APPLICATION OF FIREWALL TO INTERNET CAFÉS: A CASE STUDY OF ZONAL ALARM FIREWALL

[1]Garba, S.; [2]Abdu-Aguye, U-F.; [3]Ahmad, K.; [4]Musa, A.S.
Department of Electrical Engineering, Ahmadu Bello University, Zaria, Nigeria
[(1)]sgarba2002@yahoo.com

ABSTRACT

The ability of a skilled attacker to trick detection by exploiting ambiguities in the traffic stream as seen by the monitor is a problem for protecting networks. The viability of addressing this problem by introducing a firewall is discussed. The research work involves the examination of Firewall on a Café, examining for its effectiveness against abuses. The firewall sits directly in the path of traffic and patches up the packet stream to eliminate potential ambiguities leading to an attack. Presented is a firewall implementation that can authenticate, block, or allow traffic stream with sufficient headroom to weather a high-speed flooding attack on packets. Routines test carried out are subdivided into security (performance) index, shuttling speed, and bandwidth consumption. From the data collected using zonal alarm (firewall used), more than four-fifth (70% or more) of bytes sent on a packet are protected. Zonal Alarm practical implementation are carried out to detect viruses, spy wares, hackers, spam, abuses in mail attachment, as they being downloaded, or sent on the network; to make traffic decisions without the present of an administrator; and to keep security log activities. The Zonal alarm works more efficient because of its added qualities which include, hardware activities (segmentation processes, forwarding or blocking packet frames, and ascertaining bandwidth subscribed from the internet service providers (ISP) from the readings obtained), and Software activities (elaborate logging, examination of traffic passing, detailed audit reports, and enforcement of conservative security models monitoring). Firewalls authentication is performed at the instant of logging in, in which only authorized users are allowed. Any bridge causes complete blockage at the firewall. This has tremendously assistance in promoting trust, reliability, and confidence between users and co-host. The Zonal Alarm used is an integration of network and application layer firewalls, and equally covers cases where the administrator needs not to be physically present to monitor activities which are lacking in Anti-Viruses.

Keywords: Zonal Alarm, traffic stream.

1. INTRODUCTION

Networks need to be secured to safeguard, and to add confidence to their user. Firewalls are systems that offer such. A firewall is a system designed to prevent unauthorized access to or from a network. They are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet (Strebe and Perkin , 1995). All data entering or leaving the network pass through the firewalls, which examine each packet and block those that do not meet specified security criteria. With the advent of firewalls, single block point can be provided with security and audit. In these regards, they provide an important logging and auditing function (Bulk and Kevin, 2001).

The communication efficiency provided by the Internet has caused a rush to attach private networks directly to it. When LAN is connected to the Internet, users can reach and communicate with the outside world. At the same time, the outside world is enabled to reach and interact with the LAN (King, 2000). Direct Internet connections make it easy for hackers to exploit private network resources. To counter intruders, firewall package, as a measure of protection used. Firewalls, in their barest sense, are routers through which the

data traffic flow. If intruders attempt unauthorized access to a private network, they are stopped at the firewall and not allowed any access into the network (Neils, 2002).

Packet-filtering devices such as screening routers are often augmented by other devices called firewalls. Firewalls, because they operate at various layers of the Open System Interconnection (OSI) model, depend on the functions it is asked to perform (software or hardware firewall protections). A Firewall has to be configured and given complete information on the applications, functions on which to base their decisions (Charles and Kenneth, 1991). There are several approaches to building a firewall. From the different Security level discussed in chapter two, firewalls use Level A, which is currently the highest level of security validated. Also, firewall follows and allows all the TCP/IP suite, sub netting and routing activities discussed earlier. Types and topologies of firewall will be discussed in this chapter, from which the preferred firewall will be chosen for its practical implementation.

2. MATERIALS AND METHODS

2.1 Transmission Control Protocol/ Internet Protocol.

Sets of protocols have to be integrated for communications to be fully established between networks. TCP/IP (Transmission Control Protocol/Internet Protocol) happens to be among such. These communications protocols allow the routing of information from one machine to another through the Internet. This includes delivery of e-mail and news, downloading files and books, and the use of remote login capabilities. TCP/IP provided users with all the facilities mentioned and even more from one site to another on the Internet. It became clear that a wide range of benefits and advantages are available with TCP/IP, and that it is possible to provide cross-country network links (Thompson, 1996).

