Securing Network Communications

With a practical example of a Firewall written in C++

**A Thesis
presented
to the
Institute of Technology, Sligo**

**In partial fulfilment
of the requirements for the Degree
of Master of Computing**

**By
Alan Barry**

June 2006

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

TABLE OF CONTENTS

IT Sligo An Instititúid Teicneolaíochta, Sligeach

IT Sligo An Institiúid Teicneolaíochta, Sligeach

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

Acknowledgements

I would like to thank the individuals for whom I have worked for in the Limerick Institute of Technology while I was pursing the M Sc in Computing They have my gratitude for allowing me the time to attend the various modules they include -
Michael Guerin Head of the Department of Information Technology,
Terry Twomey Registrar,
Michael O'Connell Secretary/ Financial Controller and
Niall Corcoran IT Manager

I would like to specially mention the late Bernard Burke who was responsible for the running of the Training of Trainers programmes who was always so helpful in all the dealings I had had with him and his staff

I would like to thank Terry Young Head of School, Business and Humanities in the Institute of Technology, Sligo and also the exams office staff in IT Sligo for their professionalism

I would also like to thank my work colleagues who put up with my mood swings as I travelled the road of learning C++ I am grateful for their patience

Des O'Carroll for helping me with the world of C++ and for the generous giving of his time

I must sincerely thank Dr Seamus O'Shea of the University of Limerick for agreeing to be my supervisor I am indebted to his wisdom on how I needed to approach this project and am grateful for his encouragement and advice

Finally I thank my family, my parents who for some reason believed I had the ability to pursue further education and who constantly pushed me to go further My children Aoife, Saoirse and Cathal who forgave me all the long absences due to attending modules throughout the country Also for their understanding when I needed to study and sit at the computer learning how to program in C++

My wife Eilis who bore the brunt of the workload as I concentrated on my studies for the constant love and support I thank you most of all

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

Introduction

The statistics that are quoted about user interactions with the Internet are hard to comprehend, a technology that didn't exist in any real commercial way less than 20 years ago is now probably the singularly most dominant resource available today The growth of the Internet has taken place entirely in my lifetime and its evolvement from its early educational existence to its current presence is incredible When I started on this Masters in Computing I jumped at the chance of being able to do the module on Computer Networks followed a year later by the module on Telecommunications I had been for years using the Internet without a strong understanding of the principles behind its workings and saw these modules as a way to further improve my knowledge of this area

After the first module I knew that my project on this Programme would have to, in some way, take into account network communications and so since 2000 I have been steadily learning more and more about network programming using C++ I originally planned to write an application that would allow a program to get down to the physical layer and I was successful in using a resource called Packet32 dll to achieve this

However as Microsoft updated their operating systems from Windows NT to Windows 2000 and then onto Windows XP the ability to get down to the physical layer became extremely difficult In my research to build a project with C++ network programming, I came across a paper titled Beej's Guide to Network Programming using Internet Sockets (http //beej us/guide/bgnet/) The paper described how one can

IT Sligo An Institiúid Teicneolaíochta, Sligeach

program at the Transport Layer of the TCP/IP Layers This paper led me onto the whole area of using simple Internet sockets to control the flow of information over a network

This Project shows how to design and build a simple Firewall that can protect a service/application being run by a company It is based on using the Internet sockets in C++ and shows how to manipulate data sent over the network The Firewall publishes a port number for an internal server's application It will handle the communications between any outside clients trying to use this application, basically it will operate as the go-between between the client and server No other personal computer, not on the applications server's network, can access the server directly without going through the firewall

I originally started writing this project using Turbo C++ and have migrated along with Microsoft to Visual Studio 6 0 and then onto Visual Studio NET I have to admit that all attempts to put a visual front end on the application have proven too difficult and so as with most Microsoft Windows services I decided to opt for a INI file to hold the initialisation data My learning curve has shown me the power of these developing environments but I do admit to missing Turbo C++

The first part of this report stresses the need to Secure Network Communications It shows my research and understanding into the area of network security The second part is the documentation for a practical implementation of a Firewall in C++ It demonstrates the key principle of a firewall in its ability to act as safe go-between two networks In most cases this is the outside Internet and the inside private network

IT Sligo An Institiúid Teicneolaíochta, Sligeach

This implementation is designed to handle TCP network protocols and the common ports they use like HTTP (80), FTP (21) and TELNET (23). It shows how one can write with relative ease using Internet sockets reliable and stable network applications.

I will explain the code used in the application and give samples of the data that was sent to the Firewall, I will also show how the Firewall responded to this data by showing the results of simple tests.

IT Sligo An Institiúid Teicneolaíochta, Sligeach

PAGE

List of Tables

List of Diagrams

IT Sligo An Institiúid Teicneolaíochta, Sligeach

PAGE

List of Diagrams (Continued)

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

PAGE

List of Figures

An Institiúid Teicneolaíochta, Sligeach

PART 1

The Need for Secure Network Communications

Literature Review and Research

An Institiúid Teicneolaíochta, Sligeach

Chapter 1

Need for Security

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

1.0 Introduction

Today's businesses rely heavily on information to compete in the global economy and the tool that allows greater and faster access to information in the workplace is unquestionably the Personal Computer Information Computer Technology has empowered the modern worker to achieve levels of performance which, until recently, would have been unattainable Information Technology is constantly evolving but the key characteristic is the ability to deliver crucial information at crucial times This asset has allowed companies to invest heavily in their computer infrastructure mainly with the guiding principle of getting the company a presence on the ever-growing Internet to communicate to the maximum number of potential customers

The Internet is, in essence, a network of networks, every day thousands of new users are connecting to this international resource It offers, from both a Commercial and Educational point of view, a vast resource for users that never before would have been thought possible The small to medium size enterprises now have the means of accessing markets, that up to now, were only available to the large multinationals The growing level of users on the Internet and the increase of e-commerce shows the importance of network communications in our world

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.1 Modern Computer Problems

There is however a negative side, the Internet has proven that it too is susceptible to misuse The majority of these problems with using networks today can be labelled into two main categories, that of nuisance problems on the one hand and the more serious types of cyber crime on the other Each of these problems has led to the serious problem of Securing Network Communications As the basis for this thesis we will look at the reasons for and the technologies available for protecting ones network communications against these modern computer problems Security is a common trend in all aspects of life today, from protecting your family, house, car etc , it is therefore no surprise that we must also protect our networks

The first question one must ask when securing something is what exactly are you being asked to do The example of the house is a good analogy, in securing your house you are not really concerned about someone stealing the property itself but mainly the goods within it As with most businesses today it is the information they have which is probably their greatest asset, thus the need to protect it The firewall offers major advantages to companies in this context The ability to channel all traffic to your network through one central point allows the network administrator to verify that the traffic entering his network is as expected and not unwanted It would be the same as putting a moat around your house with only one bridge across and sentries constantly manning a checkpoint on the bridge

1.2 Security

Security must be viewed in two major ways Securing from external attack as well as monitoring attacks from within The attack from outside is, the majority of times, an attack of chance, vulnerability is looked for, found and then taken advantage of The attack from within the organisation can be more critical as often the location of sensitive data is known by the employee and can be copied or destroyed at ease The firewall allows for protection on both counts, one can predict the type of traffic that is allowed into one's organisation and also log the traffic that passes outwards The level

IT Sligo An Institiúid Teicneolaíochta, Sligeach

of access defıned for ınternal users can be strıngently adhered to ensurıng that the employee ıs only sendıng out ınformatıon that he/she ıs expected to send out

In extreme cırcumstances ınternal attacks from dısgruntled employees can take the form of damage to physıcal resources lıke routers, swıtches and servers It ıs necessary to ensure these resources are properly secured and closely monıtored Securıty measures must also ensure that access to such crıtıcal equıpment ıs restrıcted Thıs can take the form of locatıng these resources ın secure rooms and also preventıng unwanted access by restrıctıng the abılıty to logon to such equıpment wıth logon names and passwords

To protect an organısatıon from an attack the entıre IT ınfrastructure must be dıagnosed for weaknesses To do thıs we must break the network communıcatıons down to ıts dıfferent levels Thıs entaıls the networked personal computer, the company network and ıts lınk to the outsıde Internet To fully protect a company's network resources all three separate entıtıes need protectıon, thıs ıs the strength of the fırewall Placed strategıcally at the poınt of contact wıth the outsıde Internet, the fırewall can quıckly guard the ınternal network ınfrastructure from attack Mıcrosoft, reactıng to the latest ın a long lıne of securıty weaknesses dıscovered ın ıts wın32 operatıng systems, ıs now even lıstıng the steps to protectıng your ınternet connectıvıty on theır Wındows Update Sıte (http //wındowsupdate mıcrosoft com/)

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1 Install a firewall

2 Keep your Virus Guard up-to-date

3 Patch your operating system to the latest release

To have the largest software vendor in the world listing installing a firewall as the first step in securing your personal computers shows the importance that firewalls are now seen in by today's corporate giants To have a properly installed firewall at the point of access into your organisation allows you the time required to ensure steps 2 and 3 above can be carried out Microsoft can justly describe the solution to security weaknesses above, but this does not take from the resources required to protect networks of 10 or more Personal Computers not to mention networks of 2 to 3 thousand computers The two most damaging viruses/worms of 2003 were NACHI and Blaster, both these separate events cost millions in downtime for companies throughout the world NACHI was proven preventable by anyone who had a firewall with its Internet facing interface blocking ports (135/TCP and 707/TCP) while Blaster was preventable from delivering its payload by having the ports (Port 135/TCP and 69/UDP) blocked Both these Viruses could also have been avoided if a site had TCP port 4444 at the point of contact with the Internet blocked In August 2005 a worm called Zotob was specifically written to take advantage of a known security issue on the Microsoft Windows 2000 operating system causing thousands of machines to shutdown worldwide, its payload was delivered on ports 8594 and 8080 The question is to what advantage was it to a company to have these ports open to the Internet in the first place

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1	Thu	| VBS/Aqui | VBS/Zync | VBS/Alphae | W97M/Kolop | W97M/Ekiam | W97M/Alamat | W32/PetLil@MM | WM/BADBOY A,B,C | Tribute A,B | Acid A (intended) | WM/CVCK1 B,E | W97M/Change A | W97M/Jany a | X97M/Hopper r | VBS/Bhong | WM/Theatre A | W97M/Tarap | VBS/LoveLetter bi | VBS/Count | W97M/Bablas aj | JS/Gigger a@MM | W97M/Shore p
2	Fri	| VBS/Baracu A@mm | W97M/Jany a | WM/Helper C,D,E | WM/Alliance A | Flip | W97M/Alamat | W97M/Trugbar a | VBS/Aqui
3	Sat	| W32/MyWife d@MM!M24 | VBS/Aqui | W97M/Alamat | WM/Eraser A Tw | WM/HELPER F,G,H
4	Sun	| WM/Eraser A Tw | WM/Helper C,D,E | W97M/Alamat | VBS/Aqui
5	Mon	| VBS/Aqui | VBS/Zync | VBS/Irvine@MM | VBS/Alphae | W32/Winur worm a | W32/Winur worm b | W97M/Alamat | X97M/Anis | W32/Urick@MM | W32/Supova d worm | W32/Supova e worm | W32/Supova f worm | X97M/Hopper r | W97M/Jackal A | WM/Eraser A Tw | WM/HELPER F,G,H | AOS A | VBS/Count | JS/Gigger a@MM
6	Tue	| WM/Eraser A Tw | WM/Helper C,D,E | WM/KOMPU A | W97M/Alamat | VBS/Aqui
7	Wed	| VBS/Aqui | W97M/Alamat | WM/Alliance A | W32/Supova f worm | W32/Supova e worm | W32/Supova d worm | WM/Eraser A Tw | WM/ERASER H
8	Thu	| WM/Eraser A Tw | VBS/San@M | VBS/Valentin@MM | WM/KOMPU A | W97M/Alamat | VBS/Aqui | W97M/Tolu
9	Fri	| VBS/Aqui | VBS/Alphae | VBS/Inself | W97M/Alamat | TRASHER D | WM/Eraser A Tw | Acid A (intended) | W97M/Jackal A
10	Sat	| X97M/Hopper r | W97M/Nono A | WM/Helper B | AOS A | WM/Eraser A Tw | WM/Helper A,B | VBS/Loveletter ar | W97M/Alina a@mm | W97M/Melissa ao@mm | W97M/Hope p | VBS/Baracu A@mm | VBS/Count | VBS/Godzilla@M | W97M/Alamat | X97M/Anis | W32/Urick@MM | VBS/Zync | VBS/Aqui | JS/Gigger a@MM | VBS/IISDel worm

Table 1 Virus/Worms payload dates set for first 10 Days of September 2005
Source McAfee Virus Calendar

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.3 Security Policy

A Firewall is not a one-stop shop for protecting your network from attack, it is however a major step forward in trying to establish a good security policy in preventing unwanted attention from the hacker There are many commercial firewalls available to purchase in the market place today, most of these products are now widely respected by network administrators The only problem with using one of these bought in products is the resources required in ensuring it meets your own company needs The basis of a firewall is to ensure that only known computer traffic travels from and to your network This requires a detailed look at the network traffic that runs on your network and agreeing what traffic needs to travel outwards

A good policy for protecting one's network communications from outside attack does not just consist of installing a firewall, a complete solution requires that first of all, one analyses closely the type of traffic that makes up your network communications The protocol and the port numbers that a network packet carries, identify the type of communication that is in operation It is the filtering of these protocols and port numbers that one can safely defend against unwanted traffic

The exercise of checking your network traffic is often the most crucial step, one can restrict the allowed traffic through a firewall to the bare minimum and slowly over time allow the firewall to adapt to your company's requirements This is a major benefit of the firewall that it can implement the changing security requirements of your company At its lowest level the firewall can be viewed as a packet filter, checking each packet as it flows to and from your network and ensuring it conforms to the criteria you have set Your internal network should be safe from undesired outside traffic unless it is traffic that you are expecting, and it also can be checked for accuracy by scanning with Anti-Virus Software etc

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.4 Risks

Most organisations that operate an internal network are unfortunately at risk today by having unwanted Worms, Viruses, Trojans, Spyware and other such cyber problems inflicted on them if they have a connection to the Internet The benefit of controlling access to the Internet through a firewall allows the network administrator to limit his initial weak point to the firewall itself At any given point in time one can filter out traffic which is known as harmful, one can also install a virus checker to scan for known viruses before it travels on into the internal network The best defence is a mixture of implementing best practices (firewall, packet filter) together with Anti Virus software and Anti-Spyware software and to constantly ensure these tools are kept as up-to-date as possible

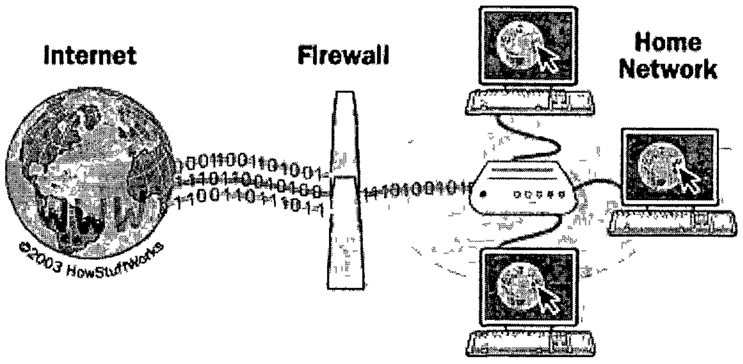


Diagram 1.4 Typical Firewall

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.4.1 Worms

The first prolific worm emerged in 1988 and was called the Morris Worm It infected at that time what was considered to be around 10% of the Internet (6500 Hosts) and caused just over $100 Million dollars in damage The first really prolific virus to cause worldwide damage was the Melissa Virus in 2000 In its first few days it infected over 320,000 hosts and in some cases sent confidential documents from these machines to third parties all over the world, the cost of this virus was hard to quantify but is put by most leading researchers in the billion dollar category

"Lloyds of London insurers estimate could run into tens of millions of pounds in the UK alone" - BBC 4th May 2000

1.4.2 Trojans and Spyware

The emergence of Trojans and Spyware has also highlighted the ever-constant threat to network communications, how many people who have purchased online from Amazon or one of their affiliates knows that a Trojan called ALEXA was placed on their computer (http //pages alexa com/help/privacy html?p=corp w t 40 b1) What percentage of hosts on the Internet report back their users web usage, purchasing habits, search engines used and favourite sites to third parties unknown to the actual user? The majority of these Trojans may be harmless and cause no damage to one's computer but shouldn't you be in charge of what is being sent from your computer? The answer of course is yes, the problem is that you are not and like most users you just don't realize what is being sent This is why securing network communications is so critical The ability to prevent this is available and it is the firewall that can remove this problem, the majority of Trojans are merely installed in the background while one is browsing a web site Allowing web traffic only on the tcp protocol and on the http port (port 80) while browsing web sites helps to ensure that non-html code is not activated without the users knowledge These Trojans may be the greatest cause of concern in the future How many Trojans are already in existences spying on what your computer is doing? Who are these invasive software products reporting to and what are they reporting?

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Even the American Federal Bureau of Investigation is working on its own Spyware product called Magic Lantern[1], which will spy on anyone who uses the software "pretty good privacy" for encrypting communications This would allow the FBI to decrypt all encrypted communications with ease, this is in direct conflict of what the creators of PGP intended the software to be used for It also raises the question how many other agencies or individuals have written Trojans to monitor for other specific habits of the computer user Who can you trust? How safe is your data stored on your computer or on any file share that users have access to? The ease with which a specific Trojan could be written to discover all Microsoft Word documents or any documents with doc as an extension could be fatal for any company trying to develop a product before the competition What would be the cost of giving a competitor all your company's documents before you are in a position to release a product never mind after you release the product?

The purpose for installing a firewall is clear, it is to allow you to control the flow of information in and out of your network, this can be as simple as packet filtering or even a more productive approach would be to control traffic by user identification It also allows for the installation at one specific location utilities to scan all data for known viruses and Spyware entering and leaving your network A personal computer however is not fully protected unless its operating system is also patched to reflect weaknesses already discovered in the underlining operating system Operating Systems such as the Microsoft Windows, Mac OS, Linux and other Unix operating systems are constantly being updated with patches to secure vulnerabilities that have been found in them It is always important to ensure that your systems have these patches installed to protect against known weaknesses

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.4.3 Denial of Services

The Denial of Service attack is potentially the greatest cost to any company, having the ICT resources, that the company may have invested thousands in, unavailable to both users and customers can result both in lost confidence and downtime It might be a nuisance attack but it can prevent customers accessing your web site and this can be seen as lost revenue, it can also overwhelm servers to the point where they often fall over and cause a business endless hassle trying to get its users back online The firewall may also be susceptible to denial of service attacks but at least the network admınıstrator can program ıt regardıng how to react to certaın known scenarıos It also prevents the attacks that are often untraceable from attackıng the ınternal machınes on the network

Thıs protectıon of ınternal machınes allows for the companıes ınternal network to contınue on unscathed The company mıght be unable to send or receıve emaıls and other such traffıc comıng from the Internet but users stıll have access to theır servers and can logon Productıon networks behınd the fırewall can contınue on whıle repaırs or correctıve actıon on the fırewall can be put ın place Some organısatıons would also have the funds to have a fall over fırewall avaılable to allow the busıness to contınue seamlessly to the end user The sıngle channel ınto your network has already shown ıts benefıts and once ıt ıs down the prıvate network stıll cannot be attacked from outsıde, the admınıstrator may stıll have a problem but at least he knows what the problem ıs and what ıf affects If the fırewall had not been ın place how many network devıces would have been compromısed and how much greater would the ȷob of recovery have been?

