Securing Local Area Networks with Firewalls: An Overview of its Application to Windows NT and Unix-Based Networks

Shakir A Sanni
Sash0001@stcloudstate.edu
(320) 252 0811

Department of Statistics/Microcomputer Studies Program
St. Cloud State University
720 Fourth Avenue South
St. Cloud MN 56301-4498

Abstract

The issue of computer network security has generated concern and attention in the past few years more than ever before. Over the years, the control of computer information has shifted more and more to desktops and remote sites via networking. As a result of this, organizations have continued to use the services of third parties companies to convey important data information within their intranet and the internet. This paper provides an extensive review of network security, specifically Firewall implementations, on Local Area Networks of Windows NT and Unix Operating Systems. It addresses the basics of computer network security, its evolution, and the problems faced in securing data over networks where it is desirable to permit access to some users while simultaneously denying others such access. In addition to this,

Firewalls implementations are arguably the most secure way of protecting data from intrusion on computer networks. As a result, this document provides an insight into computer security problems that necessitated the design and implementation of firewalls. The paper discusses various firewall implementations in relation to different architectures and addresses the issue of securing Local Area Networks from unauthorized intrusion from within and outside the network.

Other areas covered in the review include the economics of implementing firewalls, governmental regulations and policies affecting computer network and security, and the overall efficiency of firewall technology.

Introduction

Computer networks can be looked at as all the services and resources employed to guide and secure computer data from unauthorized access. Companies and business concerns are depending more on the capabilities of computers, and with increasing reliance on computer networks, the cost of breaching computer security continue to increase. Over the years, the control of computer information has shifted more and more to desktops and remote sites via networking [2]. As a result of this, organizations have continued to use the services of third parties companies to convey important data information within their intranet and the internet.

The issues in computer network security has changed over the years from the early mainframe computers to the modern microcomputers in terms of criteria specification and requirements [2]. With early mainframe computers, a lot of importance was attached to the security of the processing unit and less to terminals and physical location of the system because of its size and complex design which was a security device on its own. In the last two decades, the portability, intelligent systems attributes and user-friendliness of modern microcomputers makes the issue of computer security more critical than ever before. Microcomputers have distinctive security problems that needs to be well addressed for an effective security policy [2]. Some of the issues that needs to be addressed include physical accessibility, hardware, software, data communication, and networking and Disaster recovery [2]. This paper focuses on the issue of computer security on microcomputers with respect to software and specifically the issue of implementing firewalls in Unix and Windows NT Operating Systems Platforms.

Security Problems of Computer Networks

Modern commerce and the urge to remain competitive in the dynamic business environment is driving major business concerns to create business presence on the internet. When an organization creates its presence on the internet, and no adequate security for its data is put in place, its electronic information and data becomes a target of attack from hackers and malicious users on the internet. There are several risks that electronic data of organizations are exposed to and some of these dangers are:

- Loss of classified or private information such as accounting records, strategic planning records and design prototype materials not yet made public and loss of control of this critical information on the network [3].
- Loss or corruption of important services such as Electronic Data Interchange (EDI) and Enterprise Resource Planning (ERP). This could hinder the entire long term business plans of business organizations [3].
- Loss of public confidence in organizations with no proper network security policies and attendant risk of legal liability [3].

Firewall implementation assists in managing a network and addresses all the issues listed above. Because it is designed basically for securing the network for varieties of intrusion, it provides network managers with a series of guidelines and management strategies that can assist in implementing efficient security policies.

