cisco switch that allowed connections to be made between devices on the network. For testing purposes, an external system can be connected to fa0/4 which was configured as a LAN port to ensure proper connectivity and test the model network.

Fig 2 shows the RJ45 straight through cables used in designing of the system

Configuration of the switch and assigning switch port to each virtual LAN (VLAN) network was carried out. VLAN 2 was configured as active trunk port with interface fa0/2 assigned to it while fa0/3-fa0/4 were assigned as access ports to the same VLAN. VLAN 4 was configured as the WAN with fa0/5 assigned to it as an access port. VLAN 3 was configured as radius server (hotspot) VLAN with interface fa0/6 was assigned to it as an access port. These virtual LANs were created to ensure that traffic from one part of the network does not interfere with another part i.e. the client would not be able to see traffic coming from and going to the admin. For better performance, configuring the radius server was done after the switch had been setup. The radius server was the microtik hotspot, an open source radius server. Fig 3 shows the user manager as seen by the admin, the creation of a user and user plan for the authentication process.

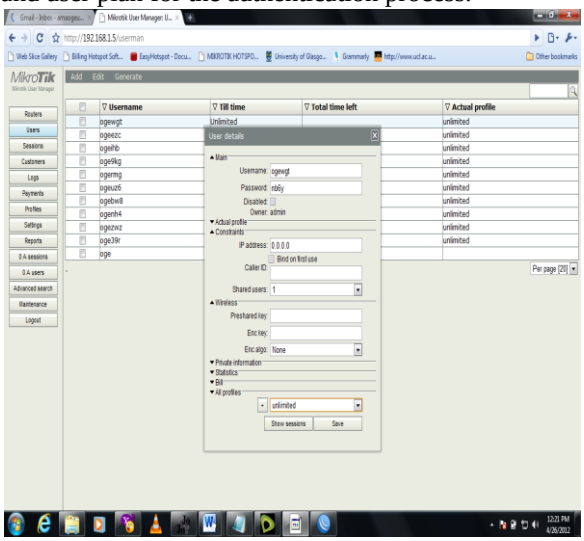

Fig 3 User Manager Mikrotik homepage

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Fig 4 shows the user manager dashboard with already assigned users on the list

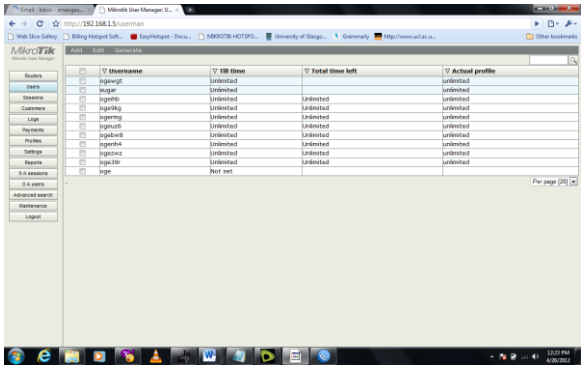

Fig 4 User Manager Dashboard

Fig 5 shows the user authentication login page

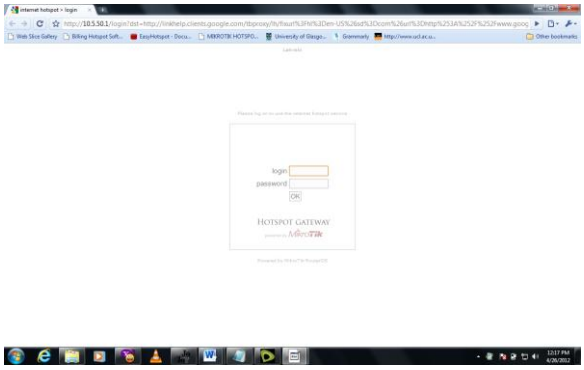

Fig 5 User authentication login page

The radius server generates a means of authentication, authorizes the client to use the network and accounts for the usage of the client on the network. A user can also be forcefully disconnected as for reasons only stated by the admin personnel. After the radius server was setup, the firewall was configured. The firewall in use is the PFSense, also an open source firewall applicable for use in AAA. The configuration of the firewall is done on the server through command line interface it is pertinent to note that the server in use is the Ubuntu server and as such uses only command line interface for its configuration purposes. Fig 6 shows some of the server configuration made on the firewall

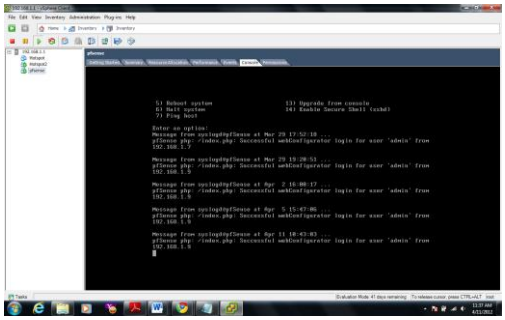

Fig 6 Server configuration

The firewall was configured with an ip address of 192.168.1.3 255.255.255.0 subnet mask. After the CLI configuration was completed, the GUI was enabled on the host system where the interfacing of the firewall and WAN network was carried out. Fig 7 shows the traffic monitoring of some authenticated users.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