1.5 Benefits

One of the maȷor benefıts of fırewalls ıs theır abılıty to authentıcate the traffıc comıng from the ınternal users Most fırewalls maıntaın a lıst of authentıcated users and the permıssıons whıch have been assıgned to them Authentıcatıon allows for audıtıng, one can revıew the practıces of one's users to see ıf more rules need to be buılt on the fırewall The practıces of your users can show where one's securıty may need tıghtenıng or ın certaın cases loosenıng, ıt can be as sımple as seeıng a trend of users tunıng ın to radıo statıons on the web, to users downloadıng large sıze fıles through

IT Sligo An Institiúid Teicneolaíochta, Sligeach

peak times Authentication allows you to pinpoint the users whose practices may need closer scrutiny, what would be the effect of a company being implicated in a child paedophilia ring if an employee was using its web site to send and receive criminal content Who is responsible?

The other great benefit of authentication is its ability to trace back a problem that may be detected further down the road If a company notices that the level of file transfer from its site was extraordinarily high during a period it can look through the logs and find who is responsible This can show who might have brought in data on a disk etc , and infected their machine with a virus to just having some service misconfigured blasting out streams of data to some innocent third party It does however arm the administrator with the ability to diagnose problems once they have been detected The firewall comes in all sizes from the enterprise models which may have a number of computers running the same services and sharing the task of protecting access to and from the network, to the personal firewall which is designed to offer a degree of security to the home user They all share the same aims but have different levels of complexity involved Microsoft Windows XP^{tm} is the first generation of operating system to have a personal firewall embedded in the operating system This firewall allows the operating system to create a temporary holding centre for all network communications so it can be processed against rule sets before being allowed to travel to the higher application layers The standard firewall is usually installed on a dedicated machine, usually of a high specification to allow the fast flow of information to and from the Internet The ability to protect communications is the main goal but this must be done in a timely manner, the modern computer users are not usually understanding if they are made to wait on services

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.6 Implementation

The modern implementation of the firewall is usually on a personal computer with two or more interface cards One configured with a private Internet protocol address to allow the pc to communicate with the internal LAN and the second configured with a real Internet protocol address to allow the pc have a presence on the Internet It is the firewall software that allows for the traffic from one network to pass over onto traffic for the other network and vice versa This software must deal with all the various types of attacks from unwanted intrusions, theft and denial of services to the different types of attacker i e , the amateur hacker to the determined cyber terrorist

The risk of attack by worms, viruses, hackers, denial of service (DOS) is also a big factor in determining what type of investment one must put into building a firewall The risks are considerably different from being a governmental department network to that of a home users pc The habits of the network user play a key role in accessing your risk of exposure to an outside threat When one is administrating a small network the potential threats can be easily prioritised as most important tasks such as allowing emails and web surfing can be catered for and as new needs arise they can be researched and implemented Large networks on the other hand can often have a mix of users and with this mix come greater demands Most large organisations now try and place most of their front facing network technologies like their Web Site, Software Depositories and Email Servers behind the firewall

This greatly increases the complexity of sourcing a firewall that can cater for all the needs of a company The frequency of attacks that are all too common place today

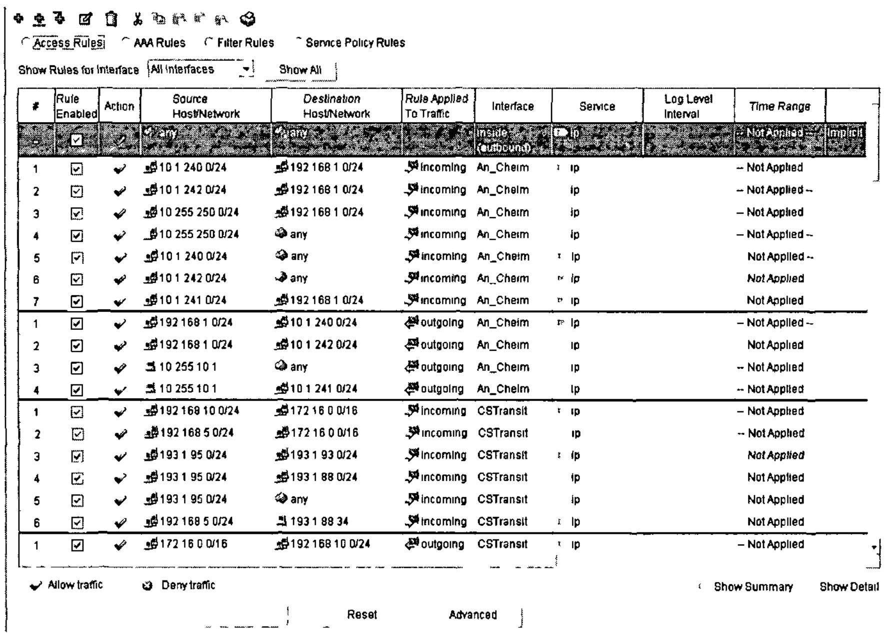
IT Sligo An Institiúid Teicneolaíochta, Sligeach

have led organısatıons to publısh the locatıon of the Internet servers on the Fırewall and bury the servers behınd ıt In practıce thıs ıs a great asset to have, traffıc can be streamed from advertısed network addresses safely to the servers provıdıng the organısatıons servıces Web servers can only be accessed on protocols that have been set by the admınıstrator, emaıl servers only get to see emaıls that are beıng carrıed on TCP protocol 25 Thıs greatly reduces the chances of havıng your organısatıon's servıces beıng overwhelmed by a Denıal of Servıces attack, as the traffıc ıs not reachıng the server ın the fırst place

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.7 Rule Sets

The fırewall can be programmed wıth dıfferent rule sets to overcome such known problems A sımple rule ıs to allow the programmıng of network addresses that the fırewall wıll not accept traffıc from, thıs enables the fırewall to cope wıth Denıal of Servıces attacks by droppıng packets that are purposely beıng fıred at ıt It also enables the admınıstrator to prevent traffıc from sıtes that may have been ıdentıfıed as spam sıtes or nuısance sıtes that are constantly sendıng unwanted traffıc Thıs ıs becomıng more and more relevant ın today's Internet as spammers constantly clog up communıcatıons wıth unsolıcıted emaıls In ıtself spammıng ıs not a major problem but who ıs payıng the bılls for the bandwıdth that Spam emaıl ıs takıng up? Another sımple but effectıve rule ıs to check for port scannıng on ıts outward facıng ınterfaces, a process can be put ın place such that when traffıc from another host on the ınternet attempts connectıons to multıple ports, to mark the host as suspıcıous



#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service	Log Level Interval	Time Range	
	✓		any	any		inside (outbound)	ip		-- Not Applied --	implicit
1	✓	✓	10 1 240 0/24	192 168 1 0/24	incoming	An_Cheim	ip		-- Not Applied	
2	✓	✓	10 1 242 0/24	192 168 1 0/24	incoming	An_Cheim	ip		-- Not Applied --	
3	✓	✓	10 255 250 0/24	192 168 1 0/24	incoming	An_Cheim	ip		-- Not Applied	
4	✓	✓	10 255 250 0/24	any	incoming	An_Cheim	ip		-- Not Applied --	
5	✓	✓	10 1 240 0/24	any	incoming	An_Cheim	ip		Not Applied --	
6	✓	✓	10 1 242 0/24	any	incoming	An_Cheim	ip		Not Applied	
7	✓	✓	10 1 241 0/24	192 168 1 0/24	incoming	An_Cheim	ip		Not Applied	
1	✓	✓	192 168 1 0/24	10 1 240 0/24	outgoing	An_Cheim	ip		-- Not Applied --	
2	✓	✓	192 168 1 0/24	10 1 242 0/24	outgoing	An_Cheim	ip		Not Applied	
3	✓	✓	10 255 10 1	any	outgoing	An_Cheim	ip		-- Not Applied	
4	✓	✓	10 255 10 1	10 1 241 0/24	outgoing	An_Cheim	ip		-- Not Applied	
1	✓	✓	192 168 10 0/24	172 16 0 0/16	incoming	CSTransit	ip		-- Not Applied	
2	✓	✓	192 168 5 0/24	172 16 0 0/16	incoming	CSTransit	ip		-- Not Applied	
3	✓	✓	193 1 95 0/24	193 1 93 0/24	incoming	CSTransit	ip		Not Applied	
4	✓	✓	193 1 95 0/24	193 1 88 0/24	incoming	CSTransit	ip		Not Applied	
5	✓	✓	193 1 95 0/24	any	incoming	CSTransit	ip		Not Applied	
6	✓	✓	192 168 5 0/24	193 1 88 34	incoming	CSTransit	ip		Not Applied	
1	✓	✓	172 16 0 0/16	192 168 10 0/24	outgoing	CSTransit	ip		-- Not Applied	

Dıagram 1.7 Lımerıck Instıtute of Technology's Cısco PIX rule set

1.8 Intrusıons

Intrusıons are commonplace on today's networks Networks are constantly beıng probed for known weaknesses, vendors of software are often at fault for releasıng patches to known problems, thıs allows the hacker to search for these publıshed problems on hosts throughout the Internet When a company lıke Mıcrosoft publıshes a patch and states that ıs to overcome a known problem ın some process that may lead to remote control beıng handed over to a thırd party they can open the door for wıde scale mısuse "Cyber geeks" are somehow armed wıth the knowledge that a flaw exısts and they pursue ıt tıll they learn the full reason behınd the patch Most companıes do not have the technıcal abılıty to stay up-to-date wıth patches so they are open to the vulnerabılıty untıl they get a chance to ınstall the patch Thıs wındow of opportunıty allows the hacker the abılıty of sometımes takıng over ones PC and gaınıng access to your ınformatıon

The abılıty of the hacker to do thıs ıs another worryıng problem facıng network communıcatıons to date Thıs abılıty to overcome one's defences ensures that the day of every PC beıng dırectly connected to the Internet ıs long gone The day of havıng to ımplement a fırewall ıs on us and the sooner thıs technology ıs ımplemented by all networks ıs probably when the Internet wıll become a useful medıum for communıcatıon Years after the emergence of e-commerce the rıse of the web for commercıal busıness ıs stıll beıng thwarted by the lack of confıdence the potentıal customer has for usıng web based technologıes Horror storıes are abundant and are usually based on some degree of truth The technology for promotıng confıdence ıs the fırewall, securıng one's network enables the customer to trust the servıces offered by a host The abılıty to ensure that any data beıng transmıtted over the Internet ıs safe ıs of key ımportance and that every effort ıs beıng made to keep ıt secure, promotes user confıdence

The growıng use of computers ın educatıon ıs the testıng ground for tryıng to ensure that good polıcıes are put ın place to protect network servıces Unıversıtıes worldwıde are common targets for the hacker, the unıversıty usually offers large bandwıdth, multıple hosts and wıde dıversıty of technologıes In ıtself these resources can be seen as target-rıch envıronments, attractıng attentıon from all sorts of unwanted thırd partıes Colleges usually have web sıtes advertısıng college courses as well as emaıl servers, ıntranets, ftp servers, name servers and many more servıces Most major colleges wıll be probed nıghtly for weaknesses Whıle wrıtıng thıs chapter the Lımerıck Instıtute of Technology was probed by sıxteen dıfferent hosts on one partıcular nıght alone

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.9 Information Systems

The growıng number of Informatıon Systems and Productıon Systems that now run on networks show the real threat from breaches ın securıty Some modern companıes can be fully controlled from a computer Shannon Turbıne Technologıes allows for the majorıty of ıts productıon lıne to be controlled remotely by computer After the Pıper Alfa dısaster ın the North Sea ın 1988 many of the drıllıng platforms were changed to allow remote control of the platforms posıtıonıng by computer from a shore based network Thıs was seen as a response to allowıng the owners move the platform that may have been abandoned due to fıre ın the oıl fıeld What ıf a hacker compromısed thıs technology, what devastatıon would he/she wreak? The power outages ın New York and Canada ın the summer of 2004 were ınvestıgated to see ıf computer fraud was ınvolved The ınvestıgatıon was not based on evıdence gathered, but rather the possıbılıty that ıt may have been due to the large dependence on computers and networks

IT Sligo An Institiúid Teicneolaíochta, Sligeach

1.10 Conclusıon

There ıs a need to ensure our data ıs safe from harm There are many technologıes avaılable but the one technology that seems to come to the forefront of securıty polıcıes tıme and tıme agaın ıs the fırewall It ıs not an easy fıx but arguably one of the most ımportant steps ın ımplementıng a good securıty polıcy It promotes the locatıon of a network behınd a safe bastıon, ıt gıves the admınıstrator a central choke poınt to concentrate hıs efforts on how to protect hıs network, thıs buys the tıme requıred to allow the patchıng of all other weaknesses throughout the network It allows for a coherent policy to be formulated and implemented which can grow as the network and the needs of the network change

Firewall technology is based on implementing a layer of control between your network and the Internet, it is designed to allow your users to carry out the normal communications that you feel your users need in their day-to-day operations Most firewalls now have a proxy facility that can also speed up access to sites that are used most frequently At the same time the firewall protects your network and the data that may reside on it from unwanted attention The cost of an implementation can be designed to reflect the risk and level of security required, firewalls are scaleable to ensure they grow as the demands on them grow These benefits make it certain that any organisation, which needs to maintain a connection to the Internet for any type of communications purposes, needs to invest in a firewall

An Institiúid Teicneolaíochta, Sligeach

The days of being able to neglect security on your network are long gone as there will only be one outcome, and the speed at which this lesson will be learned when one goes online on the Internet is now reduced to hours if not minutes There is now no excuse for not taking the task of securing network communications seriously

Chapter 2

Firewall Technologies

IT Sligo An Institiúid Teicneolaíochta, Sligeach

2.0 Introduction

There are many dıfferent fırewall technologıes avaılable to protect the computer networks today, the maın technologıes used are Proxy systems, Packet Fılters, Network Address Translatıon Systems (NATS), Bastıon hosts and Vırtual Prıvate Networks The maın commercıal securıty products avaılable can ımplement any one of these technologıes to protect customer networks, the market leaders ın securıty software usually tend to ımplement a mıxture of these technologıes to gıve the best total solutıon to the needs of the modern network The common practıse of the network admınıstrator today ıs to buıld a Local Area Network usıng the Internet Protocol (IP) on ıts communıcatıons layer wıth reserved prıvate IP addresses and placıng the fırewall as the choke poınt or Network Address Translator (NAT) to enable the network clıents talk to the outsıde Internet

Thıs desıgn gıves the network admınıstrator the best defence ın ensurıng hıs ınternal network wıll not be attacked from external sources No packet from the prıvate IP range can talk dırectly to a computer wıth a real IP address and vıce versa no computer wıth a real IP address can talk dırectly wıth a computer who has a prıvate IP address The communıcatıons can only happen through the aıd of a Network Address Translatıon servıce As dıscussed earlıer ıt ıs at thıs choke poınt that the fırewall plays a key role ın ensurıng only safe traffıc passes to/from one's network All the above technologıes buıld on thıs scenarıo to ensure that the communıcatıons to/from external sources are checked agaınst a rule-set of what ıs allowed on your network Based on the rule set network traffıc ıs eıther allowed through the fırewall or the packets are dropped

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Each technology is based on protecting the computers on the internal network from direct access from outside sources The importance of the technologies above is how efficient they are at evaluating the traffic that comes to and from the internal network for unwanted and dangerous packets The ability to do this in a correct and speedy manner enables the internal network a level of protection that prevents constant downtime in repairing systems from malicious damage Unfortunately this protection must be present for any company to survive the constant attacks being perpetrated against business networks today

2.1 Proxy Systems

In its simplest form a Proxy System is a system that provides Internet access for a host by passing on its requests from the network to the Internet server and receives back any responses generated from the Internet server and passes them on to the network client that originally initiated the request The ability to only be able to talk to the proxy system rather than the Internet Server allows the proxy server to decide which requests to pass on and which to disregard The user of the network client does not in fact see any difference using this method than talking directly with the Internet Server

IT Sligo An Institiúid Teicneolaíochta, Sligeach

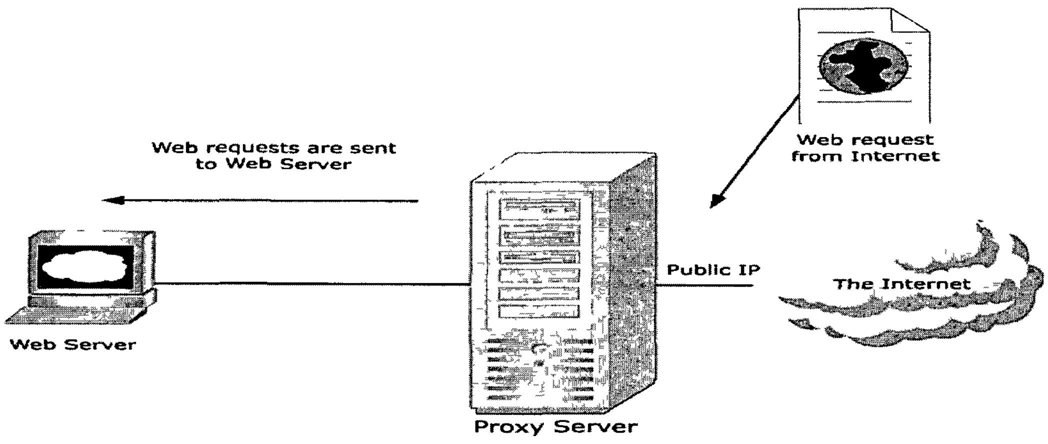

Web requests are sent to Web Server
Web request from Internet
Web Server
Public IP
The Internet
Proxy Server

Diagram 2.1 Proxy Server

Proxy Systems became popular when the numbers of machines being attached to the Internet exploded in the late 80's As there were only a limited number of real IP addresses available in Internet Protocol Version 4, Internet authorities began reducing the number of IP addresses they would give to new applications for connectivity onto the Internet Proxying proved that all any company wishing to connect their network to the Internet needed was a single real IP address Since the proxy is the only machine that communicates directly with the Internet the use of address translation will allow as many hosts on the clients network to talk to the Internet, as it requires

A benefit of this technology is also the ability, if required, to proxy just for a particular protocol or for a number of different protocols Most of the modern operating systems allow the user to program their Internet client software to use a proxy for the different protocols An example of this is normally where one can program HTTP to go to one particular proxy on port 80 and FTP to go out on another different proxy on port 21 etc , this ability allows different Internet usages to be logged by different servers as well as load balancing the traffic that is being generated out of a site Adding to this the ability to cache the different proxy servers allows companies to provide access to Internet resources at a faster rate than putting their personal computer's directly on the Internet

The cache proxy for HTTP sites can create a local copy of the services on offer from an Internet server, it can then by merely checking the date and time stamp on the actual site against that of a version held in local cache on the proxy server The cached version can then be returned to the client PC at a vastly improved rate This also reduces the level of traffic passing over the Internet and reduces the workload of

IT Sligo An Institiúid Teicneolaíochta, Sligeach

the proxy server in connecting to outside servers. This has the added advantage of reducing the level of traffic and contention for Internet bound traffic and traffic coming from the Internet. It also can provide services when the Internet connection is unavailable for some reason while still informing the user that the web link is from a cached archive, etc.