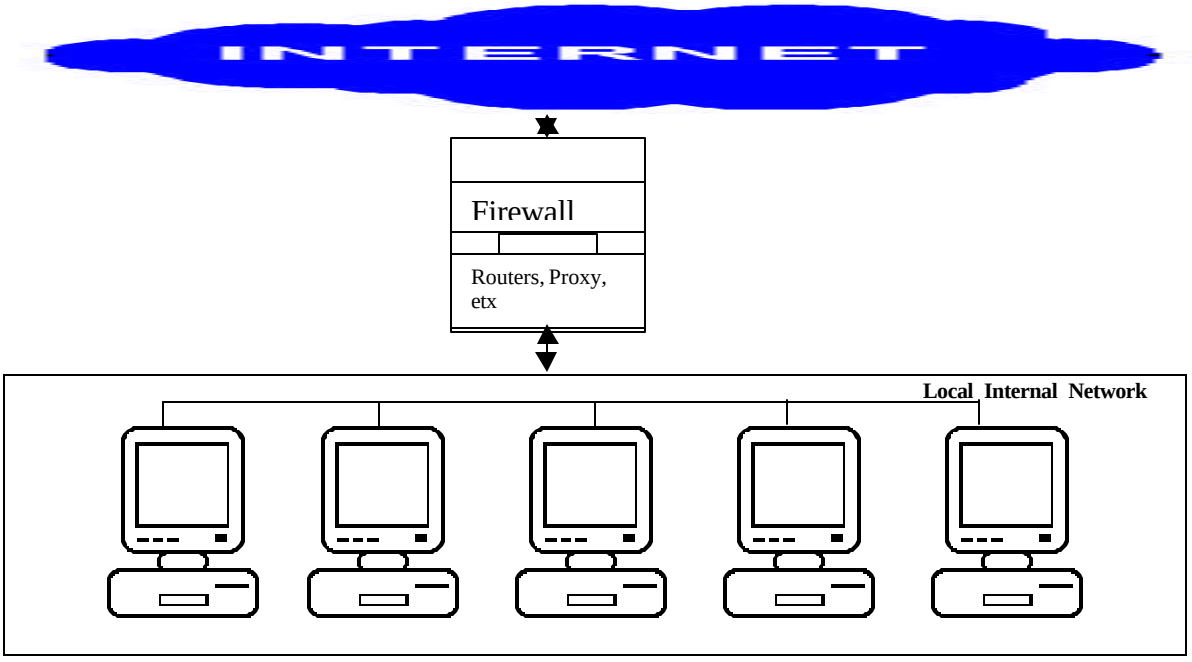
Computer Firewalls

Firewalls originally came in to being to control the spread of fire on plantations and buildings. Modern Computer Firewalls are devices and systems carefully integrated together to control data information flow between two networks. Firewalls could be as simple as a router configured for IP filtering on a local computer to more complex devices of a combination of several systems to analyze all packets and services passing into and out of a local area network and performing statistical and combinatorial analysis on them. A typical firewall could contain one or more of the following components [5];

- A Packet filtering router
- Application-level gateway (or proxy server)
- Circuit-level gateway

Figure 1 shows how these devices work together to achieve a common goal of preventing the network from intrusion from unauthorized user.

Fig 1 Conceptual Firewall Design



Firewalls prevents intrusion into computer networks and they are valuable tools for Computer Network Administrators to control the inflow and outflow of data on networks [1]. The operations and implementations of firewalls is in two folds namely to control the

inflow and the outflow of data on a network. At this point, it is important to note that firewalls is not just a single device like a router that links the local network to external networks but a combination of devices and services that ensures the overall security for a network. Essentially, for firewalls implementation to work and be adequate, it normally includes all resources pulled up together to arrive at an efficient security program for an organization. By this, security standards circulated among members of an organization to adhere to, corporate policies on account creation, password standards and network access rules and regulations are also included. Frankly, a detailed and a comprehensive overall network policy is fundamental to the success of firewalls implementation [5].

Deploying Firewalls on Windows NT and Unix Operating Systems

Preliminary Considerations into Firewall Designs

There are several strategies to the organization and implementation of firewall designs. Several decisions are made on issues like the primary functions of the firewalls, the overall security policy of the company in question, the economics of implementing the firewall and the information being protected and finally all the devices and resources to be deployed in building the firewall system.

The primary functions of the firewall could be looked at from the perspectives of a pessimistic or optimistic security strategy. The former is a strategy whereby firewalls deny access to all incoming traffic into the network. This method inspects all desired traffic into the local network. While this method is recommended and appears to be the most secure, it puts a lot of processing load on the overall system. Another limiting factor of this method is that it puts security ahead of ease of use and user friendliness of applications and services. The latter method allow all network traffic to be forwarded and traffic flow from all sources except those considered to be potential threats to the organization. This could arguably be described as not as secure as the first one but the overall network performance could be better and the advantage of ease of use is also a benefit of this policy.

The integration of the firewall planning and the overall security planning of the organization is also a crucial factor in the successful implementation of firewall systems. Organizations must have a concrete security policy and know the documents to actually prevent from intrusion. It is also recommended to categorize data and electronic information based on the level of security needed to be placed on them. Another important consideration is in the cost of firewall implementation viz a viz the importance of the data that is being prevented from intrusion. The cost of firewall implementation could vary. While simple implementations could cost about $4,000.00, with already existing expertise deployed to implement and manage, some firewall implementation could cost as much as $100,000.00 or more and require highly skilled experts on network security to implement and maintain. After thorough evaluation of the primary functions of the firewall in the organization including the cost and the security policy of the

organization, all the equipment to use to build a suitable firewall is also an important initial consideration before the actual implementation.