2.1.1 Transmission Control Protocol. Transmission Control Protocol (TCP) takes large blocks of information from an application and breaks them into segments. It numbers and sequences each segment so that the destination's TCP protocol can put the segments back into the order the application intended. After these segments are sent, TCP (on the transmitting host) waits for an acknowledgement of the receiving end's TCP virtual circuit session, and retransmitting those that aren't acknowledged (Staron and Lierley, 2002). Before a transmitting host starts to send segments down the model, the sender's TCP contacts the destination's TCP to establish a connection, thereby creating a virtual circuit. This type of communication is called connection-oriented. During this initial handshake, the two TCP layers also agree on the amount of information to be sent, before the recipient's TCP sends back an acknowledgement. The path is then established for reliable communication to take place. TCP is a full-duplex, connection-oriented, reliable, and accurate protocol. However it is complex and costly in terms of network overhead.

2.1.2 Internet Protocol. IP (Internet Protocol) essentially is the Internet layer. Most other protocols found merely exist to support it. IP is aware of all the interconnected networks. IP looks at each packet's address, then, using a routing table, it decides where a packet is to be sent next, choosing the best path. Identifying devices on networks requires answering these questions: Which is it on? And what is it Internet Description (ID) on the network? The first answer is the software address, or logical address. The second answer is the hardware address. All hosts on a network have a logical ID called an IP address. IP address is the software, or logical address containing valuable encoded information simplifying the complex task of routing. IP receives segments from the host-to-host layer and fragment them into datagram. IP then re-assembles datagram back into segments on the receiving side. Each datagram is assigned the IP address of the sender and of the recipient. Each router that receives a datagram makes routing decisions based on the packet destination IP address (Staron and Lierley, 2002).

2.2 Examining Security Level

Several level securities are used to protect the hardware, software, and stored information from attack. These levels described different types of physical security, user authentication, reliability of the operating system software, and user applications. These standards also impose limits on types of other system to be connected to the system (Staron and Lierley, 2002).

2.2.1 Level D_1 - This is the lowest form of security available. In it standard state, the entire system is not trusted. No protection is available for the hardware, the operating system is easily compromised; and there is no authentication regarding users and their right to access information stored in the computer. This level security typically refers to operating systems like MS-DOS, MS-Windows.

2.2.2 Level C_1 - Level C has two sublevels of security-C_1 and C_2. Level C_1, the Discretionary Security Protection system, described the security level on the basis of access right. Protection exists for the hardware because it cannot be easily compromised, although it is possible. User must identify themselves to the system through a user login name and password. This combination is used to determine access right to programs and information (Reigh, 1997).

2.2.3 Level C_2 - Level C_2 has all the features of C_1, and includes additional security features that create a controlled access environment. This environment has the capability to further restrict users from executing certain commands or accessing certain files based not only upon the permission, but upon the authorization levels. In addition, this level of security requires that the system be audited. This involves writing an audit record for each event that occurs on the system. Auditing is used to keep records of all security-related events, and requires additional authentication. The main disadvantage of auditing is that it requires additional processor and disk sub-system resources. With the use of additional authorization, it is possible for users on a C_2 system to have the authority to perform system management tasks without having the root password. This enables improved tracking of system administration-related tasks because the individual user performs the work and not system administrator.

2.2.4 Level B_1 - B-level security contains three levels. The B_1 level is the first level that supports multilevel security, such as secret and top secret. This level states that an object under mandatory access control cannot have its permission changed by the owner of the file.

2.2.5 Level B_2 - The B_2 level, known as structured protection, requires that every object be labeled. Devices such as disks, tapes, or terminals have a single or multiple level of security assigned to them. This is the first level that starts to address the problem of an object at higher level of security communicating with another object at a lower level of security.

2.2.6 Level B_3 - The B_3, or security domain level, enforces the domain with the installation of hardware. Memory management is used to protect the security domain from unauthorized access or modification from objects in different security domains. This level also requires that the user's terminal be connected to the system through a trusted path.