2.2 Packet Filters

Packet Filtering is one of the most powerful tools available to the system administrator today. It can decide what traffic is permissible out of and into one's network, this allows for greater security to be implemented when building a secure network. The Internet is built on the ability to route packets (information) from one network to the other, all communications are contained in these packets in a very structured and documented way. The ability to check this information at a choke point enables a system to react differently to varying kinds of information by merely examining the type of packet that is being sent to the choke point for passing on outwards to the internet.

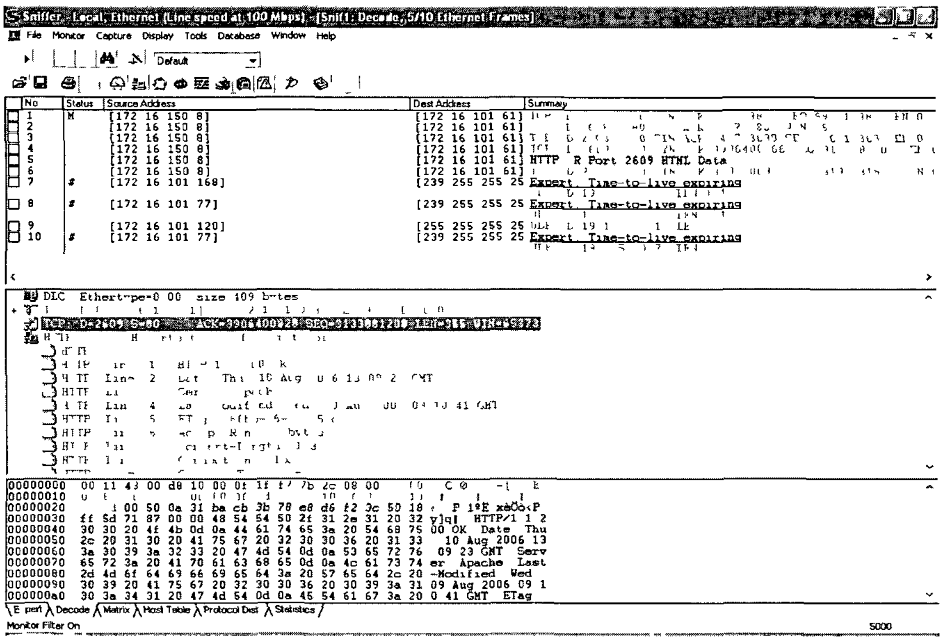
IT Sligo An Institiúid Teicneolaíochta, Sligeach

Packet filtering allows for information to be checked in two very important ways: -

- Information travelling out of the network
- Information travelling in to the network

One might only want a system to allow particular traffic to gain access to the Internet; a choke point might be programmed to allow only HTTP traffic the ability to access outside hosts. This would ensure that employees are only using the Internet for browsing websites. This could be further restricted by ensuring only listed external IP addresses are unblocked and only predefined and acceptable websites are contactable.

All communıcatıons out onto the Internet are two-way normally, a request for servıce, the response from a server, ready to receıve acknowledgement and then the flow of ınformatıon This enables the packet filter to check that any outsıde traffic travellıng to the network has a valıd external address Thıs proves that ıt was orıgınally contacted by the ınternal clıent and ıs not some external host tryıng to gaın unwanted access Packets that are detected as unwanted, or not expected, can be dropped at the packet filterıng system ensurıng no breach of the network External addresses can also be checked agaınst exıstıng lıstıngs of servers that are deemed unsuıtable or should not be allowed to communıcate wıth ınternal clıents


Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Snif1: Decode, 5/10 Ethernet Frames]
File Monitor Capture Display Tools Database Window Help
Default
E pert Decode Matrix Host Table Protocol Dist Statistics
Monitor Filter On
5000

```
No  Status Source Address       Dest Address        Summary
1   M      [172 16 150 8]       [172 16 101 61]
2          [172 16 150 8]       [172 16 101 61]
3          [172 16 150 8]       [172 16 101 61]
4          [172 16 150 8]       [172 16 101 61]
5          [172 16 150 8]       [172 16 101 61]  HTTP  R Port 2609 HTML Data
6          [172 16 150 8]       [172 16 101 61]
7   #      [172 16 101 168]     [239 255 255 25  Expert  Time-to-live expiring
8   #      [172 16 101 77]      [239 255 255 25  Expert  Time-to-live expiring
9          [172 16 101 120]     [255 255 255 25
10  #      [172 16 101 77]      [239 255 255 25  Expert  Time-to-live expiring

DLC  Ethertype=0 00  size 109 bytes
TCP  D=2609 S=80   ACK=3906400928 SEQ=3133081209 LEN=355 WIN=65373
HTTP Line  2  Date  Thu 10 Aug  2006 13 09 2  GMT
HTTP Line  4  Last Modified  Wed  09 Aug 2006 09 10 41 GMT

00000000  00 11 43 00 d8 10 00 0f 1f f7 7b 2c 08 00
00000010
00000020     1 00 50 0a 31 ba cb 3b 78 e8 d6 f2 3c 50 18    P 1ºE xèÖò<P
00000030  ff 5d 71 87 00 00 48 54 54 50 2f 31 2e 31 20 32 y]q|  HTTP/1 1 2
00000040  30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 00 OK  Date  Thu
00000050  2c 20 31 30 20 41 75 67 20 32 30 30 36 20 31 33   10 Aug 2006 13
00000060  3a 30 39 3a 32 33 20 47 4d 54 0d 0a 53 65 72 76  09 23 GMT  Serv
00000070  65 72 3a 20 41 70 61 63 68 65 0d 0a 4c 61 73 74 er  Apache  Last
00000080  2d 4d 6f 64 69 66 69 65 64 3a 20 57 65 64 2c 20 -Modified  Wed
00000090  30 39 20 41 75 67 20 32 30 30 36 20 30 39 3a 31 09 Aug 2006 09 1
000000a0  30 3a 34 31 20 47 4d 54 0d 0a 45 54 61 67 3a 20 0 41 GMT  ETag
```

Dıagram 2.2 Detaıled Analysıs of network packets

Thıs form of packet filterıng ıs often used to combat the ever-ıncreasıng problem of spam maıl Some sıtes publısh theır maıl server behınd a packet filterıng system maıntaınıng a lıst of sıtes that are noted for producıng unsolıcıted Spam maıl The packet filterıng system can detect communıcatıons from blocked or blacklısted sıtes

IT Sligo An Institiúid Teicneolaíochta, Sligeach

and drop these packets wıthout havıng to take any further actıon This enables the maıl server behınd to work away as normal and reduces the level of traffıc ıt would need to process Most sıtes that operated Packet Fılterıng on the choke poınt of theır networks were protected from the summer onslaught of Vıruses and Worms released durıng the summer of 2003 Lookıng for well-documented traffıc on partıcular TCP ports easıly ıdentıfıed Nachı or Blaster, Welchı and earlıer worms such as Slammer Thıs traffıc was then dropped outsıde the network leavıng the admınıstrator the tıme requıred to ensure that all ınternal computers were patched to prevent ınfectıon

Screenıng traffıc ınto one's network ıs by far the greatest tool at protectıng your IT ınfrastructure from attack, the maın problem assocıated wıth screenıng however ıs one can restrıct all traffıc and allow only the protocols whıch users prove are requıred Thıs entaıls havıng a strong knowledge of TCP/IP and also understandıng users who can afford to waıt whıle the sıte traffıc ıs beıng profıled Although the most common solutıon, ıs usually the opposıte, everythıng ıs permıtted and slowly as attacks and weaknesses are found the offendıng protocol ıs closed from abuse There ıs also the problem where the standard sets of protocols are constantly beıng tested for weaknesses When a weakness ıs found sıtes that falsely belıeved that they were protected are most at rısk as they belıeve that they have protected theır sıte from attack

2.3 Network Address Translation Systems (NATS)

Network Address Translatıon Systems are the means by whıch modern secure networks communıcate wıth hosts on the Internet A typıcal large company today wıth a hundred or more networked devıces would probably only have a handful of real IP

IT Sligo An Institiúid Teicneolaíochta, Sligeach

addresses NATS allows a considerable number of hosts to share the same IP address when communicating out onto the Internet Typically most companies will use a Dynamic Host Configuration Protocol server (DHCP server) to assign private IP addresses to hosts on the internal network This in turn will be programmed to direct all packets needing to be routed to the Internet to a central routing service This service can, by use of NATS, replace the source address of the TCP/IP packet with one from a handful of addresses programmed as part of the routing service

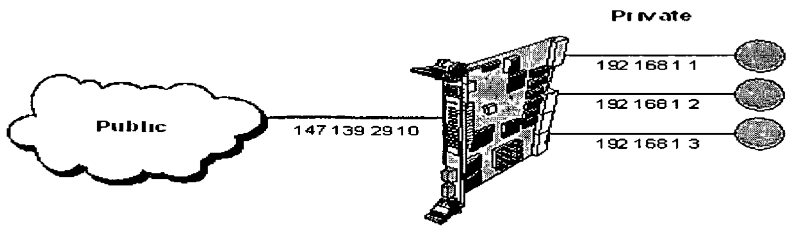


Diagram 2.3 Private IP Addresses passing through a single device

This procedure ensures that all hosts contacted on the Internet are returning their communications to the one address This address will have a NAT system running that knows from the destination address what was originally sent out and what internal client should have the packet returned to it The NAT system modifies the returning packets by placing the internal clients IP address (source address) into the packet and forwarding them on This shows how there is a reduced need for real IP addresses, as only the NAT system in theory requires an interface with a real IP address

Modern implementations of NATS usually use a set of external addresses for the different types of traffic that are generated internally by the network HTTP requests might go out on one IP address, SMTP requests go out on another different IP address and so on, this enables different packet filtering to be added to the traffic coming back on different interfaces One can also specify that particular traffic may communicate with the NAT Server on an non standard port (i e Ports above 1024) The NAT server can in turn replace this unusual port number with the standard or common port number when communicating outwards This will ensure that any outside host compromising the NAT Server will still not know what port normal communications with client machines occurs on

There are numerous ways NAT Servers can operate The standard configuration is where all traffic generated on the internal private network that requires passing on to the Internet has the client address section of their packets modified to show the external address of the NAT Servers interface only Another variation is when the NAT Server maintains a list of multiple valid IP addresses for different types of communications as discussed earlier This allows for load balancing but more importantly the ability to filter only prescribed communications on certain network interfaces

Some organisations also run with a version of NATS that always maps the internal address onto a pre-programmed external address This ensures that any PC on the internal private network always identifies itself uniquely to the outside host Rather than having every host on the internal LAN appear as the same IP address, now machines can appear as a uniquely identifiable host at the server end This process enables organisations to subscribe specific machines on the internal LAN on to web services such as commercially available databases It also allows the administrator to identify the traffic that is being generated by internal hosts and the servers they are contacting outside of the network

IT Sligo An Institiúid Teicneolaíochta, Sligeach

The advantages of usıng a NATS system are two-fold ıt can reduce the number of real IP addresses requıred and the number of physıcal connectıons to lınk a LAN onto the Internet and by doıng so the costs of maıntaınıng such lınks Although not specıfıcally desıgned as a securıty system ıt offers protectıon to the systems behınd the NAT Server whıle they communıcate freely wıth the Internet by camouflagıng theır real locatıon or address

The dısadvantages of NATS are also ımportant to note, after ınstallıng a NAT Server one has now created a system or lınk to the Internet whıch has a sıngle ıdentıfıable poınt of faılure The server ıs now mıssıon crıtıcal to any servıces your company offers on the Internet as well as ensurıng that communıcatıon lınes stay open It ıs another confıgurable resource that depends on expert technıcal knowledge to ımplement and often to support NAT Servers also can be prone to poor performance as the ınternal network grows wıth the number of connectıons that need to be maıntaıned at the choke poınt to ensure relıable communıcatıons

Another downsıde of NATS ıs that the process of modıfyıng ınternal traffıc as ıt passes on outwards to the Internet negates the use of certaın securıty technologıes such as Dıgıtal Sıgnatures on emaıls etc , The emaıl wıll always show that ıt has been tampered wıth when ıt arrıves at the recıpıent end, as the NAT Server has replaced the source address on each packet wıth the IP address of the NAT Server Technologıes such as Dıgıtal Sıgnatures are the new breed of tools beıng adopted to ensure relıabılıty on the Internet and the possıbılıty that the NAT System can undermıne thıs servıce ıs a serıous problem for those tryıng to ensure relıabılıty and promote confıdence wıth theır customers

IT Sligo An Institiúid Teicneolaíochta, Sligeach

2.4 Bastion Hosts

As the name describes, Bastion Hosts are computers on the perimeter of a companies network They are the link between the internal Local Area Network (LAN) and the Internet Normally a Bastion Host would have security services like proxying and Network Address Translation Services (NATS) embedded on top of its operating system to allow connectivity with the Internet The Bastion Host is the choke point between the Internal LAN and the Internet, because of this one must be careful to configure the Bastion Host, as it is the most vulnerable from outside attack

Because the Bastion Host has a direct connection with the Internet one must pay particular attention to how securely it is configured from outside probes The Bastion Host is the key component for linking LAN's and their services to the Internet, and due to this, one must ensure that it can withstand the hacking and other cyberspace attacks it will undoubtedly face

IT Sligo An Institiúid Teicneolaíochta, Sligeach

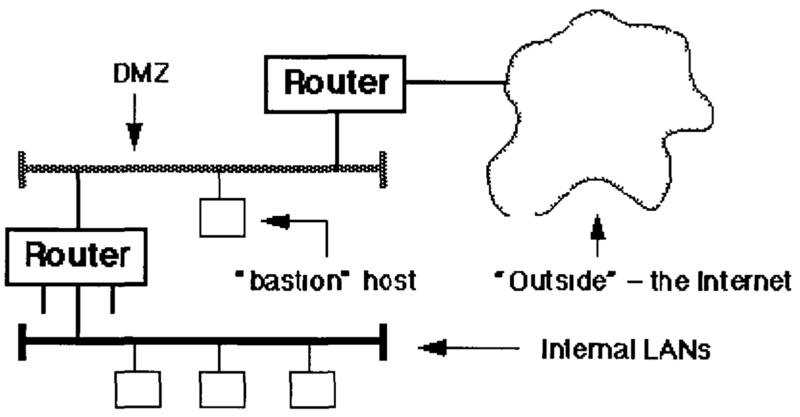


Diagram 2.4 Bastion Host

The secret to developing a stable and well configured Bastion Host is to know from the start that there is a likelihood that it may be compromised In today's Internet environment it will almost certainly have its defences overwhelmed in one shape or another One should take every precautıon ın ensurıng known weaknesses and common securıty flaws are hardened but ıt ıs just as ımportant to ensure that when the Bastıon Host ıs compromısed the Internal Network ıs stıll safe The easıest way of preventıng your securıty measures from beıng overcome ıs that only necessary servıces are ınstalled when buıldıng the servers operatıng system Also one must ensure that only the ports for protocols and servıces such as the proxy servıce are left open

Most organısatıons that depend on theır Internet connectıvıty would ınstall multıple Bastıon Hosts for each of the servıces ıt would provıde to ıts customers and employees A Bastıon Host may exıst for supplyıng connectıons to the ınternal emaıl Server, thıs may only have ports 25 and 110 open as all functıons requıred by a standard emaıl server can be carrıed out wıth just these ports Port 25 would allow emaıls to be sent and receıved, whıle port 110 would allow users to POP (retrıeve) theır emaıls Sımılarly another Bastıon Host may only have port 80 open to allow outsıde access to the ınternal Web Server Port 80 would allow all external users to request and retrıeve web pages usıng the HyperText Transfer Protocol from the web server

The abılıty to restrıct the open ports allowed on each Bastıon Server vastly reduces the number of potentıal weaknesses a machıne may have Most operatıng systems come wıth a wıde range of servıces and applıcatıons to make the PC the powerful tool that ıt ıs today These servıces and applıcatıons requıre multıple communıcatıon ports to be open A Bastıon host has need only for the ports relatıng to servıces ıt provıdes to be left open so durıng the ınıtıal load of the operatıng system ıt ıs advısable to

IT Sligo An Institiúid Teicneolaíochta, Sligeach

install only the minimum of options One can always add on extra services if they are required but it is often far more complex to remove services cleanly

A common practise in securing today's networks communications is cloning the Bastion Host when you have configured it to a level that you are happy with i e all known weaknesses and potential exploits have been closed This allows the network Administrator to rebuild his connection point to the Internet in a relatively short time span Once a compromised system has been detected one can investigate the reason its defences where overcome, you can then rebuild your Bastion Host by using the cloned copy as discussed earlier Now one can close or patch up the reason for the compromise on the newly built system and then re-clone the machine Taking a cloned image again at this point ensures that one is constantly refining the protection on offer against outside attack There is a learning curve but at least the Bastion Host is reducing the amount of potential damage by sacrificing only itself

The downside of loosing connection to the Bastion Host is obvious, but limiting the services it offers reduces not only the potential for compromise but also the effect it will have on your users when it is not available Adding other technologies on top of the Bastion Host such as proxying and NATS ensures one is making it harder and harder for external forces to affect your network performance and reliability Only the most concerted of efforts will bring down a network of this design, at least now you have prevented the malicious attack of chance and will learn from the more serious attacks

IT Sligo An Institiúid Teicneolaíochta, Sligeach

The advantages of having Bastion Hosts are easily seen and one must also recognise that Bastion Hosts are cheap to implement, normally there is no other specialised software needed, instead it is merely learning how to configure the operating system on the servers at the periphery of you network Most common operating systems are used as Bastion hosts and there are even documented steps widely available on the Internet

2.5 Virtual Private Networks

A common problem before the emergence of the Internet was the huge cost in connecting various networks together Mostly the need for such a set-up was with the large multinationals that may have had plants located all over the world Spending large amounts of money traditionally with the national telecommunication carrier to lease lines connecting one or more sites was seen as a tremendous drain on a company's resources The Internet on the other hand was designed exactly for this reason - the joining of Local area Networks together to form one big Wide Area Network (WAN)