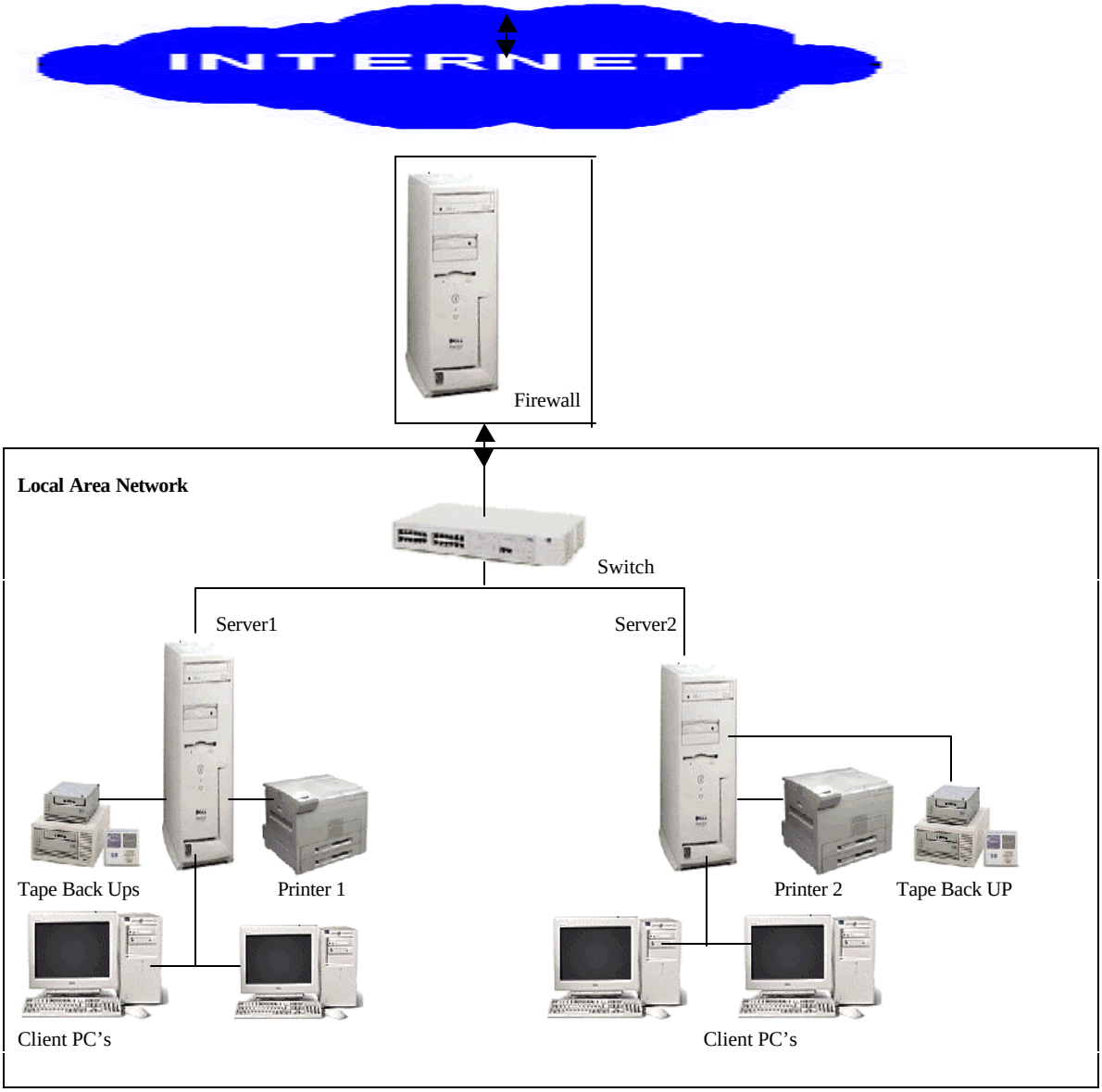
Firewalls on Windows NT and Unix Operating Systems

Windows NT and Unix operating system are by far the most popular operating systems available today. They are the operating systems that are used for enterprise networking and they have certain attributes such as multitasking, multiprocessing, discretionary access control mechanisms which make them suitable for most enterprise networking environments. While the designers of both operating system continue to update and improve the performance of their system applications, unscrupulous users of this system continue to subject the systems to series of tests so at to map out strategies of rendering the security and integrity of this operating systems questionable. These operating systems, in order to overcome all this problems, employ inbuilt security measures and also implement firewalls in their quest to overcome all these threats. In general, an efficient and effective firewall technology implementation on any operating system is broken down into four parts namely preparation, configuration, testing and implementation.

