Network Security and Firewall Technology: A Step to Safety of National IT Vision

Afolayan A. Obiniyi, Ahmadu Bello University, Nigeria
Ezugwu E. Absalom, Ahmadu Bello University, Nigeria
Mohammed Dikko, Ahmadu Bello University, Nigeria

ABSTRACT

With the explosion of the public Internet, corporate networks connected to the Internet, if not adequately secured, are vulnerable to damaging attacks. Hackers, viruses, worms, Trojan horses, and spyware try to invade privacy. This research examines how these threats affect the corporate network and ways to reduce them. MikroTik routerOS was configured as the router to examine these threats. Network Address Translation and packet filtering where the key features configured to make the network hidden for unauthorized users and filter unwanted traffics that might reflect malicious acts. The configuration and test were carried out at Iya Abubakar Computer Center, Ahmadu Bello University, Zaria, Nigeria. At the onset, the targeted network was full of virus, worms, Trojan horses, spyware, and vulnerable to unauthorized users. The signal strength of the network was usually very poor due to the effect from the threats affecting the bandwidth. The firewall was configured to filter out inherently dangerous services, exposing the network to fewer risks. After the research, the performance and efficiency of the network was improved tremendously.

Keywords: Bandwidth, Data Security, Firewall, Hackers, Internet, Network, Risks, Threats

1. INTRODUCTION

Data security has been the foremost area in computing sciences that has not been adequately addressed today as hackers and crackers incessantly attack people’s privacy. Often there has been a necessity to guard information from prying eyes. In this electronic age, information that could otherwise be of advantage to an individual can also be used against such groups or individuals. Industrial surveillance among highly competitive businesses often necessitates that vast security measures be put in place.

The term security reminds us of all sorts of items and subjects that relate to data protection and prevention from incursions. The process of protecting data and equipment from unsanctioned access is collectively known as network security (Lammle, 2007). The significance of carrying out good network security is pointed out when considering the unintended consequence of not taking such preventive measures: data can be mistakenly or purposefully erased from the system, a competitor can gain an undue
advantage of getting classified data, and the use of network resources can vanish leading to inefficient or lack of productivity.

Establishments now have continual upsurge dependence on their information and communication systems as the nerve to day-to-day functions and for future stratagem of activities and thus have a lot of security problems to solve, this entails intranets and Internet. However the majority of network security threats originate from within the establishment, there is a growing threat of outside intrusion. This menace is escalated by connection of private (corporate) networks to public networks such as the Internet. In order to lessen the risk of outside parties having access to a private network, a firewall technology is implemented. Possibly it is best to explain first what a firewall is not: a firewall is not simply a router, host device, or groups of device that makes available security to a network. To a great extent, a firewall is a method of security; it assists in carrying out a larger security policy that states the services and accesses to be permitted. It is the provision of that policy in terms of a network setup, one or more host systems, routers, and other security measures such as advanced user identification in place of static passwords.

The major reason for firewall system is to regulate access to or from guarded networks. It carries out a network access policy by strengthening the link to pass through the firewall, where they can be scrutinized and appraised. A firewall system can be a router, a personal computer, a host, or a group of hosts, configured precisely to protect a site or subnet from protocols and services that can be misused by hosts outside the subnets. A firewall system is in most cases situated at a higher-level gateway, such as a site’s linked to the Internet. However, firewall systems can be located at a lower-level gateway to provide protection for some smaller collection of hosts or subnets (Loshin, 2003).

2. FIREWALL TECHNOLOGY

A firewall is a device designed to avoid unsanctioned access to or from a private network. Firewalls can be put into effect in both hardware and software, or both of them joined together. Firewalls are most often used to preclude unsanctioned Internet users from getting private networks linked to the Internet. All data entering or leaving the corporate network pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria (Kao, 2001). Usually, firewalls are setup to guide against unsanctioned interactive logins from the outside world. This assists to disallow “hackers” from logging into machines on a network. More complex firewalls hinder traffic from the outside to the inside, but allow users on the inside to exchange information a little more freely with the outside. Firewalls are important since they can make available a single block point where security and audit can be enforced. Hypothetically, there are two types of firewalls

a. Network Layer Firewalls: These types of firewalls make their decision based on the address of the point of origin, the endpoint address and ports in individual IP packets. A simple router is the traditional network layer firewall, since it is not able to make particularly complicated decisions about what a packet is actually talking to or where it actually came from (Arkin, 2005). There is an upsurge of complexity in modern network layer firewalls, and they now uphold the information about the state of the links going through them at any time. The most vital things about a network layer firewalls is that traffic is routed directly through them.

b. Application Layer Firewalls: These types of firewalls are hosts running proxy servers, which allow no traffic by straight connection between networks, and which accomplish complex logging and scrutiny of traffic going through them. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively masks the origin of the initiating
Related Content

Towards a Rational Technology Approach: Considerations for Building Trust in B2B E-Commerce
www.irma-international.org/chapter/towards-rational-technology-approach/60592/

Technology Related Policies
www.irma-international.org/chapter/technology-related-policies/60587/

Impediments to and Affordances of Creating Trust over the Internet: The Case of Israeli Youth*
Oren Golan (2010). Trust and Technology in a Ubiquitous Modern Environment: Theoretical and Methodological Perspectives (pp. 91-106).
www.irma-international.org/chapter/impediments-affordances-creating-trust-over/42902/

Tensions in Collaborative Cyber Security and how They Affect Incident Detection and Response
Glenn Fink, David McKinnon, Samuel Clements and Deborah Frincke (2010). Collaborative Computer Security and Trust Management (pp. 34-63).
www.irma-international.org/chapter/tensions-collaborative-cyber-security-they/39380/

Internet Trust as a Specific Form of Technology Trust and its Influence on Online Banking Adoption
www.irma-international.org/article/internet-trust-specific-form-technology/51604/