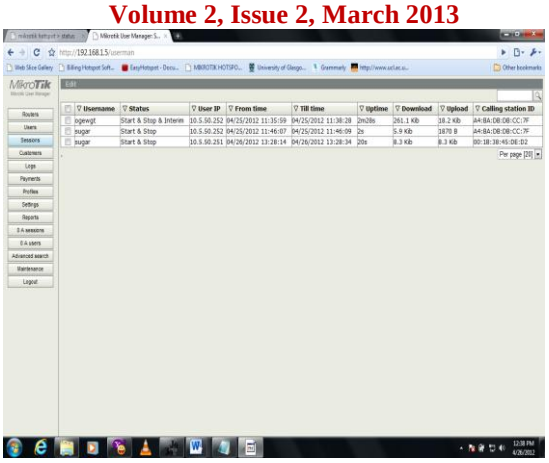

Fig 7 Traffic monitoring of some authenticated user

Fig 8 shows the logged in state of a user

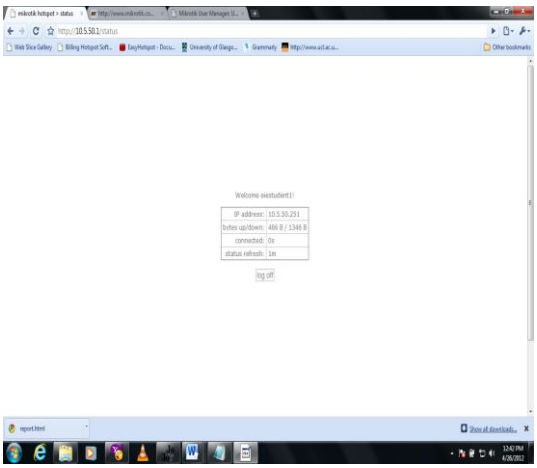

Fig 8 shows the user authenticated login page

Fig 9 shows the logged out state of a user.

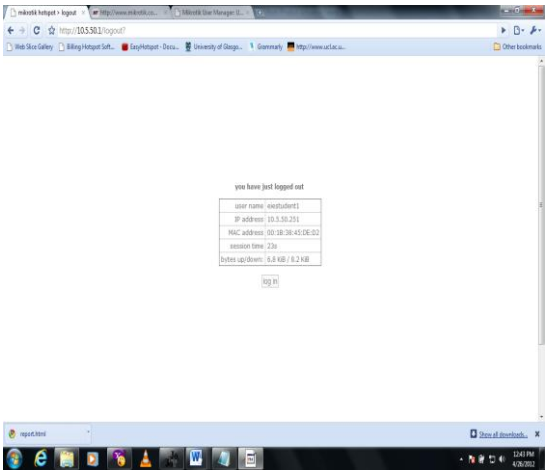

Fig 9 successful authenticated user logged out of the network

The firewall was configured as the base for authorization and accounting in the network. The radius server can handle AAA but for versatility purposes, the firewall was made to monitor incoming and outgoing traffic in the network. Fig 10 shows the structure of the proposed model.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

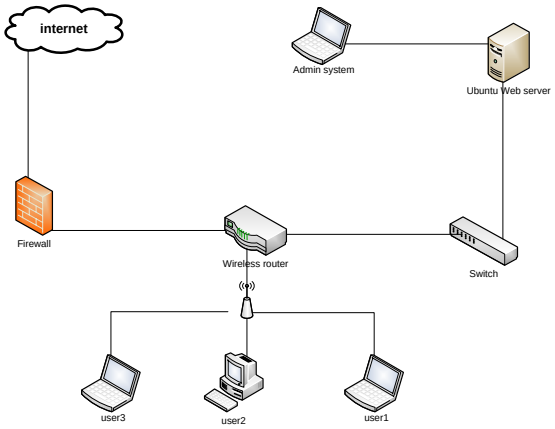

Fig 10 Structure of the proposed model

The firewall and radius server were based on a virtual machine, Vsphere Vclient. It reduces the cost and increase utilization and efficiency in the network management.

V. CONCLUSION

With increasing insecurity in our networks, the ability for a network to be built and be well secured from external sources becomes necessary. AAA has created a platform using various protocols to enable an administrator secure a network and monitor users activity on the network. The radius server enabled AAA, on the platform of authentication, authorization and accounting. Networking is not just about creating a network but also seeing to it that the organization of the network created can be trusted and that confidential information of the company are secured. Therefore, as the world advances, new methods of securing networks are discovered and older ones made obsolete. It should also be noted that the billing system used was determined by the admin.

REFERENCES

[1] Bhavya Daya, “network security; history, importance and future” university of Florida, department of electrical and computer engineering.

[2] Kim j., Lee k., Lee c.," design and implementation of integrated security engine for secure networking," in proceedings international conference on advanced communication technology, 2004.

[3] Salah alabady, “design and implementation of a network security model for cooperative network” in international Arab journal of e-technology, 2009.

[4] Chen s., Iyer R., and Whisnant k,. "Evaluating the security threat of firewall data corruption caused by instruction transient errors," in proceedings of the 2002 international conference of the 2002 international conference on dependable systems & network, Washington, D.C, 2002.

[5] Kim H., "Design and implementation of a private and public key crypto processor and its application to a security system," IEEE transactions on consumer electronics, vol. 50, no 1, February 2004.

[6] Rybaczyk P., "Cisco router troubleshooting handbook", M&T Books, 2000.

[7] Jo S., "Security engine management of router based on security policy," proceedings of world academy of science, engineering and technology, volume 10, ISSN 1307-688, 2005.

[8] **“About ubuntu”**. Ubuntu.com. Retrieved 2011-05-27.

[9] Q. Ali., and Alabady S., "Design and implementation of a secured remotely administrated network," in proceedings international arab conference on information technology, ACIT'2007.

[10] Alabady S., "Design and implementation of a network security model using static vlan and AAA server," in proceedings international conference on information &communication technologies: from theory to applications, ICTTA'2008.