2.2.7 Level A - Level A, or the verified design level, is currently the highest level of security validated. It includes a stringent design, control, and verification process. For this level of security to be achieved, all the components of the lower levels must be included. These include memory management, mandatory access control, audit analysis of converted channels, and trusted distribution. Trusted distribution means that the hardware and software have been protected during shipment to prevent tampering with the security systems.

2.3 Firewall Types

2.3.1 Network Layer Firewalls - This type generally makes it decisions based on the source address, destination 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 packet is actually talking to or where it actually came from. Modern network layer firewalls have become increasingly more sophisticated, and maintain internal information about the state of connections passing through them at any time. Network layer firewalls route traffic directly through them. A validly assigned IP address or

a private Internet address block needs to be used, for it proper operation (Thompson, 1996).

2.3.2 Application Layer Firewalls - These generally are host proxy servers, which permit no traffic directly between networks, and perform elaborate logging and examination of traffic passing through them. Since proxy applications are simply software running on the firewall, it is good for logging and access control (Mneghur and Oyfreh, 1990). Having an application in the way in some cases may have an impact on performance, and may make the firewall less transparent. Application layer firewalls initially are not transparent to end-users and require skilled training. However recent application layer firewalls are transparent. Application layer firewall provides detailed audit reports and enforces conservative security models than network layer firewalls (Clements, 2000).

2.4 Firewall Topologies

In this section, different ways a firewall can set up are looked at. Depending on needs, from simple firewall setup, this provides enough protection for personal computer or small network, to a more complicated setup which provide more protection and security.

2.4.1 Simple Dual Firewall - The dual-homed firewall is one of the simplest and possibly most common ways to use firewall. The Internet comes into the firewall directly via a dial-up modem, or through some other type of connection like an Integrated Services Digital Network (ISDN) line or cable modem. The firewall passes packets that meet its filtering rules between the internal network and the Internet, and vice versa. It may use IP masquerading as it major function. This is known as dual-homed host. The two "homes" refer to the two networks that the firewall machine is part of. One interface connected to the outside home, and the other connected to the inside home. This particular firewall has the advantage of simplicity.

2.4.2 Two-Legged Network Firewall - In this more advanced configuration, the router that connects to the outside work is connected to a hub (or switch). It caters for full exposed De-Militarize Zone (DMZ) configuration. Machines that want direct access to the outside world, unfiltered by the firewall, connect to this hub. One of the firewall's network adapters also connects to this hub.

The other network adapter connects to the internal hub. Machines that need to be protected by the firewall need to connect to this hub. Any of these hubs could be replaced with switches for added security and speed, and it would be more effective to use a switch for the internal hub.

There are good things about the exposed DMZ configuration. The firewall needs only two network cards. This simplifies the configuration of the firewall. Additionally, controlling the router provides access to a second set of packet-filtering capabilities. Using these, gives the DMZ some limited protection completely separate, from the firewall. On the other hand, if the router is not controlled, the DMZ is totally exposed to the Internet. Hardening a machine enough to live in the DMZ without getting regularly compromised can be tricky. The exposed DMZ configuration depends on two things: An external router and Multiple IP addresses.

Connecting via modem dial-up, or not controlling the external router, or wanting to masquerade DMZ zone, or having only a single IP address, something need to be done to provide the needed protection. There are two straightforward solutions to this, depending on a particular problem.

One solution is to build a second router/firewall. This is useful if connecting via modem dial-up. One machine is the exterior router/ firewall (Firewall No.1). This machine is responsible for creating the modem dial-up connection and controls the access to the DMZ zone. The other firewall (Firewall No.2) is a standard dual-homed host, and its job is to protect the internal network. This is identical to the situation of a dual homed firewall where the modem dial-up machine is the local exterior router. The other solution is to create a three-legged firewall.

2.4.3 The Three-legged firewall - An additional network adapter is needed in the firewall box for DMZ zone. The firewall is then configured to route packets between the outside world and the DMZ differently than between the outside world and the internal network. The three-legged setup can also give

installation of the software relies on (Jones and Albeit, 1998).