Preparation

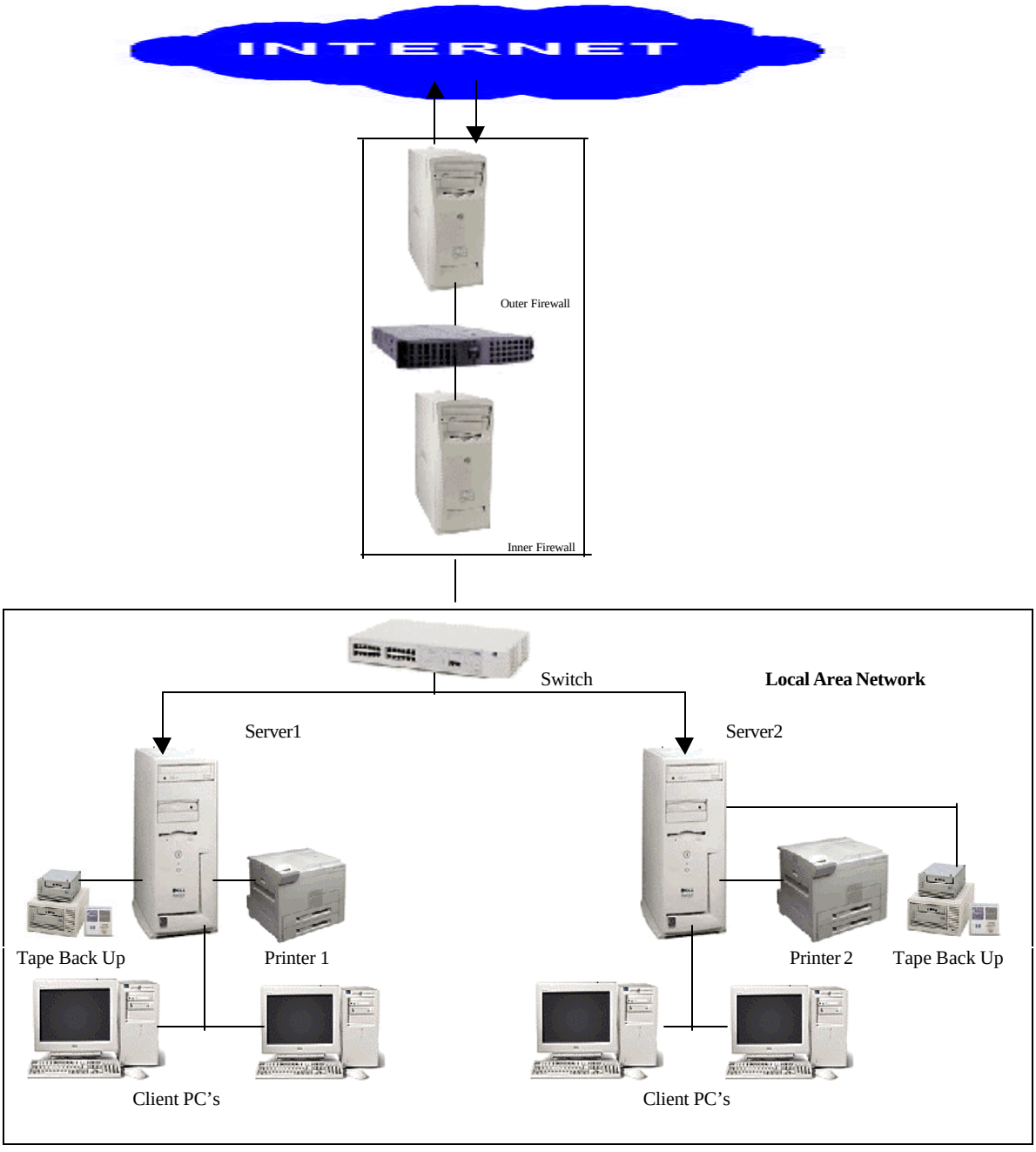
A well designed network system either in Windows NT or Unix platforms or their combination requires the logical separation of computers into groups based on their functions. This group known as domains is the bedrock of large scale local area networks and it involves grouping computers of computers operating under a common security policy together for easy administration [10] . Whenever domains interact, there is bound to be potential problems of network security and this is where firewall implementation comes in to play. Preparation of firewall involves getting the materials and equipment to use together. It includes knowing the level of security to place on data so that the most suitable firewall design is identified for the network architecture in question. The most common firewall implementation is usually to safeguard a local area network from the internet. Two main designs are explained below and these are single layer firewall design and multi-layer firewall design. The single layer design involves a situation where a unique host is charged with all the responsibilities of the firewall implementation and the host controls all access into the entire local network. This design is usually convenient for small to medium sized network where cost is a limiting factor and it is easier to implementing However, the pitfall to this style of design is that its vulnerable to implementation flaws and its over simplicity makes the entire network insecure as there is only a single focal point for security implementation.

Figure 2 depicts a simple one layer firewall implementation design



The other type of firewall implementation which is referred to as the multi layer firewall design involves spreading the responsibility of securing the network over more than one host which in most cases are connected in series. This design is difficult and complex but it not only spare a single host from a lot of bandwidth and processing resulting from securing the entire network, it also provides an avenue to implement a lot of security mechanisms over a lot of host. Hence the probability of and entire security failure is highly reduced. This type of firewall is however costlier than the previous one. The diagram below Figure 3, is a representation of the multi layer design of firewall implementation.

Fig 3 Example of Multi-layer Firewall Design



Another thing to consider whichever of the two designs adopted is whether the firewall will be implemented as packet filtering or application proxies. It is important to note that while services like SMTP, HTTP, or NTP are better monitored and controlled through packet filtering, services such as DNS and FTP may require some complex and scripting

features which are only available through proxies to achieve desired security on the network [7].