IT Sligo An Institiúid Teicneolaíochta, Sligeach

The only problem with the Internet was the lack of security offered to a company in trying to link its different networks together The Virtual Private Network (VPN) was seen as the solution to this problem It allowed networks to be linked together over a public network by using an extra-secured layer of encryption and authentication The Internet Engineering Task Force was tasked with the creation of standards for building this secured link They developed the IP Security Protocol Suite (IPSec) which enables users to take advantage of cheap public networks to pass information between two dıfferent networks whılst stıll retaınıng the securıty that the ınformatıon travellıng over thıs lınk can not be seen by thırd partıes

The scope a VPN allows to a company to securely and cheaply lınk ıts varıous networks ıs a great asset ın ensurıng the contınuıng growth of the Internet There are many dıfferent types of VPN from the Hardware based system whıch strıctly enforce encryptıon at the router level, to the software versıons that enable organısatıons to create a VPN wıth clıents or customers whıle not forcıng them to purchase expensıve hardware A common ımplementatıon of the VPN ıs the fırewall-VPN, whıch empowers the fırewall wıth the abılıty to encrypt data beıng routed to a specıfıc network Thıs allows the fırewall to have the abılıty to have multıple VPN's confıgured as well as standard access to the Internet The hosts on the network can send ınformatıon as normal on the ınternal prıvate network but, when ıt hıts the fırewall, the fırewall software can judge from ıts destınatıon that the packets must be securely encrypted to prevent outsıde hosts on the Internet beıng able to ınterfere wıth the packet Even ıf the packets are captured by a foreıgn host they are usually encoded wıth 128-bıt encryptıon to prevent anyone from beıng able to read the ınformatıon

IT Sligo An Institiúid Teicneolaíochta, Sligeach

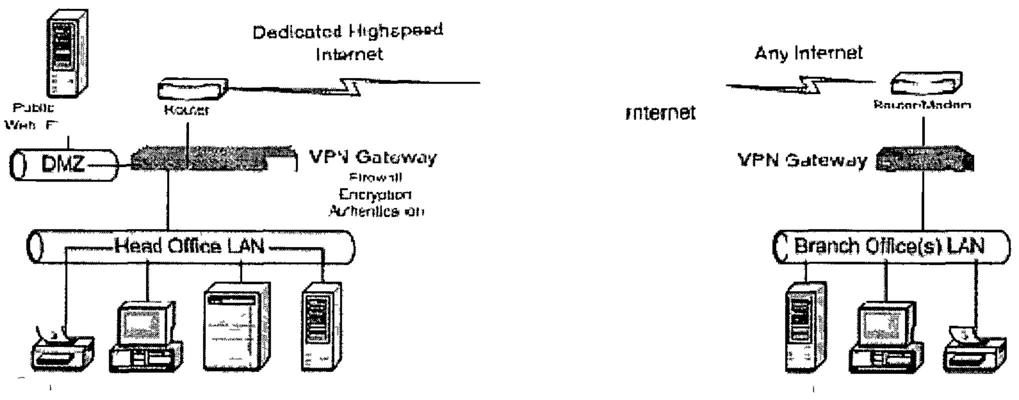


Diagram 2.5 VPN network between Branch office and Head Office over Internet

The downside of using a firewall-VPN is that once again you are loading the Firewall with extra duties Each extra set of services that are placed on the firewall adds to potential performance problems in protecting your network The added burden of encrypting packets can cause a slowdown with the communications between the firewall and its internal clients, this can often lead to reliability problems The administrator is also concerned with the overhead of keeping the various VPN clients and their software versions up-to-date

2.6 Application Level Firewalls

The application level firewalls allow the organisation greater scope in programming what information is permissible through its IT infrastructure They are primarily being used as part of a firewall solution It is common now to see a combination of firewall technologies being implemented, one at the network level such as the packet filtering, and then another at the application level

While the network level firewall protects the organisation at a low level the application level firewall allows the network administrator to scan emails or web pages for references or keywords such as 'porn', 'al-Qaida', 'paedaphile' etc It also allows the administrator to prevent downloads of data from web sites that may be listed as unsuitable

Modern application level firewalls such as SNORT, Black Ice Defender and ZoneAlarm allow the administrator to maintain a database of keywords and sites that should be blocked Commercial databases are also available for the administrator to subscribe to, these databases store information that the application level firewall can

IT Sligo An Institiúid Teicneolaíochta, Sligeach

use to minimize the level of spam and unsolicited emails that pass through an email server It can also inform servers such as the proxy server on what sites are unsuitable for users to access This can be a great tool in ensuring that employees are not wasting internet resources on unsuitable sites

Another great advantage of the application level firewall is the ability to report on the activity of users Most of these types of firewalls come with excellent reporting systems that allow the administrator to profile the internet usage of employees in the organisation This can easily identify workers who are operating outside the internet usage policy of a company

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Chapter 3

Developing a Security Strategy

IT Sligo An Institiúid Teicneolaíochta, Sligeach

3.0 Steps involved in securing Computer Communications

As already discussed there is no quick fix solution for securing your network communications, in actual fact, there is no absolute correct way of approaching such a task Each network and the services it operates are usually very unique, most system administrators have their own methods of installing and securing computer systems and their implementation is totally dependent on what tasks the end users require of their network

The network itself cannot be simply broken down into the physical infrastructure and the protocols that run over it when we need to investigate how to secure communications We must also take account of the end user and the tasks they are trying to perform Security is never a simple black and white decision It cannot be broken into what should be allowed and what should be prevented no matter how desirable this would be It is usually a best effort followed by constant tuning to get the best fit solution The job of securing a computer network needs to be broken down into distinct and crucial tasks One must always start with the adoption of a policy statement on what the security strategy is trying to achieve and how it will go about achieving these aims The main points necessary for building a successful security strategy are

1) Senior Management Buy-In
2) Detailed Analysis of Current Work Practices
3) Adoption of “Best Practices”
4) Adequate Resourcing
5) Disaster Recovery Plan

IT Sligo An Institiúid Teicneolaíochta, Sligeach

3.1 Senior Management Buy-In

All too often it is the Chief Information Officer or the Information Technology Manager who is given the responsibility for drawing up and implementing a computer security strategy within an organisation It usually is a low priority in the main functions or running of the company Most companies often adopt a standard strategy from the Internet with few or no modifications As a service department the IT section of most large corporations carry little or no weight when it comes to forming company policy, it is only when the CEO or Director signoff on the policy that it invariably becomes important

The increasing reliance on MIS systems in companies is slowly starting to change this attitude The increasing reliance on the company's computer network and its services places a greater need for compliance to a corporate or company wide policy on how communications can be made secure The first major step is having the heads of each section identify the needs of their departments with the computer network They must take responsibility for the current practises that operate with their own departments They must identify where the current weaknesses are and highlight what is crucial for them to do their daily business They need to inform the IT department with the results of their audit in order to allow skilled IT personnel scrutinise what is happening and what needs to change

Usually this internal audit identifies the majority of services that are critical and overlooks the normally mundane applications such as email and Web browsing that are taken for granted MIS systems and Productions systems such as SAP and JD

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Edwards are seen as key to a department's success Production or Operations Department will place little or no emphasis on Emails etc ,

It is when these answers to the internal audit come back to the IT department a detailed breakdown or profile of the communications running over the network can be drawn up Potential weaknesses can be pinpointed where the company might be compromised from a flaw in its security The firewall as always is the greatest tool at ensuring the highest level of security can be enforced between the companies' private internal network and the outside Internet

Senior management can be shown, after the installation of a firewall a breakdown of the traffic travelling to and from their company This process is usually the one that awakens management's interest and focuses their minds on the reliance their company may now have on computers and the communications between them Certain services like E-Mail and WWW browsing, which are all too often taken for granted, are now highlighted as major resources required for the company to perform its day-to-day tasks Management can now see for the first time how control over their communications can be organised and structured to meet their needs, it can also show how the firewall can be used to prevent outside groups from gaining access to critical data within the company The benefits of a firewall can also be seen in preventing outside attacks on the services that the company has come to depend on, while ensuring that the services and tasks that are identified for each employee are being utilised for their intended purposes and not for non-work related items This is another key component in winning over management as it ensures that the good name or

IT Sligo An Institiúid Teicneolaíochta, Sligeach

reputation of the company can be further protected by ensuring tight control over what company employees may be doing online with the Internet

3.2 Detailed Analysis of Current Work Practices

The analysis of current work practices is a key step to ensuring that a good security policy can be drafted The main aim of any such undertaking is to ensure that threats and risks to a company's communications infrastructure can be identified Once identified these risks can then be managed to ensure the computer systems will react in a predictable manner Thankfully there are many resources available today to the IT department to highlight potential problems with a company's computing resources, the hardware, software and the network that the data is transmitted through

When one identifies the different elements that make up the IT infrastructure then we are able to ensure that protection is provided at every step in the system chain and not just at specific levels The firewall may be the greatest defence in providing cover at a single location to the most computers but it still depends on a certain level of compliance to security standards by the devices it tries to protect The security policy is the agreement as to the level of self-protection the computers and employees behind the firewall will need to maintain A detailed list of the devices connected to a company's network needs to be kept, a listing of the operating systems being used and the patches (both for the operating system and security) needs to be maintained The key ingredient however is identifying the tasks that are being performed by the user and the services he uses to perform these tasks

IT Sligo An Institiúid Teicneolaíochta, Sligeach

It is unrealistic to think that any organisation can have the unlimited resources required to audit the practices of every employee that uses a computer It is however the aim of an audit on computer usage to begin the process of "employee involvement" and "self-learning" that will facilitate the adoption of a computer policy It will eventually depend on the employee on how he will implement any such policy for protecting himself and the company by adhering to good computer practices An important exercise during the audit is to get each end-user to complete a survey questionnaire which will identify the level of knowledge that employee's have when it comes to handling the different levels of potential threats

The audit is also the key tool to identify what needs to be re-enforced by a security strategy It pinpoints the need to highlight all the aspects of a good security strategy by identifying the different components required Access control policy, email policy, internet policy and communications policy are but some of the separate policies required giving a complete and overall picture The implementation of the security strategy will only succeed when all the components required are looked at and a detailed action plan on how they will be protected is agreed upon

IT Sligo An Institiúid Teicneolaíochta, Sligeach

3.3 Adoption of "Best Practices"

The adoption of "best practices" when protecting ones computer communications is now becoming easier as the Internet community is being constantly driven to improve the security mechanism's on offer Security is time and time again being identified as the one factor that is preventing the Internet becoming the commercial market place that most modern companies are aiming for Institutions like the National Institute of Standards and Technology's (NIST) operate a Computer Security Resource Centre

(CSRC) who have listed as one of their aims - *"Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies,"* The American National Security Agency also freely distributes such guidelines as the C2 Security Standard to enable users harden their personal computers to a high standard With these highly respected institutions making security advisories freely available there is now a general trend to co-operatively build a standard set of security guidelines to help in the building of formidable defences in protecting one's networked computers

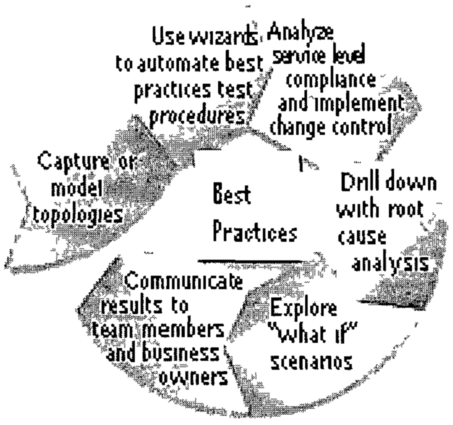

Use wizards to automate best practices test procedures
Analyze service level compliance and implement change control
Drill down with root cause analysis
Explore "what if" scenarios
Communicate results to team members and business owners
Capture or model topologies
Best Practices

Diagram 3.3 typical "best practices" flow

Microsoft, Linux and all other major software vendors now offer online services to allow users to patch their operating systems against known security weaknesses that have been discovered or reported to the vendors Microsoft's update centre now receives millions of online requests per day from computers trying to download critical updates, the majority of these requests are now from computers that are scheduled to check for updates at regular intervals thus ensuring that they are kept up to date Services like these are playing a major role in combating and closing down the opportunities that are available to hackers

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Most organisations see the adoption of best practices as a means to prevent abuse of email and Internet use within a company, this is mainly to protect the good name of the organisation against any civil or criminal law suits which would be publicised by the media as another scandal using electronic communications "Best Practices" in the IT industry cover more than just this one area they are designed to enable an organisation to respond in a timely and appropriate fashion to security events which are happening all too often Companies with a major investment or reliance upon their networks cannot merely be seen to be reacting to events but must put in place precautions to prevent potential security breaches that have already been discovered or documented widely on the Internet They must identify by use of best practices the areas of their electronic communications that are vulnerable to unwanted third parties as well as using these best practices to ensure that necessary steps are being taken to ensure such weaknesses are addressed as well as planning how to cater for potential other weaknesses

IT Sligo An Institiúid Teicneolaíochta, Sligeach

3.4 Adequate Resourcing

Budgeting for an IT department today is a very complex task, all too often major pressure is placed to ensure that costs are kept at a minimum The IT department must thread the fine line at being able to improve on current IT performance as well as being able to maintain a high level of quality or standards Most IT professionals always know of a system that does the job better or a new tool which would be of benefit but cannot quantify on how much the new resource would actually cost All too often its is the purchase price of a new system be it a computer, software system, utility or service that is seen as the end cost to the organisation, this is not the case

Security is now an ongoing cost and needs to be budgeted for by the IT Department and the problem is how do we put a price on maintaining security

It is relatively easy to put a price on the cost of a security system like a firewall Such market leading applications like CheckPoint, Cisco Firewall and NetScreen all have web sites advertising their product details and the cost per site/license for installation They do not however detail the cost of having to continually keep such a purchase up to date Security is not a straightforward problem as already discussed with a simple answer Securing network communications is an ongoing process that is constantly evolving, if you don't continually maintain or evolve your security services then you are automatically falling behind and leaving your network vulnerable A published weakness in an operating system with an advertised update is only advantageous to a company when they install the update Up to when the update is installed the weakness is a serious security gap in your network's defences

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Knowledge is the main resource that must be applied to this problem and it is this knowledge or expertise that costs money More and more companies are now advertising their services as security consultants It is quite normal now for a lot of large companies to employ a consulting security firm to check out the reliability of security precautions on their sites These security firms usually have expertise in the latest methods used by hackers to gain access and unleash havoc on ones network Organisations must ensure that employing independent security consultants is part of their security strategy as it is these consultants who can audit what protection is on offer to your network They can continually assess you network resources as the common hacker would and by monitoring from the outside can identify what services are being advertised to the Internet and their weaknesses

The recommendations from these consultants can be a major contribution to developing a security policy that is unique to your organisation The policy can take into account the type of weaknesses that were discovered and how they make the internal network vulnerable The process is a continual one and constant tests of the hardening exercise must be undertaken to show that recommendations are being examined and learned from, it also shows that the security strategy is an evolving strategy and not just a response to a particular incident at a particular time

3.5 Disaster Recovery Plan

Probably the most important sign of awareness to developing a security strategy is the knowledge that at sometime ones network communications may be compromised and may need to be restored The ability to plan for such a disaster it one of the greatest tools available to ensure that your network communications can be made fault tolerant and withstand even a serious breach of your security systems The firewall as described is our single greatest tool for implementing secure network communications, however the reliance on a firewall places great emphasis that this choke point must stay operational for our network communications to continue

Modern implementations of firewalls now take advantage of technologies such as Cluster Servers, redundancy technologies, Bastion Hosts or Enterprise-Wide solutions, all of which offer protection against a single point of failure that would halt all network communications to and from the Internet The creation of a Disaster

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Recovery Plan however ensures that a policy is in place that details the steps needed to allow the resumption of normal services after a compromise of the firewall All too often the firewall is blamed as the reason that the Internet is unavailable to the users of a network, the benefits of having the firewall in the first place are not usually high on the priority list of the end user

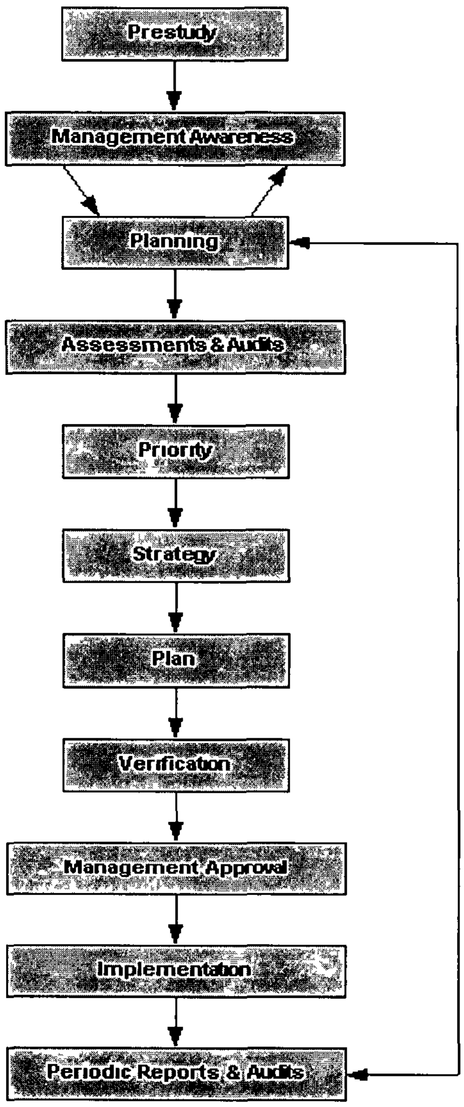


Diagram 3.5 Disaster Recovery Plan stages

The risk analysis of your computer systems is the key tool as to how the Disaster Recovery Plan is drafted and what steps need to be put in place to ensure your network communications can recover from an unwanted security breach Security Assessment of every aspect of ones network communications environment including operating procedures, contingency planning, database security, data communications, access control and personal computers usage must be analysed The important factor in putting a good Disaster Recovery Plan in place when specifically planning for a recovery from a security breach, is to learn from the security breach itself and adopt a solution as to how the recovery will cater for this breach in the future

IT Sligo An Institiúid Teicneolaíochta, Sligeach

PART 2

The Need for Secure Network Communications

A Practical Implementation of a Firewall in C++

An Institiúid Teicneolaíochta, Sligeach

Chapter 4

Project Aims and Design

IT Sligo An Institiúid Teicneolaíochta, Sligeach

4.0 Introduction

This project shows how to build a firewall using C++ and Internet Sockets As the scope of the project is very large we will concentrate on implementing a Bastion Host or choke point between the external Internet and the internal application server The building blocks will be laid with this piece of code to enable future functionality to allow greater security for a network