Firewall-1 supports the following major features:
- ▶Protocol specific content filters
- ▶Network Address Translation
- ▶ Virtual Private Network (VPN)
- ▶User authentication is handled transparently through the various protocol content filters.

Firewall-1 supports the following features:
- ▶Firewall-1 Performance
- ▶Policy-Based Configuration and Management
- ▶Content Vectorial Protocol
- ▶Client/Server management
- ▶Automatic Address Translation
- ▶Firewall Module Synchronization

Minimum platform requirements for Firewall-1 are:
- ▶Pentium processor
- ▶At least two network interface
- ▶40MB of disk space
- ▶32MB RAM
- ▶CD-ROM drive

2.5.2 Net Guard Guardian Pro - Net Guard's Guardian Pro (Sygate firewall) is a policy-based crateful inspection firewall for windows NT/2000. Policy-based firewalls are configured based on lists of pass/block rule sets that are human readable, as opposed to IP addresses and protocol numbers. Sygate firewall does not contain proxy service applications, nor does it include protocol filters. This makes it the easiest firewall to establish and configure (Reigh, 1997).

Minimum platform requirements are:
- ▶Pentium Processor
- ▶At least two network adapters
- ▶170MB of disk space
- ▶64MB RAM
- ▶CD-ROM drive

Guardian provides the following major features:
- ▶Packet filtering firewall
- ▶Network Address Translation
- ▶Virtual Private Network (VPN)
- ▶User authentication

Guardian supports the following features:
- ▶Bandwidth Control
- ▶Transparent Address Resolution Protocol (ARP) support
- ▶flood protection
- ▶Anti-spoofing control

2.6 Installation

The installations in both processes (Firewall-1 and Net Guard Guardian Pro) will stop after a short automatic security survey if the machine fails to meet the minimum requirements or some glaring security problem exists with the machine. The most common problems are when the processor speed is low. Once the installation begins, the firewall detects all network adapters (whether inside or outside). Once each adapter is assigned, the firewall will take it trusted network information from the IP addresses of the inside adapters. When the installation is complete, the computer needs to be restarted.

3. RESULTS AND DISCUSSIONS

3.1 Routines Test Carried Out

The Routines test carried out involves installation, monitoring, and performance of Zonal Alarm firewall; inspections and collections of data were carried out. In order to ease the analysis, the data collected are subdivided into: Security index; Shuttling speed; and Bandwidth consumption. These readings are collected over series of days, twice a day, putting into considerations, clients on the network to detect viruses in mail attachment, as they are being downloaded, or sent from server on their network, etc. It equally has adept update amenity.

3.2 Performance-Security

After installing the Firwall-1 (named Zonal Alarm), it was allowed to view data security indices for weeks in order to fully exploit it functions. Later, Security indices are collected

for couple of days, taking into consideration the following:

1. The minimum platform requirements for firewall-1. 32MB Ram, CD-Rom, 40MB hard disk, and Pentium processor are the platforms;
2. The peak usage period of the network at **Online;**

The security indices offered to data packets by firewall-1 are recorded. It has a maximum value of 25 (best) and a minimum of 5 (risk). The Unit used is bytes protected per packet. The data are tabulated for couple of days in Tables 1 to 4.

Table 1: Zonal Alarm Security Indices for Day1

Index	Morning Readings	Night Readings	Average	Gain
Anti-Hackers	19.45	21.07	20.26	81.04
Antispyware	14.86	15.49	15.17	60.68
Anti-Virus	23.01	21.73	22.37	89.48
Anti-Abuse	12.69	10.87	11.78	47.12
Anti-Spam	18.84	17.49	18.16	72.64
Security level	16.79	19.61	18.20	72.80

Table 2: Zonal Alarm Security Indices for Day2

Index	Morning Readings	Night Readings	Average	Gain
Anti-Hackers	20.19	20.36	20.27	81.08
Antispyware	16.23	16.26	16.25	65.00
Anti-Virus	22.58	20.47	21.52	86.08
Anti-Abuse	11.79	11.31	11.55	46.20
Anti-Spam	19.32	16.41	17.86	71.44
Security level	17.49	18.43	17.96	71.84