Packet filtering, usually implemented on routers and special purpose computers are usually fast in terms of processing. Proxy systems are usually general purpose computers that run applications that effectively conceal the identities of systems on the local area network from prying eyes on the internet and other external intrusions. Proxies operations of authentication and security controls are generally slower and arguably more secure than packet filtering. Proxies generate a lot of overhead and also use a lot of computing resources. For example consider a Unix Operating System where a certain firewall technology running on a UNIX platform needs to support 200 concurrent HTTP sessions. The host must be capable of supporting 200 HTTP proxy processes with reasonable performance. Add 100 FTP sessions, 25 SMTP sessions, some LDAP sessions, and some DNS transactions and you have a host that needs to sustain 500 to 1,000 proxy processes. For organization where security is paramount to the successful running of their business, applying both techniques is usually advised.

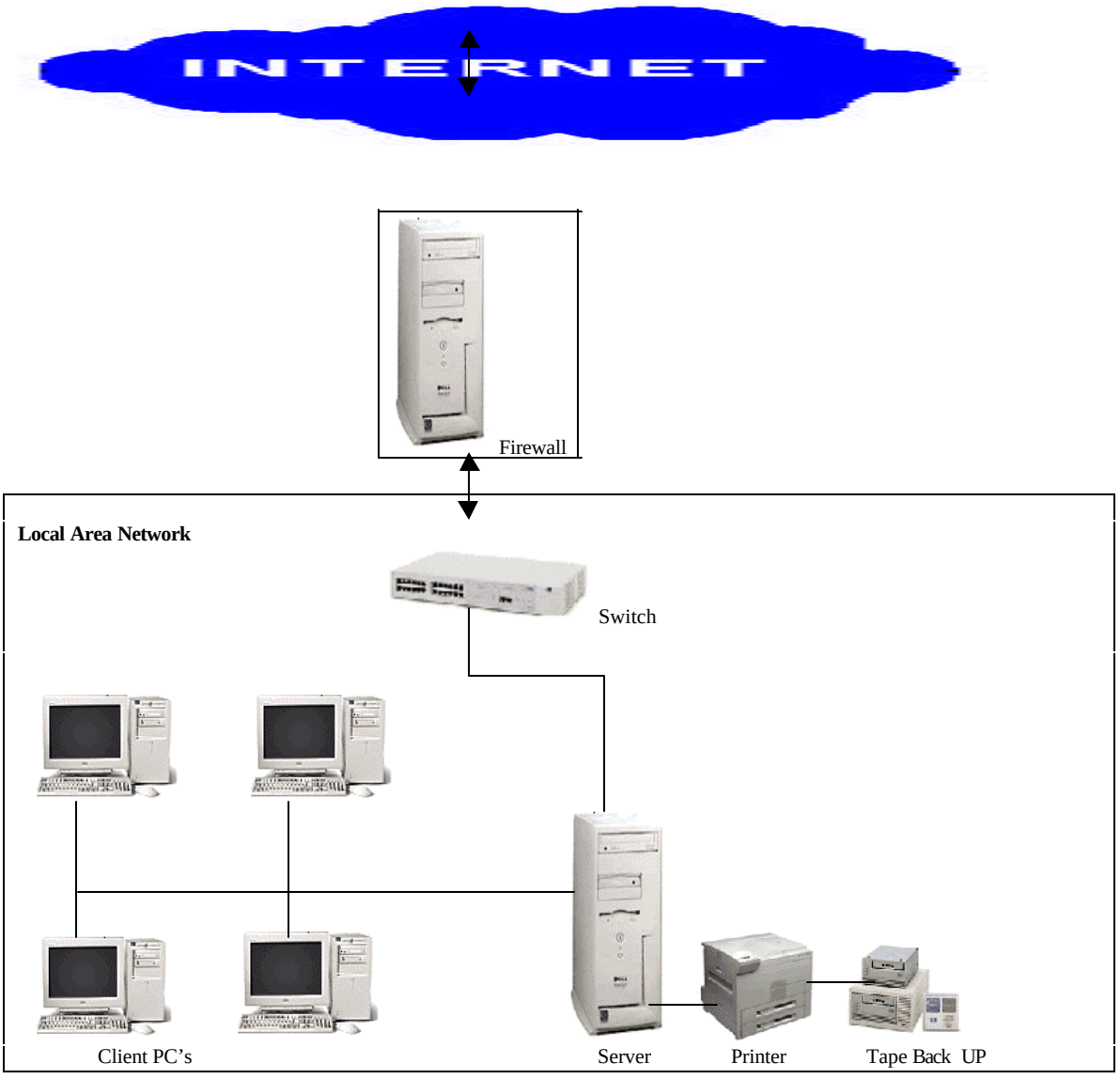
Having explained firewall design, this paper next evaluates three different firewall topologies. Any of these topologies could be implemented in either of the two firewall designs previously discussed. These are explained below.