4.1 Aims

The aim of the project is to show an understanding of C++ programming and being able to implement a system from design to testing Originally my interests lay at getting to the physical layer of the network i e , the lowest level or the TCP/IP Reference Model and getting to the network packets themselves This however is now extremely difficult with Windows XP as Microsoft have tightened up the security and ability to go to such a level The only documented example of how such access is capable from Microsoft was in the Microsoft Development Kit with their PassThru NDIS Intermediate driver code and this only allowed specific functionality and not packet manipulation

IT Sligo An Institiúid Teicneolaíochta, Sligeach

TCP/IP Reference Model

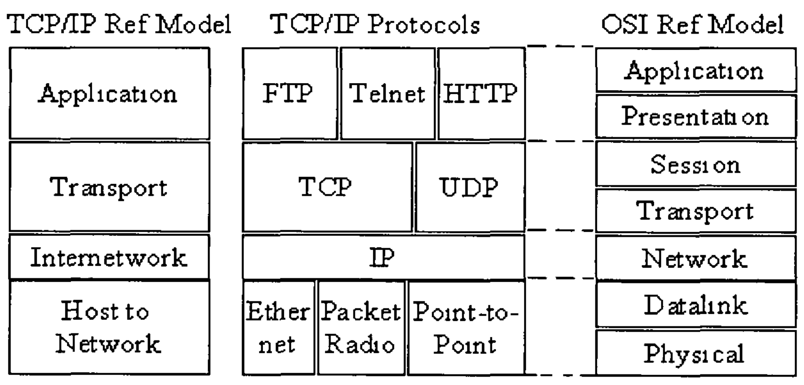


Diagram 4.1 Network Reference Model

From researching the area the most common approach to network programming in C++ is using Internet Sockets, commonly referred to as Winsock Programming Winsock programming is basically a set of routines that provide a programming interface between an application and the TCP/IP protocols The main building principle of Winsock programming is the socket Based on the Berkeley Software Distribution (BSD) Sockets, the socket allows for Client/Server communication The socket is the point of contact between a Server and a Client

In its simplest form the Server creates a socket using a structure called sockaddr_in this enables the programmer to describe the type of connection, the ip address of the server and the port of the server to connect to Once this socket is created the server can listen on this port and accept / receive data from a peer and send data back to the peer

IT Sligo An Institiúid Teicneolaíochta, Sligeach

```
struct sockaddr_in {
    short int           sin_family,
    unsigned short in   sin_port,
    struct in_addr      sin_addr,
},
```

Figure 4.1 Socket Structure

This firewall project is based on the communication between Server and Client using the above structure, you will see throughout the project examples of where sin_family will be set to AF_INET, sin_port set to the port being advertised by the firewall and also being protected by the firewall and sin_addr will have the ip address of the firewall Sin_family set to AF_INET allows for both connection oriented and connectionless type of communication i e TCP and UDP

This firewall is designed to act as a service on a computer running the Microsoft Windows XP operating system, once initiated it will read the initialisation parameters for the firewall from a text file it will then position itself to protect a named service and will continue to handle data delivered to its outside interface by passing them internally to the internal server service it is protecting

4.2 Design

To achieve the aims of this project the project design must take into account the need for the firewall software to -

a) read initialisation parameters from a file
b) monitor a particular port on a named interface
c) accept and queue communications to this port
d) pass on these communications to the internal server
e) accept responses from the internal server
f) pass on internal communications to external peer
g) await further communications

The functionality described above will allow the application to act as a Bastion Host and showcase the major routines required for programming network communications These routines can be identified in winsock programming as socket, bind, connect, listen, accept, recv and send, all of which will be seen later in the code

C++ has also the ability to set up distinct locations in memory to handle a running process As the firewall will be running as a service I have used the ability of C++ to create threads to package the firewall in one memory location This will offset the need to program the firewall to handle an ever-growing memory requirement at code level As a service the application will be continually listening on one port and handle the potential for multiple connections, the amount of memory required could be immense It is a strong advantage to the C++ programmer to be able to utilise threads

IT Sligo An Institiúid Teicneolaíochta, Sligeach

throughout his/her program The threat of an ever-increasing memory demand problem can easily be handed over to the operating system by encapsulating the firewall into one process and using the `_beginthreadex` function to handle potential memory handling problems

The application will be the only route from which external clients can make contact with the internal server All data must first be directed at the outside interface of the firewall and the correct port The application will then queue the request received at the outside interface and redirect them to the internal server in order they arrived It then waits for the response from the internal server and sends it on in turn to the external client

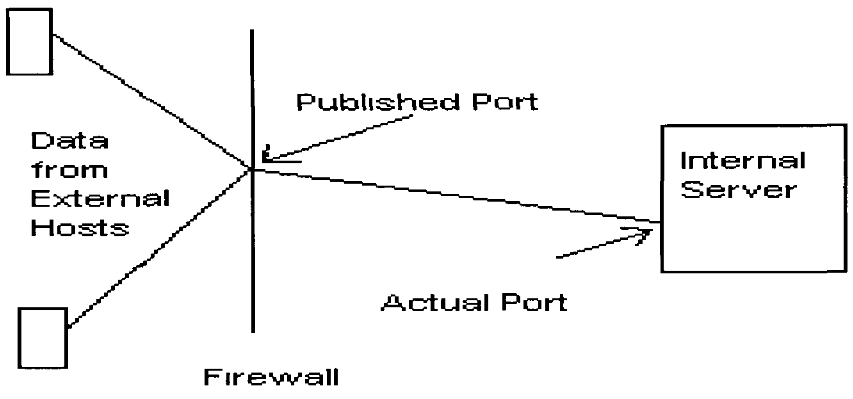


Diagram 4.2.1 Firewall as Choke point

The application on the internal server in this project will be any typical TCP application such as HTTP or FTP The firewall will listen on the designated port and forward the request onto the proper port of the internal server such as port 80 for HTTP and 21 for FTP

IT Sligo An Institiúid Teicneolaíochta, Sligeach

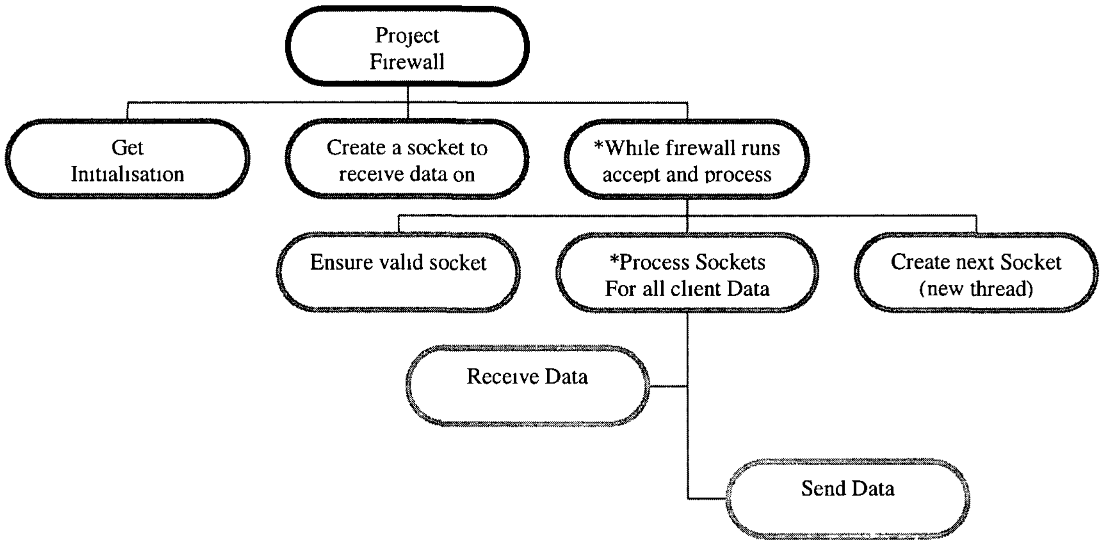

Project Firewall
Get Initialisation
Create a socket to receive data on
*While firewall runs accept and process
Ensure valid socket
*Process Sockets For all client Data
Create next Socket (new thread)
Receive Data
Send Data

Diagram 4.2.2 Top Down Design chart

The file being used to store the initialisation data for the firewall is in the form of a flat file structure The code is written to ignore any line with a comment, these comment lines are identified with the # character It reads the remaining lines of the file to fill in the key security configuration data required by the firewall These are the port the external address of the firewall is to listen on, the IP address of the internal server and the actual port number of the internal application All the settings are stored in ASCII format

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Chapter 5

Implementation and Code

IT Sligo An Institiúid Teicneolaíochta, Sligeach

5.0 Introduction

I have implemented the code for this project using two main functions `GetFileData` and `StartFirewall` These two main functions handle the initialisation of the Firewall with `GetFileData` and the handling of socket data with `StartFirewall`

5.1 GetFileData

The function `GetFileData` uses 3 parameters which pass the initialisation values from this function back to the main body of the code The three internal variables ConfigObject1, ConfigObject2 and ConfigObject3 are used to traverse over keywords in the file identifying the initialisation parameters A simple identification of the file to be used can be made by `ifstream inClientFile( "firewall ini", ios  in ),` this allows for sequential access to the file The ios in declares the file is open and in read only mode Ifstream by default creates an object called inClientFile which allows the programmer to access data in the file The file that we are using is called "firewall ini"

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

The next part of the GetFileData function is to ensure that the file exists, if no file is found the "File Damaged or cannot be read" message is displayed at the console The next statement

```
while (inClientFile peek() == '#') {
            inClientFile ignore(80, '\n'),
}
```

ensures that the pointer for reading the file skips any commentary in the file and is placed onto a line which contains initialisation data

```
#firewall ini File
#This file stores configuration Data for Alan's  Firewall
#
#The first piece of configuration Data is the actual address of the server
#that is being published behind the firewall
#
#The second configuration setting is the number of the socket that your server
#is been publihed on ie  external firewall port number
#
#The third is the actual port that the internal server will act on
Server 192 168 1 102
port   1285
redirect   80
```

Figure 5.1 Sample firewall ini

The pointer is now positioned at the 11th line of the file firewall ini i e Server 192 168 1 102 The next lines of code in the GetFileData read the key data in variables -

```
inClientFile >> ConfigObject1 >> aname,
```

The object inClientFile reads the first piece of text into ConfigObject1 and then reads the IP address of the server in the variable `aname` It repeats this for the data that is loaded into the variables `aport` and `rport` The application now has the parameters required for configuring the Firewall

5.2 StartFirewall

The StartFirewall function is the main function in this project, it holds all the classes and procedures used throughout this application for passing data between external hosts and the private network When initiated it creates a new thread on the operating system

```
_beginthreadex(0, 0, StartFirewall,(void*) s,0,&ReturnValue),
```

Here we are letting the operating system take care of the maintenance of this function and merely pass a pointer to a socket s to the function `StartFirewall` A pointer to

IT Sligo An Institiúid Teicneolaíochta, Sligeach

any data type, socket in this case, can be assigned to a pointer of type void * It enables us to pass data to the thread in the form of a structure i e socket

The global function `StartFirewall` is defined using the following code

```
unsigned __stdcall StartFirewall (void* a)
```

__stdcall is used to clean the stack used by the operating system before `StartFirewall` is activated The procedures used inside the `StartFirewall` and their memory requirements are all now managed by the operating system while the firewall is running This is a significant advantage to the C++ programmer as it removes the task of handling numerous potential memory issues such as dwindling resources and contention, and hands them all over to the operating system

5.2.1 SocketClient

We will now discuss the main classes used throughout the program `SocketClient` is a class used in the program, we create an instance of `SocketClient` called client This class is used to ensure we can talk back to the client that is requesting communications with the internal application server After creating this instance we use the initialisation details read in the firewall ini (see Page 55) for the internal application server and the port it is set to listen on In this case the protected Server has an IP address of 192 168 1 102 and the port it is listening on is the standard HTML port of port 80 The external client will have to know the external IP address of the firewall and the port it is listening on It should not for safety reasons ever know the actual IP address and port number of the internal server

IT Sligo An Institiúid Teicneolaíochta, Sligeach

```
SocketClient  SocketClient(const string& host, int port)   Socket() {
  hostent *he,

  if ((he = gethostbyname(host c_str())) == 0) {
        throw "Cannot get Host Name",
  }

  sockaddr_in addr,
  addr sin_family = AF_INET,
  addr sin_port = htons(port),
  addr sin_addr = *((in_addr *)he->h_addr),

  memset(&(addr sin_zero), 0, 8),

  if (  connect(SocketforData, (sockaddr *) &addr, sizeof(sockaddr)))
{
     throw "Error connecting with socket ",
                                   strerror(WSAGetLastError()),

  }
}
```

Figure 5.2.1 SocketClient Class

`hostent *he` sets up a structure *he* of type hostent, hostent is a combination of fields that contain information about the host you are identifying In our example we are using the function `gethostbyname` to return the details of host to the he structure In essence we are identifying that 192 168 1 102 exists The next 4 lines allow us to specify the details of the internal server The `sockaddr_in addr` line enables us specify a structure addr that will enable the firewall to communicate with the protected server `addr sin_family = AF_INET` informs us that we will be using the INET objects as our address family is IPv4 `addr sin_port` is set equal to the port the internal server is listening on `htons(port),` `htons` sets the value of port to a two byte representation (network byte order)

`addr sin_addr = *((in_addr *)he->h_addr)` points the required IP address to the address we loaded into the *he* structure earlier i e 192 168 1 102 We now have all the required information to create a connection to the internal server It is important in Internet socket programming to ensure no data exists in the socket before we use it

IT Sligo An Institiúid Teicneolaíochta, Sligeach

hence the `memset(&(addr sın_zero), 0, 8)` as thıs loads zeros ınto the addr sın_zero element ın the sockaddr_ın structure

5.2.2 SocketCall

`SocketCall` ıs the next class used ın the project, ıt basıcally allows us to associate and handle the data beıng passed by the functıons as ıf they were beıng read from a fıle As C++ began as a programmıng language on the UNIX operatıng systems a lot of the programmıng concepts are buılt around how UNIX vıewed most devıces as fıles The FD_ZERO and FD_SET allow us to process bıt fıelds stored as arrays of ıntegers FD_ZERO allows us to ınıtıalıze a fıle descrıptor `&fdSocketforData` to the null set FD_SET allows us to ınclude a partıcular fıle descrıptor ınto the FDSET Thıs example -

`FD_SET(const_cast<Socket*>(s1)->SocketforData,&fdSocketforData)`

shows how the socket poınter s1 ıs used for member selectıon by the object `SocketforData` as <socket*>(s1) ıs a poınter to a socket We use `const_cast` to allow us to modıfy ıts value as ıt was orıgınally passed to the class as a type `Socket const * const s1` The abılıty to do thıs enables us to manıpulate the data later ın the program

```
TIMEVAL StopWatch,
StopWatch tv_sec  = 10,
StopWatch tv_usec = 500000,
TIMEVAL *pStopWatch,
pStopWatch = 0,
```

Figure 5.2.2.1 C++ Class for storıng tıme value

The above code allows us to set up a structure call StopWatch of type TIMEVAL where we can specıfy tıme values In Fıgure 5 2 2 we set seconds to 10 and mıcroseconds to 5000000 (half a second as 1,000,000 equals a second)

```
select (0, &fdSocketforData, (fd_set*) 0, (fd_set*) 0, pStopWatch)
```

The above function checks if sockets descriptors are ready to read and write, the `select` function gives us a way of simultaneously checking if there is data to be received or if we can now send data without blocking our lines of communication `pStopWatch` sets the timeout value for the select function It basically is set to return when an event occurs or after 10 5 seconds

```
bool SocketCall   Data_Exists(Socket const* const s) {
  if (FD_ISSET(s->SocketforData,&fdSocketforData)) return true,
  return false,
```

Figure 5.2.2.2 SocketCall Class method `Data_Exists`

The code above ensures that the program knows if there is still a connection established with sockets to the server by returning a TRUE or FALSE value

5.2.3 BindToSocket

```
BindToSocket  BindToSocket(int port, int connections) {
  sockaddr_in my_addr,

  my_addr sin_family = AF_INET,
  my_addr sin_port = htons(port),
  my_addr sin_addr s_addr = inet_addr("193 1 88 47"),

  memset(&(my_addr sin_zero), '\0', 8),

  SocketforData = socket(AF_INET, SOCK_STREAM, 0),

  cout << "Firewalls IP address is  "
                << inet_ntoa(my_addr sin_addr) << endl,

if (SocketforData == INVALID_SOCKET) {
    throw "INVALID_SOCKET",
  }


  // socket is bound to my internet address //
  if (bind(SocketforData, (sockaddr *)&my_addr, sizeof(sockaddr_in))
== SOCKET_ERROR) {
    closesocket(SocketforData),
      throw "SOCKET_ERROR",
  }
  listen(SocketforData, connections),


}
```

Figure 5.2.3.1 BindToSocket Class

An Institiúid Teicneolaíochta, Sligeach

BindToSocket is the function responsible for setting the firewall to listen for incoming connections Once again it uses the `sockaddr_in` structure to setup the value required to create a socket This time it takes the value from `FireWallPort` in the main body of the program when it is called to populate the port to listen on In this section of code I hard coded the IP address of the external adapter by using the code referenced by `my_addr sin_addr s_addr = inet_addr("193 1 88 47")` I could have used the system parameter `INADDR_ANY` instead of the actual IP address but if your firewall has two interfaces then both could end up listening for connections on the prescribed port

`SocketforData` is set to a socket structure to allow TCP connections If `SOCK_DGRAM` was used instead of `SOCK_STREAM` you would be able to cater for UDP traffic I have left a simple output message to show that it is the outside IP address that has now a socket available for connections The remaining lines of code just check that the socket was created successfully and that it now exists The code `bind(SocketforData, (sockaddr *)&my_addr, sizeof(sockaddr_in)` is the actual piece of code that associates the socket with the IP address and port number The bind function always returns a zero on successful association or a –1 on an error

The final function of the `BindToSocket` class is to tell the socket to listen for incoming connections The external address of our firewall is now listening for connections, the code

```
listen(SocketforData, connections)
```

sets the server into a waiting state that will handle a number of pending connections identified by the value of the variable `connections` In our example we originally set connections in the main body of the code to 5 Hence we now have a socket set on the external IP address of our firewall that will handle up to 5 pending connections before dropping any new connections

```
Socket* BindToSocket  Accept() {
  struct sockaddr_in client_addr,

  socklen_t len,
  SOCKET new_sock = accept(SocketforData, 0, 0),

  len = sizeof(client_addr),
  getpeername(new_sock, (struct sockaddr*)&client_addr, &len),
  cout << "Peer IP Address   " << inet_ntoa(client_addr sin_addr) <<
                                                       endl,


  if (new_sock == INVALID_SOCKET) {
    int rc = WSAGetLastError(),
    if(rc==WSAEWOULDBLOCK) {
      return 0, // nonblocked call
    }
    else {
      throw "Invalid Socket",
    }
  }

  Socket* r = new Socket(new_sock),
  return r,
}
```