Table 3: Zonal Alarm Security Indices for Day 2

Index	Morning Readings	Night Readings	Average	Gain
Anti-Hackers	18.76	19.81	19.28	77.12
Antispyware	17.11	14.33	15.72	62.88
Anti-Virus	19.86	21.71	20.78	83.12
Anti-Abuse	13.98	12.24	13.11	52.44
Anti-Spam	15.97	18.79	17.38	69.52
Security level	16.78	18.61	17.69	70.76

From the data collected, it can be viewed that data trafficking between networks are respectively protected. It can be viewed from Tables 1 to 4 (anti-hackers, anti-virus, anti-spam, and security level) are more than four-fifth protected. This is a significant improvement as compared to protection offered without firewalls, which are below average protection. Anti-spyware protection is above 50% protected, but protections without firewall do not offer such.

Table 4: Zonal Alarm Security Indices for Day3

Index	Morning Readings	Night Readings	Average	Gain
Anti-Hackers	17.97	22.07	20.02	80.08
Antispyware	15.67	16.82	16.24	64.96
Anti-Virus	21.41	22.67	22.04	88.16
Anti-Abuse	13.43	14.19	13.81	55.24
Anti-Spam	19.43	17.63	18.53	74.12
Security level	17.98	19.67	18.82	75.28

Subsequent data readings were further taken, at various time of the day with firewall installed, and are tabulated for couple of days. These data collected for additional days have shown that there is not much difference with regard to protection of data on the network as in first day. This has added to client confidence on assurance on sent/received, and packets security.

3.3 Shuttling Speed

Analyses are further carried on data traffic on the network. Client bandwidth rate are viewed over range of time, so as to determine the reaction to data request, latency on the mail sever. This was carried with the firewall. The Firewall-1 used is Zonal Alarm gate-way. Pinging commands are used to determine the time as regard to bandwidth.

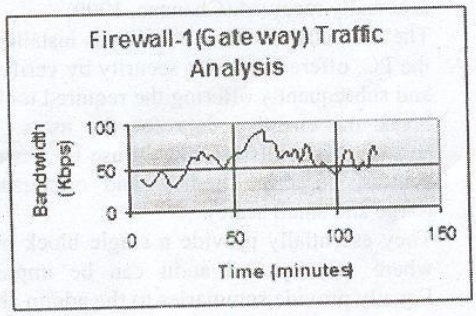

Fig 1: Zonal Alarm Inbound/Outbound Speed

The same client was used for both with regards to data traffic analysis on the network. The client named café 1, with IP address 212.199.203.23. The client "café 1" request to the Internet via the downlink bandwidth, the reply came through uplink bandwidth. The uplink bandwidth is the determining factor for speed and latency, which is recorded each 5 minutes (maximum) for 2 hours. From the data collected it's clear that there is no signal truncation, and there are more available uplink bandwidths to be pulled. This can be viewed from the fluctuation in bandwidth consumptions as time progresses. From fig 1, it is clear that latency is offered by the firewall-1, as well as inbound/outbound traffic analysis without firewall. This is the major setback of firewalls. It offers high protections, but with latency. The key reason for these, is firewall operate at a virtual private network (VPN) layer created below IP layer due to it installations. All activities of the firewall are conducted at the VPN layer, includes authentication, blocking, forwarding of packets, and allowing access. Much trun of the available down link bandwi therefore offered.

3.4 Bandwidth Consumption

The dedicated Bandwidth and the throughput can be ascertained on the g using firewall. Any bandwidth subscrib be viewed from the firewall control m This module keeps track of record of av bandwidth, as well as bandwidth buzz network. Border gate bandwidth (BGBL) was installed into the firewall to ascertain the bandwidth subscribe. BG software used to measure ban consumed, it can equally be configu firewall to act as an observer to ban subscribe. The bandwidth specification by the control module is 64/128 Kbps. a big plus to subscribers of bandwidth, firewall can easily detect any abnor offered by the Internet Service Pr (ISP). It ensures that ISP does not comp securities offered to customers.