Basic Border Firewall Topology [3]:

This is arguably the simplest form of firewall design. This system involves connecting the network to the external network such as the internet and putting in place a dedicated host between the two networks which provides all the firewall functions. The host in most cases is a packet filtering router that monitors traffic flows between the networks and allow or deny packets based on how it is configured. Below is the diagrammatical representation of its implementation.

This design is easy to implement and require minimal technical expertise unlike the other designs.

Fig 4 A Diagrammatic representation of a basic boarder firewall architecture

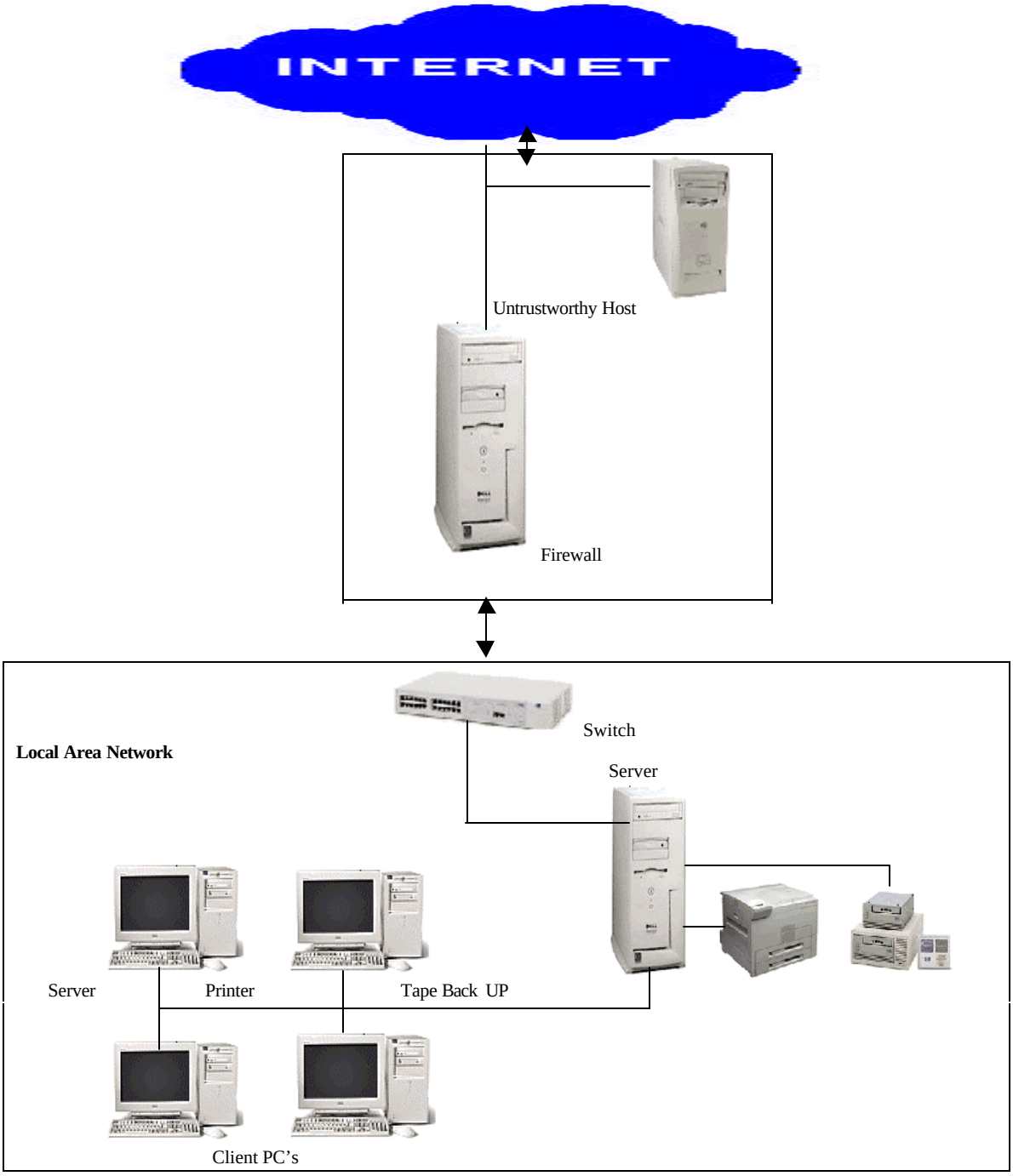


Untrustworthy Host Topology [3]:

Another popular design is the untrustworthy host design which goes a little bit further in terms of security and design than the basic border firewall design. The design is similar to the basic boarder design but the difference is the addition of a host between the external

network and the firewall that protect the internal network. With this implementation, network and application layer security are both integrated and employed with the aid of the firewall and the additional host respectively. The host is configured to provide some degree of security to the firewall that protects the local network. Below is a diagram of how it looks like.