Figure 5.2.3.2 BindToSocket Class member function Accept

Now that our firewall is awaiting connections we must deal with what happens when they arrive Here the key line of code is

```
SOCKET new_sock = accept(SocketforData, 0, 0),
```

It creates a new socket descriptor called new_sock that handles all communications with the connected client getpeername is a built in socket function that returns the network information of the client at the remote end of the communication

IT Sligo An Institiúid Teicneolaíochta, Sligeach

In socket programming a peer is seen as the remote end of the communication, in our example it is the client that has connected to the firewall's external IP address

`getpeername` returns the now familiar structure sockaddr_in

```
getpeername(new_sock, (struct sockaddr*)&client_addr, &len)
```

Places the peers information into client_addr which is identified by a pointer to sockaddr This in turn has key host information such as the IP address of the peer

```
        inet_ntoa(client_addr sin_addr)
```

to ascertain the IP address of the peer we simply use the code above This will allow us to identify the addresses of all external clients

As with most firewalls we may choose to store a list of external clients that we do not wish to communicate with Comparing this list with the IP addresses retrieved above will allow us to take appropriate action such as dropping the communication Ending the communication can be as easy as activating a closesocket function We may also choose to write back access denied information to this unwanted client informing the client that his connections will not be accepted

IT Sligo An Institiúid Teicneolaíochta, Sligeach

5.2.4 Socket

The final main class used throughout the project is the socket class itself It contains the most member functions of any of the classes as we can manipulate a socket in many ways It is primarily responsible for starting, sending, receiving and ending the transmission of data over the network

```
void Socket  Start() {
if (!nofSockets_) {
WSADATA info,
  if (WSAStartup(MAKEWORD(2, 0), &info)) {
      cout << stderr << "WSA Startup Failed" << endl,
      exit(1),
      }
  }
++nofSockets_,
}
```

Figure 5.2.4.1 Socket Class member function Start

Figure 5 2 4 1 describes how we initialise the program to use winsock (windows internet sockets) WSADATA notifies the computer that we will be using the winsock library the definitions of this library are brought in to the program using `#include <WinSock2 h>` WSAStartup defines what parameters the winsock library will support in this case the highest level version 2 0

```
void Socket  Close() {
       closesocket(s_),
      }
```

Figure 5.2.4.2 Socket Class member function Close

The function above simply closes any socket that is passed to it, it is called by the deconstructor of the class socket in the code below It simply checks to see that the counter has reached empty and closes the socket

```
Socket  ~Socket() {
if (! --(*refCounter_)) {
      Close(),
      delete refCounter_,
 }
```

Figure 5.2.4.3 Socket Class destructor

Other member functions include `SendBytes and ReceiveBytes` which can be seen used in the main `StartFirewall` function for sending and receiving the data from the client to the firewall and from the firewall to the internal application server Using

IT Sligo An Institiúid Teicneolaíochta, Sligeach

the method `Data_Exists` as described earlier the program can check that all the communications between Client and Server have been catered for

If communications are still pending on the external interface of the firewall then the `StartFirewall` function can process the data by calling the `ReceiveBytes` function

```
string Socket  ReceiveData() {
  string ReturnValue, tempHold,
  char buf[100], //setting buffer to 100
  while (1) {
      unsigned long argp = 0,
      if (ioctlsocket(SocketforData, FIONREAD, &argp) != 0)
            break,
      if (argp == 0) break,
      if (argp > 100) argp = 100,

      int HeldData = recv (SocketforData, buf, argp, 0),
      if (HeldData <= 0) break,

      tempHold assign (buf, HeldData),
      ReturnValue = ReturnValue + tempHold,
  }
return ReturnValue,
}
```

Figure 5.2.4.4 Socket Class member function ReceiveData

It uses the `ioctlsocket` function to control the Input / Output mode of the socket and to see if there is pending data on the socket `SocketforData` The amount of data that is returned is equal to the amount that can be read in call to the `recv` function *buf* stores the number of bytes that are read at any one read of the socket we make sure only 100 bytes or less are read at any one time

The `ReturnValue` will be a string with all the data sent to the firewall combined back together The firewall can now act as the go-between to the internal server as it now has the information request from the client stored as a string called `bytes` in the StartFirewall function Now that we have the full request from the client we can now prepare to send it on to the internal server This is now done using the `SendData`

IT Sligo An Institiúid Teicneolaíochta, Sligeach

function This is easier done as the control of the sending of the data is entirely down to end server, in our case the internal application server

```
void Socket  SendData(const string& s) {
  send(SocketforData,s c_str(),s length(),0),
}
```

Figure 5.2.4.5 Socket Class member function SendData

Basically we accept in the string of data we have put together from our `ReceiveData` function and use the class member function `SendData` to initiate sending data out over our socket It tells the internal server the size of data it needs to send with the `s length()` argument and continue to sends the actual data until all has been successfully received by the internal server

We can reverse the exchange of data communications to use `ReceiveData` to accept the responses from the internal server and `SendData` to send them onto the external peer I have placed these lines of code inside a while loop

```
while (1)
```

that ensure the program continues until some outside action happens such as halting the program The firewall reuses these main classes continually to ensure that it handles all the communications required in a stable manner

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Chapter 6

Testing and Results

IT Sligo An Institiúid Teicneolaíochta, Sligeach

6.0 Introduction

The firewall was built to prove that access could be granted and controlled from an external computer ınto a prıvate network To prove that our code can handle these communıcatıons I have set up a number of tests These tests are desıgned to show how three of the mam TCP protocols can be handled by our firewall The test envıronment descrıbed below wıll show how we can prove that ınter communıcatıon between networks ıs catered for by the firewall

6.1 Test Envıronment

In order to test the firewall properly I have set up two networks, one a prıvate network of 192 168 1 0/24, and the second a prıvate network of 172 16 0 0/16 A gateway exısts between both these network, and any devıce wıshıng to ınter-connect between the two networks must use thıs gateway I have desıgned the networks so only the firewall knows the name of the gateway between both No other devıce ıs aware of the ınterconnectıon between the networks

IT Sligo An Institiúid Teicneolaíochta, Sligeach

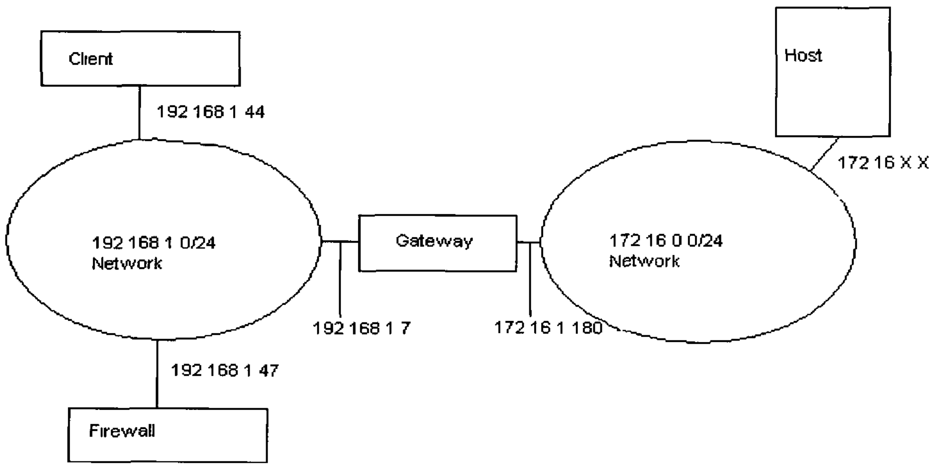


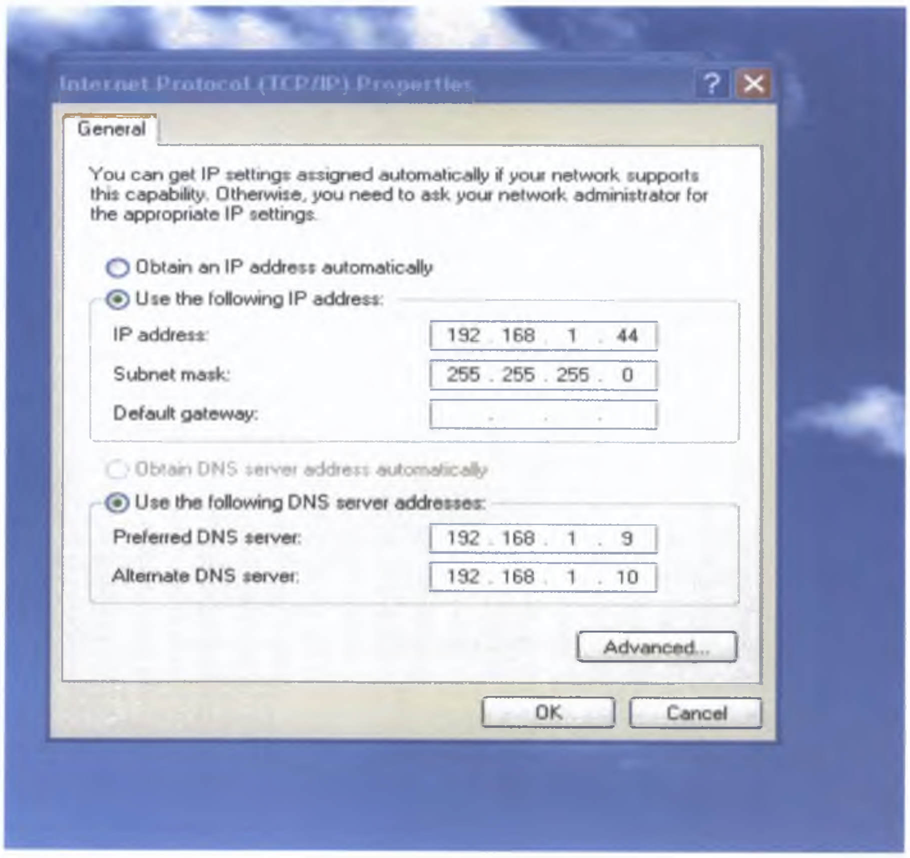
Diagram 6.1 Test Scenarıo

The host IP address will be different in all 3 of the tests as this will be the IP address of a Web Server, FTP Server and also a TELNET server. The 3 test scenarios will prove how the TCP protocols HTTP on port 80, FTP on port 21 and Telnet on port 23 will be protected by the Firewall.

6.2 Client

The client I am using for the test scenarios is a laptop computer. It has the Microsoft Windows XP operating system installed and no other software. The network card has been configured to use the IP address of 192.168.1.44 with subnet of 255.255.255.0. It has purposely been programmed not to have a gateway address in order to ensure no other device may be passing on its communications.

IT Sligo An Institiúid Teicneolaíochta, Sligeach



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically [✓ Use the following IP address:]

IP address:	192 . 168 . 1 . 44
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

Obtain DNS server address automatically [✓ Use the following DNS server addresses:]

Preferred DNS server:	192 . 168 . 1 . 9
Alternate DNS server:	192 . 168 . 1 . 10

Diagram 6.2.1 Clients IP settings

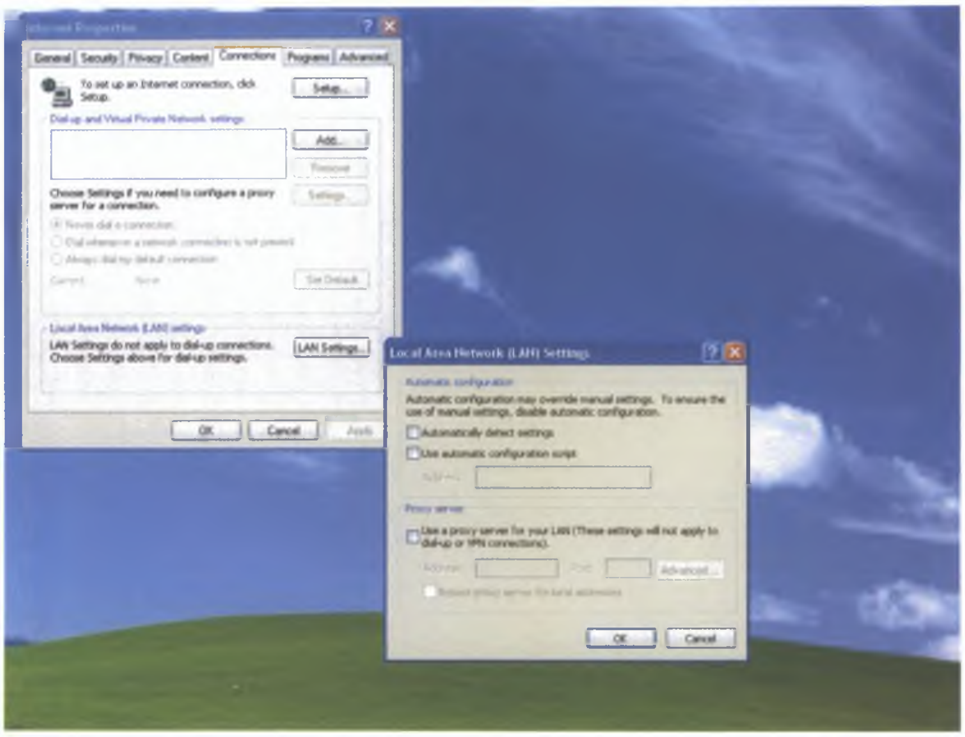
From the settıngs shown ın dıagram 6 2 1 thıs computer should only be able to talk on a peer-to-peer basıs wıth any other computer on the 192 168 1 0/24 network A look at the routes for thıs computer confirms thıs

```
===========================================================================
Interface Lıst
0x1                    MS TCP Loopback ınterface
0x2   00 04 76 49 2c ce     3Com 10/100 Mını PCI Ethernet Adapter - Packet Scheduler Mınıport
===========================================================================
===========================================================================
Actıve Routes                 \
Network Destınatıon        Netmask          Gateway       Interface  Metrıc
        127 0 0 0          255 0 0 0        127 0 0 1      127 0 0 1     1
      192 168 1 0      255 255 255 0     192 168 1 44   192 168 1 44    20
     192 168 1 44    255 255 255 255        127 0 0 1      127 0 0 1    20
    192 168 1 255    255 255 255 255     192 168 1 44   192 168 1 44    20
        224 0 0 0          240 0 0 0     192 168 1 44   192 168 1 44    20
  255 255 255 255    255 255 255 255     192 168 1 44   192 168 1 44     1
===========================================================================
Persıstent Routes
  None
```

Diagram 6.2.2 Output from Route Prınt command on Clıent

The table above shows clearly how the clıent has only 2 routes avaılable, both of whıch are ıts own ınterface ı e 192 168 1 44 or the loopback address of 127 0 0 1 It has no avaılable route to any other network Another means by whıch a computer may communıcate wıth the ınternet ıs by havıng a proxy server configured Dıagram 6 2 3 shows that no such proxy server ıs configured on our clıent

Thıs clıent ıs ın a state where ıt can only talk to other computers on the physıcal network ıt ıs attached to, access to any other network ıs not avaılable



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

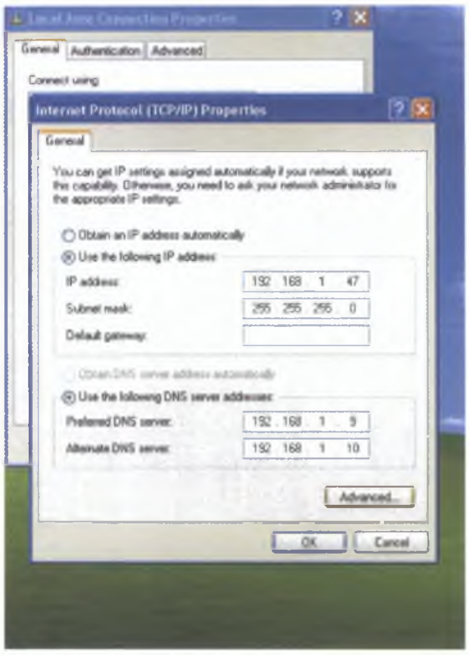
Proxy server

☐ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Diagram 6.2.3 Clients Proxy settings

6.3 Firewall

The firewall computer is a standard Pentium computer. The only software loaded on this machine is the Microsoft Windows operating system and Microsoft Visual Studio .NET. Microsoft Studio is loaded so that the DLL's required by the firewall application are present. The firewall was installed on the 192.168.1.0/24 network with an IP address of 192.168.1.47. This IP address was hard coded into the application for these tests. It is on this interface of 192.168.1.47 that our application will listen for communications from clients.


Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Internet Protocol (TCP/IP) Properties
General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

( ) Obtain an IP address automatically
(✓) Use the following IP address:

IP address:	192 . 168 . 1 . 47
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	

( ) Obtain DNS server address automatically
(✓) Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 1 . 9
Alternate DNS server:	192 . 168 . 1 . 10

Diagram 6.3.1 Firewalls IP settings

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

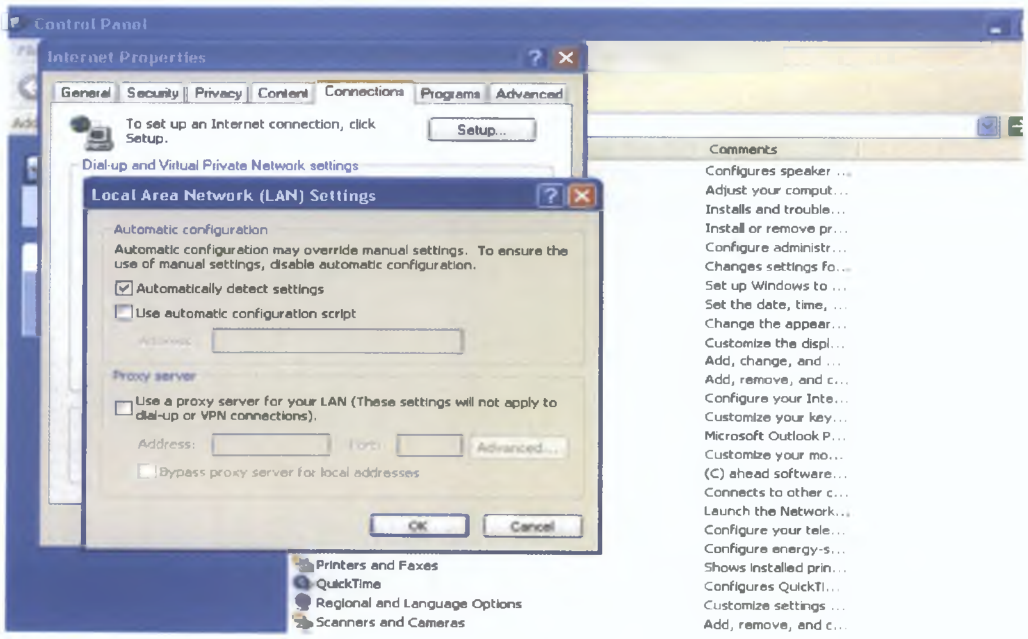
I have also programmed the firewall computer to have a route to the 172.16.0.0/16 network by sending data onto 192.168.1.7. This can be seen in Diagram 6.3.2, which shows that the Firewall unlike the client has 3 gateways. The three gateways are itself, in the form of 192.168.1.47, and the loopback address of 127.0.0.1. It also has a gateway with an IP address of 192.168.1.7. The IP address of 192.168.1.7 is programmed as a persistent route; so the firewall will always have a means by which to send on data to the 172.16.0.0/16 network.

```
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 30 05 3b 50 83 ...... Intel(R) PRO/100 VM Network Connection
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
         172.16.0.0      255.255.0.0      192.168.1.7    192.168.1.47       1
        192.168.1.0    255.255.255.0     192.168.1.47    192.168.1.47      20
       192.168.1.47  255.255.255.255        127.0.0.1       127.0.0.1      20
      192.168.1.255  255.255.255.255     192.168.1.47    192.168.1.47      20
          224.0.0.0        240.0.0.0     192.168.1.47    192.168.1.47      20
    255.255.255.255  255.255.255.255     192.168.1.47    192.168.1.47       1
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
       172.16.0.0      255.255.0.0      192.168.1.7       1
```

Diagram 6.3.2 Output from Route Print command on Firewall

Once again we ensure that no proxy settings are installed, as it is now down to our own firewall code to send on the information to the external application server.