4. CONCLUSION

This analysis offers range of firewalls and their limitation as regards to installation. Firewalls offer choice of allowance to incoming and outgoing packets of data. The hardware firewall incorporated to layer 1, 2, and 3 of OSI model data (includes routers, hubs, bridges, repeaters, switches) authenticate frames with their headers, packets of data, the converted bits, at the sending end. Later at the receiving end, authenticate the bits, as well as packets of data, and make sure what was sent is actually received (Chanana, 1999).

The firewalls software, which was installed on the PC, offered efficient security by verifying, and subsequently offering the required tools to break the encoded data for the users. The software firewalls are mostly use by business centers, corporate bodies, and organization (large and small scale).

They essentially provide a single block point where security and audit can be imposed. Equally provide summaries to the admin about what/type of traffic that has been processed through it. This is an important point: providing this block point can ser purpose of armed guard on the network. Firewalls authentication is performed instant of logging in, in which only aut users are allowed. Any bridge causes co blockage at the firewall. This tremendously assistance in promoting reliability, and confidence between us co-host.

They define the complexity, length lifetime passwords for user ac determine the best way to convey requirements. By setting firewall audit Windows 2000 can track a variety of s event types. These event types can be s wide, like user logging on, or more spe like a user attempting to open and specific file.

Firewall security options policies all administrator to control settings that force users to log off when logon exp prohibit. These policies define back restorations of files, and the ownership.

The firewall technologies that are used in screening routers provide an efficient and general way to control network traffic. They have the advantage that no changes are required to client and host applications because they operate at the IP and TCP layers' and these are independent of application-level issues.

The firewall is the chief instrument used to implement an organization's network security policy. In many cases, authentication, and security, and privacy enhancements techniques are needed to enhance the network security or implement other aspects of the network security policy.

By controlling the type of network traffic that can exist on a network segment, the PC-based packet firewall can control the type of services that can exist on a network segment. Services that can compromise the security can be restricted (Querous and Wan, 1993).

REFERENCES

Staron R.J. and Lierley M. (2002). "Security Complete", 2nd edition, Sybex Publishing inc.

Clements, A., (2000). "The principle of computer hardware", 3rd edition, Oxford Science Publications.

Strebe M. and Perkin C. (1995). "Firewall 24seven", 2nd edition, Sybex Publishing inc.

Chanana, R.N. (1999). "Reliability Evaluation of Networks", Prince-hall Pub. inc., pp.167-175. www.firewall.cx

Siyan, K. and Hare, C. (2002). "Internet Firewalls and Network Security", 3rd edition, New Riders Publishing, Indianapolis, USA.

King, R. S. (1992). "LAN Operating Systems", Oxford Publishers inc.

Gaskin, J. (2000). "Fundamentals of Networking", 4th edition, Howard W. Sams and sons company inc.

Thompson, B. K. (1996). "Internet Routing", Longman Group UK Limited.

Querous, Z. U. and Wan, E. (1993) "Network Management, & Policy", 3rd edition, Sybex publishing inc.

Govanus, G. (2000). "Mastering Networks", 4th edition, John Wiley and Sons.

Bulk, D. R. and Kevin, E. (2001). "Data Exchange on Networks", Platinum Press New York.

Todler, F. (2002). "Network Security Fundamentals" Prince hall Publishing inc.

Charles, V. and Kenneth, S. F. (1991). "Packet Filtering", 3rd edition, Sybex Publishing inc.

Neils, J.L. (2002). "Network Layer Firewalls", Hallmark publishing inc.

Reigh, U.G. (1997). "Securing Your Networks", 4th edition, Sybex Publishing inc.

Jones, A. and Albeit, T.I. (2001). "Configuring Firewalls", Missile Hall inc.

Ecylehn, W.E. (1998). "Downsizing Communicating Networks", 5th edition, Academic press inc., pp 76-89.

Mneghur, C.Z. and Oyfreh, J.D. (1990). "Network System Communication", 3rd edition, Prince hall Publishing inc., pp 256-272.

Akawi, W.; Davies, N.; and Moletti, H. (2004). "Windows Middle East", Information & Technology Publishing co. ltd London. Pp 62-67.

Karanji, S. (2003). "PC Network Integration", March 2003, New riders Pub. Indiana., pp 5-9.