Fig 5 The Untrustworthy Host Architecture



DMZ Firewall Topology [5]:

This design known as the De-militrirized Zone Firewall Design is a multi-layer architecture and is arguably the most secure of all the designs; it involves using more than one packet filtering router and another host acting as a firewall between the external network and the internal network [5]. While the routers that is directly connected to the internet protects the local network against direct external attack such as source IP address spoofing and source routing attacks, the internal router make ensures that only requests that comes from the host firewall serving as a proxy server is being allowed to pass to the internal network. By this arrangement, there is no direct flow of traffic between the external network and the local network.

Configuration:

When the appropriate design is selected, the required hardware and software are then acquired. Things like performance analysis and estimated traffic flow are also evaluated to know the actual hardware and software components to buy. Hardware components include processors, RAM, routers, switches, hubs, backup devices, network interface cards and power supply components, cables, telecommunication components and movable storage devices like floppy and CD ROM.
On the other hand, Software components include operating systems, third party software utilities driver software, network monitoring and traffic analysis softwares.

Hardware and Software Installation:

Following any of the various architectures previously discussed, the hardware and software are installed. Before the installation, it is important to verify that the entire system configuration includes all packages and services required for firewall operation. It is recommended to disable services such as X windows and NFS and any other ones not required if the implementation is in a Unix environment while services such as NetBios and anonymous guest access should be removed or disable on Microsoft NT Operating Systems.
Implement all available useful information on patches. This is usually obtainable from vendors. This patches could be test run on redundant systems to ascertain their functionality. Discretionary access control of users should also be strictly enforced and it is advisable to de-activate any IP forwarding prior to activating any interface.

In addition to all these, patches should be evaluated periodically and the architecture of the firewall design kept secret and only available to authorized personnel.

IP Routing Configuration:

Routing is the process of delivering packets to their appropriate destinations based on the network address of the recipients on the network. Packets are either forwarded to recipients or other routers on a multi domain network or discarded after a specified length of time if the destination is unreachable. The decision is done at the packet header which is controlled by the routing table. The routing functions are usually not very secure, hence a routing configuration that reflects the network topology is important so that firewall systems will be able to forward genuine packets to their desired destination.

Configuring Packet Filtering:

Packet filtering is the process of screening all incoming packets into the local network.(The packet is the basic unit of electronic information on the network). Packet filtering could be configured on devices such that packets can be accepted or denied into the local network based on criteria such as packet header information, source address, destination address, source port, destination port, packet length and packet payload.

Firewall Logging and Alert Mechanisms:

It is important to log important firewall operation s and events. The logging could be of incoming and outgoing packets to the firewall or those related to the operations of the firewall. This is crucial to ensure the continuous operation of the firewall and to monitor the pattern of information flow into and out of the network.

Testing:

It is important to test the firewall to see if it meets the desired requirement. This is done on redundant system or in a test environment. The things to watch out for in the course of testing include the Hardware Components such as processor, disk, memory and network interfaces. Other things to be tested is the Operating system and processes such as booting and console access to see how it is performing. Devices such as network interconnection equipment and firewall software must also be tested to ensure that they meet required standards.

Implementation:

The tested firewall system is now to be implemented in the production environment, which in most cases is an existing network. This should be carefully planned and executed to minimize disruption to the production environment. The new firewall system should run parallel with the existing system at the initial start up. While implementing the new firewall system, unfiltered packets should not be allowed into the firewall system and a proper documentation of all activities should be done. Below are recommended practices in both Unix and Windows Operating systems environment.

Detailed Practices when Implementing in a Unix Environment [3]:

- With the local network running the verify the integrity of the file contents on the systems. This could be done with MD5 or any other derivative.
- Scrutinize the Unix system for logs and evidence of intrusion. Inspect all logs produced by TCP Wrapper for system running Solaris 2.X also. Finally use ps to examine if there are any intrusions.
- Configure Unix Servers, Enable Process Accounting and configure tcp wrapper and syslogd to log unauthorized connection and collect logging messages on systems respectively.
- Install and configure logdaemon to log unauthorized login attempts and use swatch to analyze processes running on the server. Also, install log surfer, top 3.x on services running on server and npasswd to improve the integrity of passwords.
- Configure secure shells on systems and implement native tools on server to detect changing directories.
- Install lastcomm and spar 1.3 on systems running Solaris 2.x. Install tcpdump 3.5 x as well as Argus monitor on Solaris server
- Use news Argus log to rotate to rotate files on systems running Solaris. Install libcap to support network packet tools on the system running Solaris 2.x
- A good understanding of network intrusion detection system, disabling network services on systems running Solaris 2.x and finally installing noshell to check and control access to disable accounts on the Solaris System.

Detailed Practices when Implementing in a Windows NT Environment [3]:

- Watch out for initial attack during installation. It is advisable to isolate the system from the network during initial installation. All workstations and servers should be secured during installation.
- The primary and backup domain controllers should be secured during the initial installation.
- Use RDISK and SYSDISK to create Emergency Repair Disk and protect password data files in Windows NT respectively.
- Audit event for files and directories and windows NT registry keys and restrict access to the %SYSTEMROOT% Repair directory for Windows NT.