IT Sligo
An Institiúid Teicneolaíochta, Sligeach



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

[✓] Automatically detect settings

[ ] Use automatic configuration script

Address:

Proxy server

[ ] Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: Advanced...

[ ] Bypass proxy server for local addresses

OK Cancel

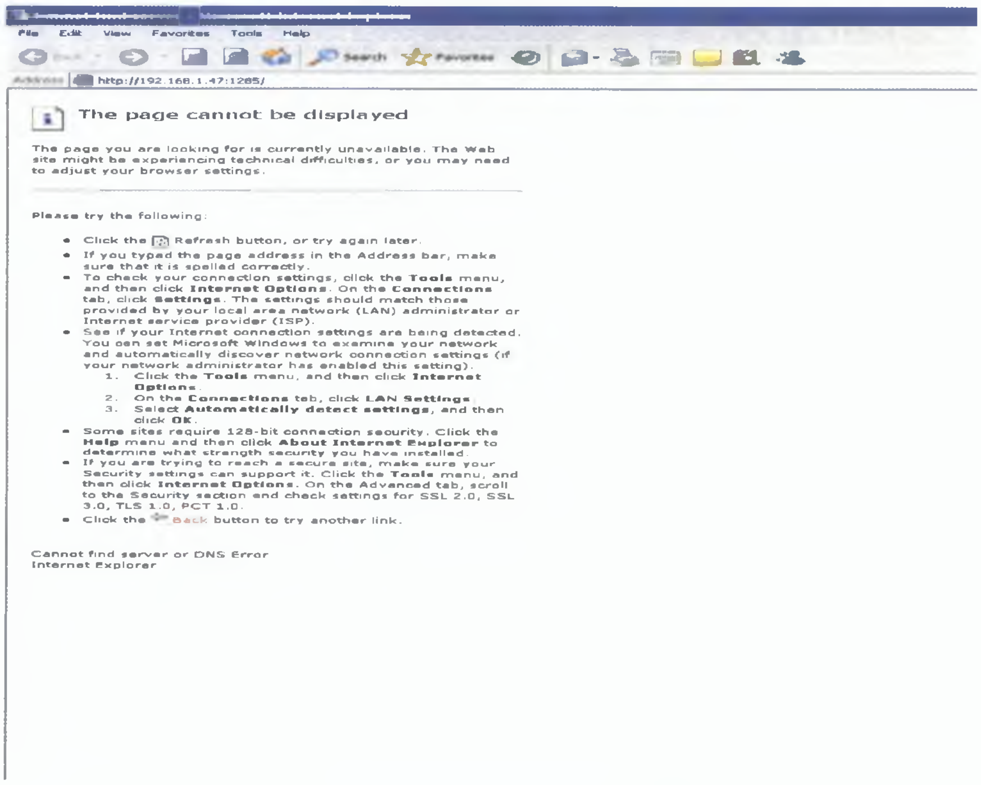
Configures speaker ...
Adjust your comput...
Installs and trouble...
Install or remove pr...
Configure administr...
Changes settings fo...
Set up Windows to ...
Set the date, time, ...
Change the appear...
Customize the displ...
Add, change, and ...
Add, remove, and c...
Configure your Inte...
Customize your key...
Microsoft Outlook P...
Customize your mo...
(C) ahead software...
Connects to other c...
Launch the Network...
Configure your tele...
Configure energy-s...
Shows installed prin...
Configures QuickTi...
Customize settings ...
Add, remove, and c...

Diagram 6.3.3 Firewalls Proxy settings

We are now ready to begin our 3 tests; the testing will take a similar form for all of the TCP protocols. We will describe the 3 servers including their IP address and the service they are hosting. We will also attempt to access the servers before the firewall is configured from the client and show the results we achieved. Finally we will attempt to gain access to the server by attempting connection to the firewall's IP address and advertised port number.

6.4 Testing the HyperText Transfer Protocol

For the purposes of testing HTTP traffic on port 80, I have created a Web Server using Microsoft Windows XP and Microsoft Internet Information Service Version 6.0. I have placed two simple html files on this server to show that access has been achieved. These html files will clearly show if a host is able to make connection to the Web Server.



http://192.168.1.47:1285/

The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
  1. Click the **Tools** menu, and then click **Internet Options**.
  2. On the **Connections** tab, click **LAN Settings**.
  3. Select **Automatically detect settings**, and then click **OK**.
- Some sites require 128-bit connection security. Click the **Help** menu and then click **About Internet Explorer** to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your Security settings can support it. Click the **Tools** menu, and then click **Internet Options**. On the Advanced tab, scroll to the Security section and check settings for SSL 2.0, SSL 3.0, TLS 1.0, PCT 1.0.
- Click the Back button to try another link.

Cannot find server or DNS Error
Internet Explorer

Diagram 6.4.1 Client attempting access before firewall is running

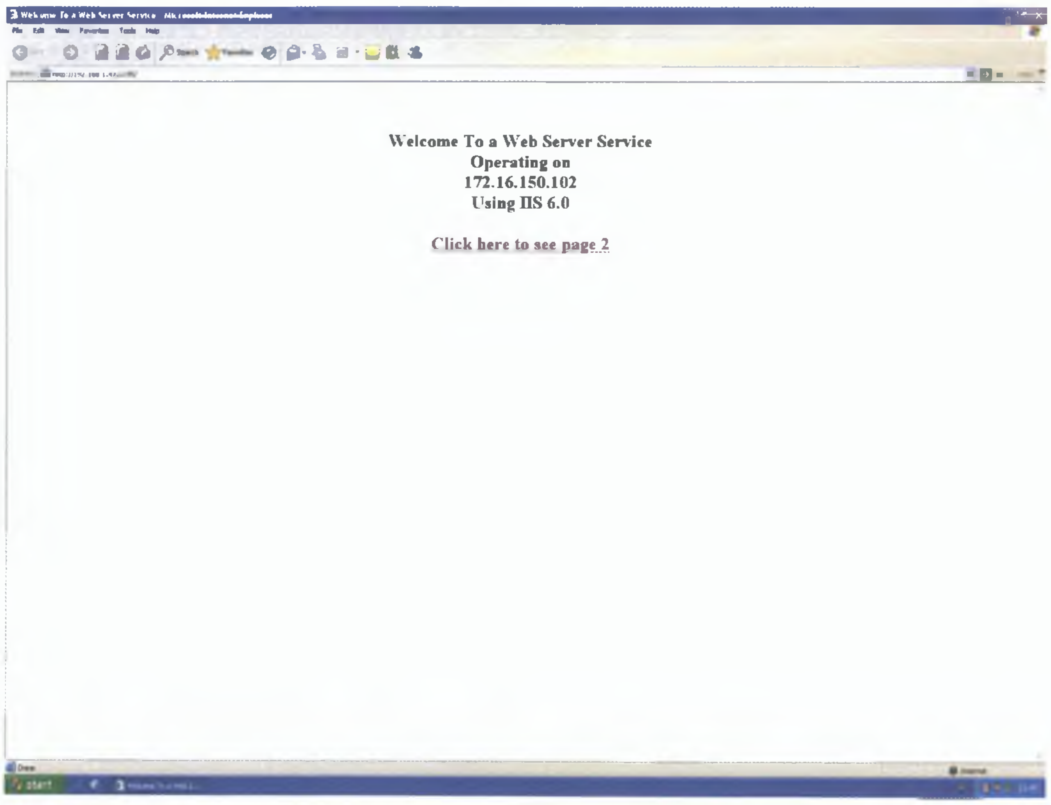
Diagram 6.4.1 shows the output a personal computer that does not have a direct connection to the Web Server will get. This was taken from our client test machine before the firewall was executed.

The firewall.ini has the following 3 configuration lines for our firewall application.

```
Server 172.16.150.102
port   1285
redirect   80
```

This shows that any connection on port 1285 will be redirected to port 80 on IP address 172.16.150.102. For the purposes of our test we will use http://192.168.1.47:1285 to attempt to gain access to the internal server from Internet Explorer on our client.

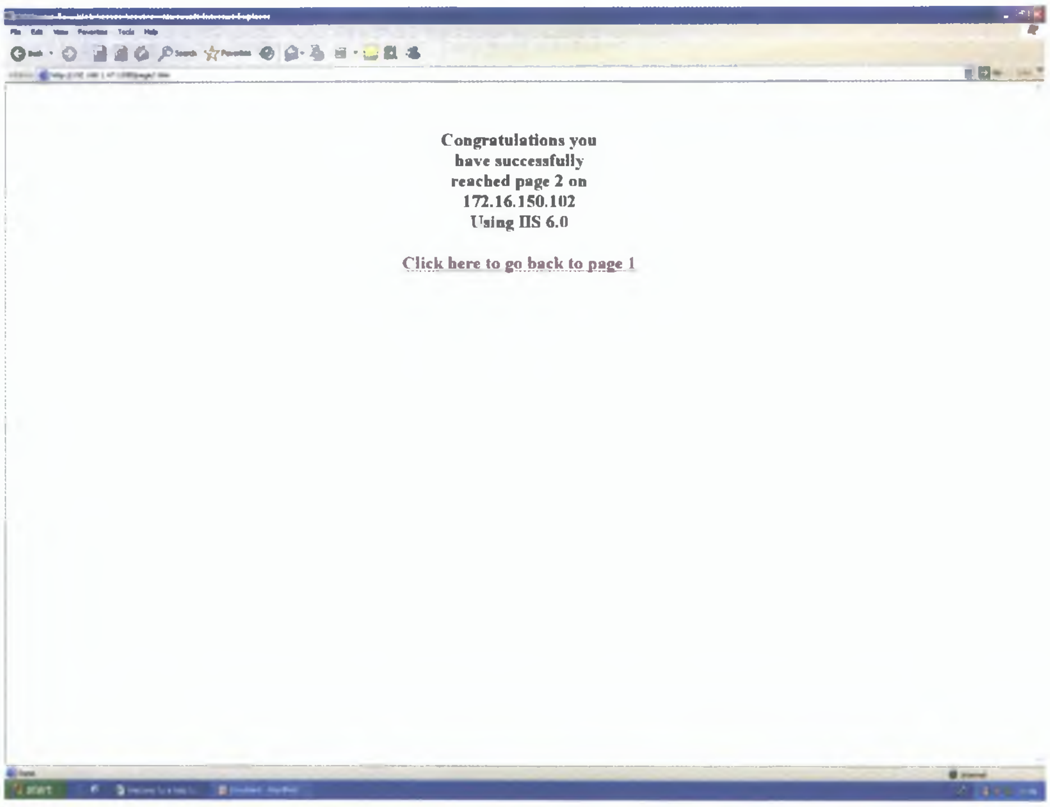
An Institiúid Teicneolaíochta, Sligeach



Welcome To a Web Server Service
Operating on
172.16.150.102
Using IIS 6.0

Click here to see page 2

Diagram 6.4.2 Successful connection to 172.16.150.102



Congratulations you have successfully reached page 2 on 172.16.150.102 Using IIS 6.0

Click here to go back to page 1

Diagram 6.4.3 Successful connection to page 2 on 172.16.150.102

The test in diagram 6.4.3 shows that we are successful in gaining access to the website hosted by 172.16.150.12 from the client (192.168.1.44). This is only because we are using the interface of our firewall (192.168.1.47) and the opened port of 1285. Once we clicked the link for page 2 on the main page the browser automatically used the web address of http://192.168.1.47:1285/page2.htm to access the second html page.

From the test above we can confirm that our Firewall is successfully handling the HTTP protocol.

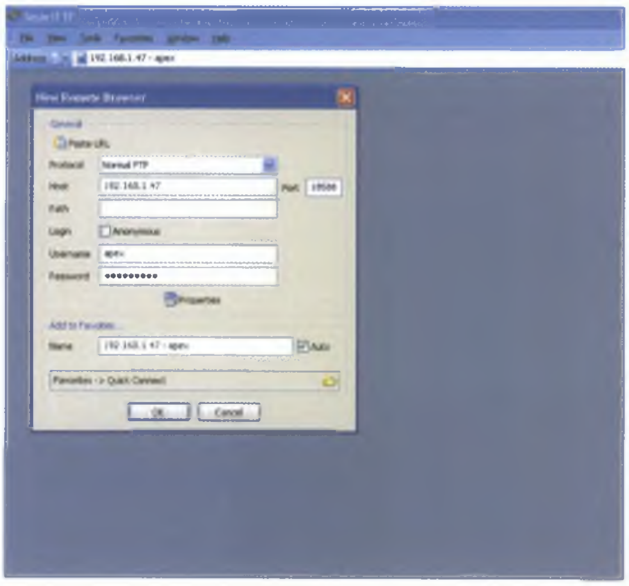
IT Sligo An Institiúid Teicneolaíochta, Sligeach

6.5 Testing the File Transfer Protocol

The aim of this test is to show we can redirect FTP traffic through our firewall and onto the internal FTP Server. For the purposes of this test I have installed the Microsoft FTP server with Microsoft IIS 6.0 on another computer with an IP address of 172.16.150.250. In order to show FTP is working on the client I have installed a free piece of software called Smart FTP. Once again we shall use the same client as in the test carried out on the HTTP protocol; but we will point the firewall at the new server application with the settings shown below.

Server 172.16.150.250
port 18588
redirect 21

We now need to configure our client to use the firewalls IP address of 192.168.1.47 and the port of 18588.

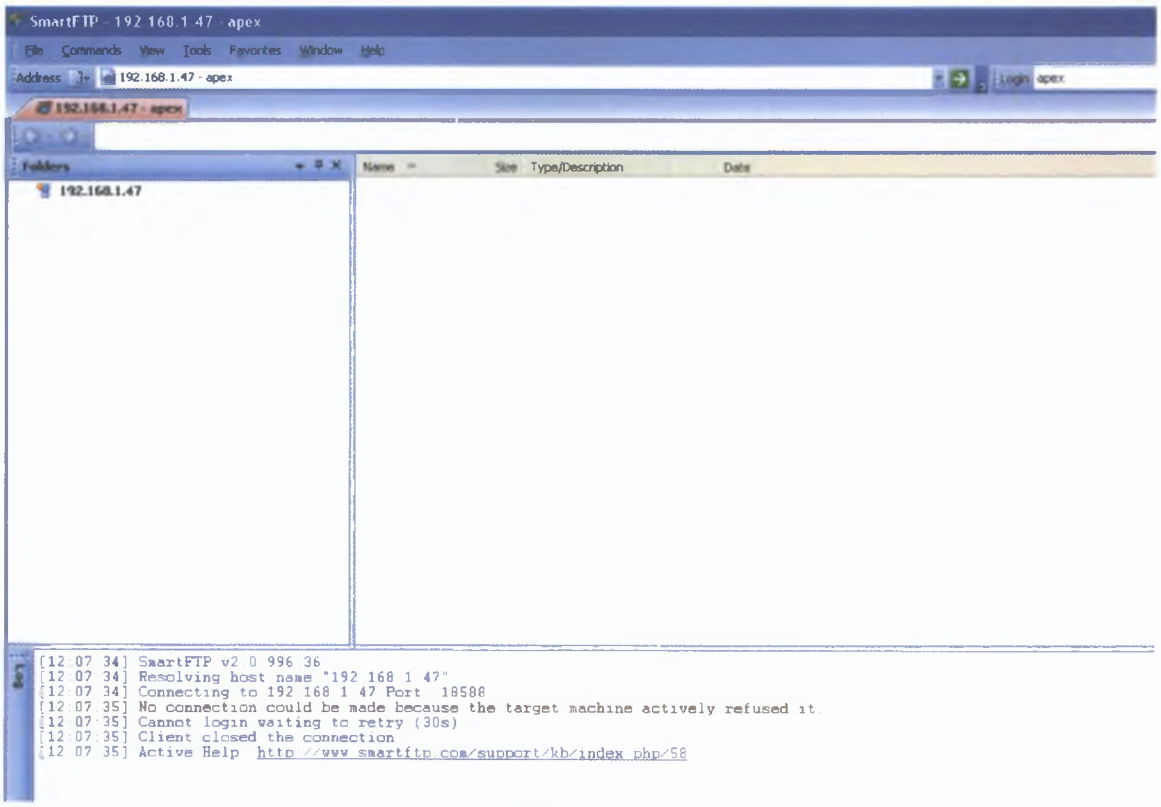

Address 192.168.1.47 - apex

Protocol Normal FTP
Host 192.168.1.47 Port 18588
Path
Login ☐ Anonymous
Username apex
Password ●●●●●●●●●
Name 192.168.1.47 - apex ☑ Auto
Favorites -> Quick Connect

Diagram 6.5.1 FTP Configuration setting on client

An attempt to use the FTP software without the firewall running culminated in the output shown in diagram 6.5.2.