- Set up log on banner and configure Windows NT to shut down automatically when writing to an event log fails.
- Audit printer events, activate event log and audit policy settings on Windows NT Systems.

Economics of Implementing Firewalls and Government Regulations on Network Security:

The financial implications of deploying firewalls could be low, moderate, or high, depending on how complex the firewalls architecture to be implemented is. Again the choice of the complexity of the firewall design to adopt largely depends on the value attached to the information and electronic documents to be secured. While some local networks require only to protect the systems from hosting illegal documents posted by malicious users, some network completely forbids preying external users from gaining any access at all to the network.

Governmental institutions on the other hand are not relenting in their effort to assist in securing computer networks. Unscrupulous internet users face stiff penalties for unauthorized intrusion in to local networks [1]. In some cases, the hackers are investigated for various computer crimes that they may have committed in the past [1]. In the United States, computer crimes such as breaking into organizations local network and de-facing web sites are federal crimes that perpetuators face stiff sanctions for. On the other hand, sharp practices by organizations such as data manipulation malpractices and infringement of licensing agreement are also federal offences which the offending party may be sanctioned or taking to court to face charges such as copyright violation.

Recommendations and Conclusions

The issue of securing local computer network is a continuous process [9]. In some cases, a vulnerability in a local network is not noticed until external users a.k.a hacker takes advantage of the weakness in the computer security [9]. While firewall implementation technology has been very useful in securing computer networks intrusion, electronic information still experience some minimal threats. Most firewalls implementation do not secure electronic information from virus attacks [5]. Allowing script access such as Active X Controls and CGI scripts on local networks are practices generally not recommended because of the vulnerability attributes of this scripting languages. In addition to all these, it is important to note that some firewalls implementation which function like proxies are optimized to control Telnet and FTP traffic while other firewall implementations such as packet filtering are optimized for IP filtering [4].

Firewalls are useful tools of security and should be strongly considered before connecting local networks to external hostile networks. Its implementation should be integrated to the entire security policy of an organization to ensure the realization of all the potentials of firewall implementation. Firewalls cannot protect the network if it is badly configured

or if implemented after security has been breached. For small networks, a good password policy in addition to the firewall is recommended as well as procuring current anti-virus software to check dangerous attachments on emails. Large corporate organizations should

References

[1] Boran, S. (2001). Personal Firewalls/Intrusion Detection Systems : An Analysis of Mini-firewalls for Windows Users. Retrieved February 18,2001 from the World Wide Web: http://www.securityportal.com/articles/introduction.

[2] Cameron, A. (2000). "Cameron Innovative Security Products : Computer Security White Paper." Retrieved February 18,2001 from the World Wide Web: http://www.isecure.com/pc-security- white-paper.htm.

[3] Cert, Cordination Center. (2000). "CERT® Security Improvement Modules" Retrieved February 18,2001 from the World Wide Web http://www.cert.org/security- improvement/modules/m08.html.

[4] Dennis, G. (2000). Lecture Notes of MCS526 (Computer Networking II) St. Cloud State University,

[5] Goncalves, M. (1998). Firewalls Complete. Mc-Graw Hill Publishing Washington

[6] Ray, Joan and Ray, William. Unix System Administration in 21 days. McMillan Computer Publishing Indiana.

[7] Reinhardt, Robert B. (1993) "An Architectural Overview of UNIX Network Security". Retrieved February 18, 2001 from the World Wide Web: http://www.alw.nih.gov/Security/Docs/network-security.html.

[8] Semeria, Chuck (1996) "Internet Firewalls and Security: A Technology Overview" 3 Com Technical Paper Series. Retrieved January 7,2001 from the World Wide Web: //http://www.3com.com/nsc/500619.html

[9] Strebe, M. & Perkins, C. (2000). MCSE: Internet Information Server 4 Study Guide Exam 70-087 Seattle: Amazon Press.

[10] Strebe, M. et al (1999). MCSE: NT Server 4 Study Guide, 3rd edition Seattle: Amazon Press.

[11] Govanus, G. (1998). MCSE Exam Notes: TCP/IP for NT Server 4. Seattle: Amazon Press.

[12] Schauer, H. (1992). "An Internet Gatekeeper. USENIX Proceedings," UNIX Security Symposium III;

[13] Stewart, J.M. (1998) MCSE Guide to Microsoft Proxy Server 2.0 Seattle: Amazon Press.

[14]Chapman, B. D. (1992) "Network (In)Security Through IP Packet Filtering." USENIX Proceedings, UNIX Security Symposium III.

[15]Garfinkel, S. & Spafford, G. (1991) Firewall Machines. Practical UNIX Security. Sabastopol, CA: O'Reilly and Associates, Inc.,

[16] Bach, M.J. (1986) The Design of the Unix Operating System New Jersey: Prentice-Hall, Inc.