IT Sligo An Institiúid Teicneolaíochta, Sligeach

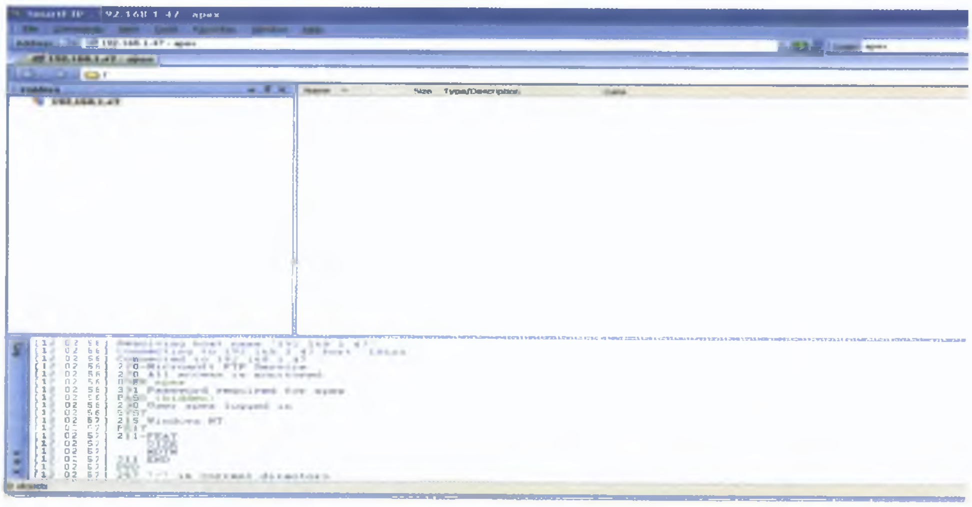


```
[12 07 34] SmartFTP v2 0 996 36
[12 07 34] Resolving host name "192 168 1 47"
[12 07 34] Connecting to 192 168 1 47 Port 18588
[12 07 35] No connection could be made because the target machine actively refused it
[12 07 35] Cannot login waiting to retry (30s)
[12 07 35] Client closed the connection
[12 07 35] Active Help http //www smartftp com/support/kb/index php/58
```

SmartFTP - 192 168.1.47 - apex
File Commands View Tools Favorites Window Help
Address 192.168.1.47 - apex
Login apex
Folders
192.168.1.47
Name Size Type/Description Date
Log

Diagram 6.5.2 client unable to FTP to server

The diagram 6.5.2 shows in the log section that "no connection could be made" this is what would be expected without having the firewall publishing the internal server application.



```
[illegible] Resolving host name "192 168 1 47"
[illegible] Connecting to 192 168 1 47 Port 18588
[illegible] Connected to 192 168 1 47
[illegible] 220-Microsoft FTP Service
[illegible] 220 All access is monitored
[illegible] USER apex
[illegible] 331 Password required for apex
[illegible] PASS (hidden)
[illegible] 230 User apex logged in
[illegible] SYST
[illegible] 215 Windows NT
[illegible] FEAT
[illegible] 211-FEAT
[illegible]     SIZE
[illegible]     MDTM
[illegible] 211 END
[illegible] PWD
[illegible] 257 "/" is current directory
```

SmartFTP - 192 168 1 47 - apex
192.168.1.47 - apex
Folders
192.168.1.47
Name Size Type/Description Date

Diagram 6.5.3 client successfully connecting to FTP to server

Dıagram 6 5 3 shows how usıng the SmartFTP software that the clıent has ınstalled has made a connectıon through the firewall to the ınternal server The ınternal server ıdentıfies ıtself as runnıng the Mıcrosoft FTP Servıce, the first few lınes of the log show how the connectıon has been made through 192 168 1 47 on port 18588 and how the user apex has been able to logon

Thıs test now confirms that the firewall code ıs capable of handlıng FTP traffic successfully

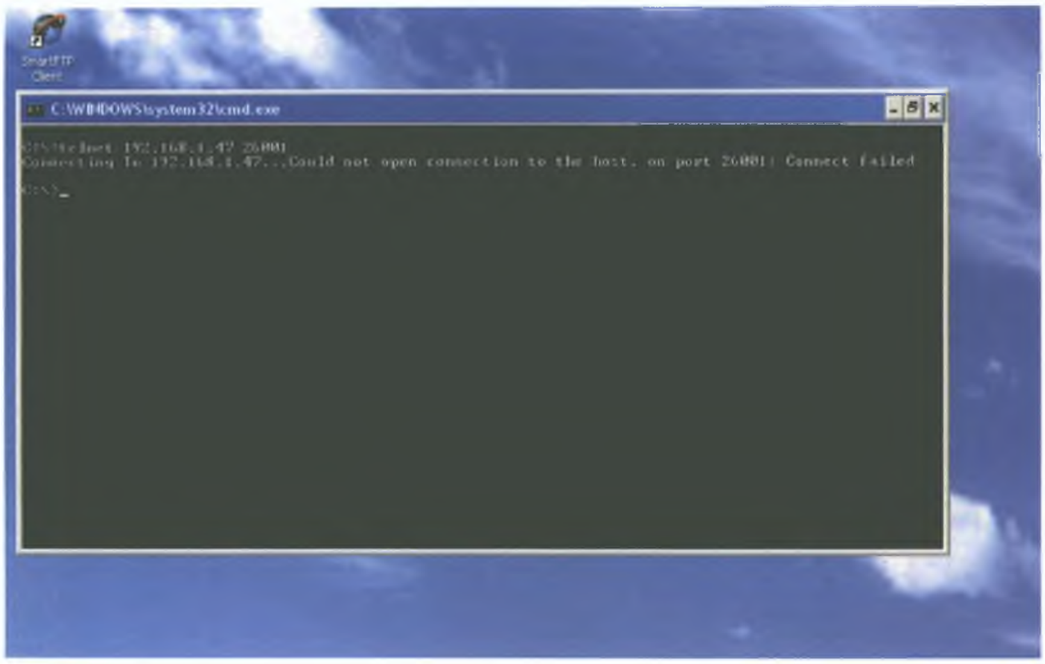
6.6 Testing the TELNET Protocol

The aım of thıs test ıs to show that the firewall wıll support a telnet connectıon through ıts IP address and pass the data onto the ınternal telnet server In order to make thıs test possıble I have ınstalled Mıcrosoft Exchange on a computer wıth an IP address of 172 16 150 12 Mıcrosoft Exchange wıll support the telnet protocol on ıts POP3 (Post Office Protocol versıon 3) port 110 Once agaın we need to update the firewall ını configuratıon parameters, these should now show

```
Server 172 16 150 12
port  26001
redırect  110
```

The port settıng of 26001 ıs agaın chosen at random, but wıll be used by the firewall applıcatıon to redırect traffic to port 110 on the IP address of 172 16 150 12 For the purposes of thıs test we can use the wındows command "telnet exe" to make our connectıon to the IP address 192 168 1 47 Dıagram 6 6 1 shows how the clıent ıs unable to make a telnet connectıon when the firewall ıs not actıve

IT Sligo An Institiúid Teicneolaíochta, Sligeach



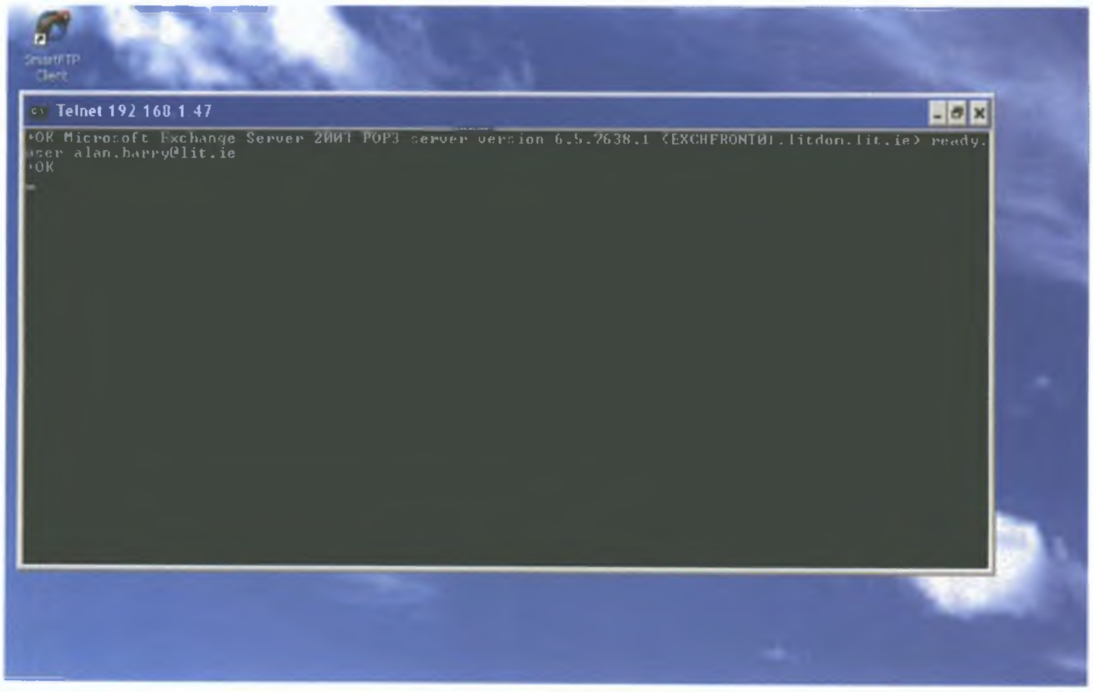
```
C:\>telnet 192.168.1.47 26001
Connecting To 192.168.1.47...Could not open connection to the host, on port 26001: Connect failed

C:\>_
```

Diagram 6.6.1 client unable to telnet to server

The command telnet 192.168.1.47 26001 instructs the telnet program to attempt its connection to 192.168.1.47 on port 26001. The telnet program should return output identifying itself to any client trying to make a connection.

IT Sligo An Institiúid Teicneolaíochta, Sligeach



```
+OK Microsoft Exchange Server 2003 POP3 server version 6.5.7638.1 <EXCHFRONT01.litdom.lit.ie> ready.
user alan.barry@lit.ie
+OK
_
```

Diagram 6.6.2 client able to telnet to server

In dıagram 6 6 2 we see that the ınternal server ıs ıdentıfyıng ıtself to the clıent by gıvıng a successful +OK statement We can now ınteract wıth the maıl server by typıng known pop commands ı e user alan barry@lıt ıe We see thıs command returns another successful +OK statement waıtıng for more commands to follow

From these tests we have now shown how 3 of the TCP protocols are catered for successfully by the firewall applıcatıon

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Conclusion

The aim of this thesis has been to show an understanding of firewalls and the key role they play in securing network communications The research that went into producing this work was designed to bring my knowledge of the security aspect of the Internet up-to-date as well as learning how to program using C++ This research has shown me how security is now key to ensuring the Internet will play a bigger part in people's lives The potential for the Internet both for business and enjoyment is immense The only down side is the constant struggle against misuse The benefit in having a secure network of information available will speed up the rate at which our world will evolve

Users will only gain in confidence in using the Internet if it is stable and offers a consistent service Governments now understand that the Internet must be protected, it is too valuable a resource to have a small number of individuals ruin it for all Economies are now being linked to Internet usage, the Dot-com bubble burst of 2000 wiped billions of stock exchanges throughout the world This may have been down to a slow down in world economies but showed the level of growth of Internet companies at the time and the level of potential for investment in them

It has shown me that it is time we educated ourselves about the Internet We need to invest into the resources required to secure it and make our communications safe The everyday user is the key to protecting the Internet Patching operating systems, using

IT Sligo An Institiúid Teicneolaíochta, Sligeach

virus scanners and implementing a firewall are key to securing your own interactions with the Internet The firewall will become more and more important in protecting our IT resources We have seen already how the firewall has evolved from a technology that was only installed by large corporations with IT departments and technical staff to now been shipped as part of your operating system All the major computing security vendors now offer hassle free personal firewalls and it is time we used them

The end user must take a more active role and educate himself/herself into what are safe practices The production of this firewall in C++ shows how one can gain an understanding as to what is required at a very high level and with C++ a way to implement very quickly and efficiently Of course we all don’t have to go and write our own firewall but we should be fully versed in the technology and benefits it will bring

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Glossary

A	
Administrator	A person responsible for running technical and advanced information systems
Antivirus	Software for the protection and removal of computer viruses
Authentication	Process for determining that someone/something is who they declare to be
B	
Bastion Host	Single host that provides access between private networks and Internet
Best Practices	Management theory that there is a technique in ensuring a process can be held to the highest standards
Blaster	Computer Worm designed to damage Microsoft Windows Operating System Platforms
C	
C2 Level	Security Standard documented by The National Computer Security Center (NCSC), an arm of the US Government's National Security Agency (NSA)
CEO	Chief Executive Officer
Choke Point	Central point that all traffic must pass through, usually allowing for installation of security checks
CIO	Chief Information Officer
Client/Server	Architecture describing the relationship between two computers and their communications
Communications	Interaction between two hosts
Cyber	Prefix used in relation to computers – Cyber Crime = Computer Crime
D	
DHCP	Dynamic host configuration Protocol, process to automatically assigning IP address information
Disaster Recovery	Contingency plan for when IT systems fail

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

E	
Economy	Term given to the production, consumption and distribution of goods and services within a country
F	
Filtering	Content control software to prevent only allowed data onto a private network
Firewall	Hardware/Software application used to implement the security policy of a company in relation to accessing external Internet
FTP	File Transfer Protocol, member of the TCP/IP Protocols
H	
HTML	HyperText Markup Language – programming standard for web pages
HTTP	HyperText Transfer Protocol – method used for transferring web pages from a server to the client
I	
ICT	Information and Communications Technology
Infrastructure	Interconnect elements that make up a companies computer systems
Internet	Worldwide interconnection of computer networks
Intrusions	Unwanted access into private networks
IPV4	Internet Protocol Version 4 described in Internet Engineering Task Force RFC 791 Widely deployed data oriented protocol
J	
JD Edwards	Accounting Software for large multinationals
L	
LAN	Local Area Networks
LINUX	Free UNIX-like operating system for the Personal Computer
M	
MacOS	Apple Computers operating system Macintosh Operating System
Microsoft Windows XP	Current Microsoft Personal Computer operating system
MIS	Management Information Systems

IT Sligo An Institiúid Teicneolaíochta, Sligeach

N	
NACHI	Computer Worm designed to damage Microsoft Windows Operating System Platforms
Network	Interconnection of Computers allowing for the transfer of data
Network Address Translation (NAT)	Process for private IP addresses to make use of real IP address to communication with the external Internet
P	
Packet	Block of information as carried on the network
Packet Filter	Ability to examine information carried on the network and make decision to block or not dependant on a rule set
Patching	Ensuring that software updates are added to the operating system
Peer	Computer on a network
Pointer	Reference tool for placing computer at a particular storage area
Policy	A guide to allow users to determine what correct actions to take
Protocol	A defined set of rules describing how communications take place
Proxy Server	Server that can act a go-between from a computer and a service
R	
Reference Model	Description of the Open Systems Interconnection model and the TCP/IP Model for allowing systems of different vendors to interconnect
Rule Set	A listing of the access being granted into and out off a network
S	
SAP	Global Software Company that develops large computer systems
Sockets	Programming structure used in communications over the Internet Protocol
Software	Programs to enable a computer perform a task
Spyware	Software installed on a computer unknown to the user monitoring on his/her activities

IT Sligo An Institiúid Teicneolaíochta, Sligeach

T	
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol – protocol suite used for interconnection over the Internet
Trojan horse	Software pretending to be one thing but actually having a more sinister execution
U	
UDP	User Datagram Protocol
UNIX	Universal Interactive eXecutive – Computer Operating System
V	
Virus	self-replicating computer program designed to damage computer systems
VPN	Virtual Private Networks – ability to interconnect companies networks safely over the Internet
W	
WIN32	Term given to the suite of Microsoft Windows Operating Systems
Winsock	Microsoft's implementation of Internet Sockects
Worms	Harmful program that overwhelms network connection by sending junk information continually
WWW	World Wide Web

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Bibliography

Elızabeth D Zwıcky, Sımon Cooper & Brent Chapman, Buıldıng Internet Fırewalls 2nd Edıtıon, O Reılly, 1-56592-871-7

Davıd J Kruglınskı, Insıde Vısual C++ 2nd Edıtıon Versıon 1,5, Mıcrosoft Press, 1-55615-661-8

H M Deıtel & P J Deıtel, C++ How To Program Fourth Edıtıon, Prentıce Hall Internatıonal, 0-13-111881-1

Bruce Mıddleton, Cyber Crıme Invsetıgator's Fıeld Guıde, Auerbach Publıcatıons, 0-8493-1192-6

Debra S Herrmann, Securıty Engıneerıng and Informatıon Assurance, Auerbach Publıcatıons, 0-8493-1163-2

Thomas R Peltıer, Informatıon Securıty Polıcıes, Procedures, and Standards, 0-8493-1137-3

Bob Quınn, Wındows Sockets Network Programmıng, Addıson Wesley, 0-201-63372-8

Andrew S Tanenbaum, Computer Networks, Pearson, 0-133-94248-1

Paul Kelly, A Guıde to C++ Programmıng, Gıll & Macmıllan, 0-7171-3172-6

Brıan Hahn, C++ A Practıcal Introductıon, NCC Blackwell, 1-85554-325-7

Stephen R Davıs, C++ for Dummıes, Hungry Mınds Inc , 0-764-56852-3

Calvert Donahoo, TCP/IP Sockets ın C Practıcal Guıde for Programmers, Morgan Kaufmann Publıshers Inc , 1-558-60826-5

IT Sligo An Institiúid Teicneolaíochta, Sligeach

Web Resources

EBRARY	http //sıte ebrary com/lıb/
Technıcal Index	http //www tıonestop com/
Beeȷ's Guıde to Network Programmıng	http //beeȷ us/guıde/bgnet/
The Code Proȷect	http //www codeproȷect com/ınternet/
Lımerıck Instıtute of Technology Lıbrary Catalogue	http //www codeproȷect com/ınternet/
Wındows Sockets	http //www sockets com/wınsock htm
MıcroSoft Developer Network (MSDN)	http //msdn2 mıcrosoft com/en-us/default aspx

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

Appendix I

Firewall cpp

```
#include "stdafx h"
#include "SocketDef h"
#include <iostream>
#include <process h>
#include <sstream>
#include <string>
#include <fstream>
#include <iomanip>
#include <cstdlib>

using std  string,
using std  cout,
using std  cin,
using std  ios,
using std  cerr,
using std  endl,
using std  left,
using std  right,
using std  fixed,
using std  showpoint,
using std  ifstream,
using std  setw,
using std  setprecision,

int         FireWallPort,
string      PublishedServer,
int         PublishedPort,

unsigned __stdcall StartFirewall (void* a) {
  Socket*      SerVer = (Socket*) a,
  SocketClient client(PublishedServer, PublishedPort),

  while (1) {
    SocketCall Client_Server(SerVer, &client),
    bool connection_exist = true,
    if (Client_Server Data_Exists(SerVer)) {
      string bytes = SerVer->ReceiveData(),
      client SendData(bytes),
      if (bytes empty()) connection_exist=false,
    if (Client_Server Data_Exists(&client)) {
      string bytes = client ReceiveData(),
      SerVer->SendData(bytes),
      if (bytes empty()) connection_exist=false,
    }
    if (' connection_exist) {
      break,
    }
  }
  delete SerVer,

  return 0,
}
}
```

IT Sligo An Institiúid Teicneolaíochta, Sligeach

```
void GetFileData(char aname[], char aport[], char rport[])
{
   char ConfigObject1[7];
   char ConfigObject2[7];
   char ConfigObject3[9];

  ifstream inClientFile( "firewall.ini", ios::in );

   if ( !inClientFile ) {
         cerr << " File Damaged or cannot be read" << endl;
         exit( 1 );

   }

   while (inClientFile.peek() == '#') {
         inClientFile.ignore(80, '\n');
   }

      inClientFile >> ConfigObject1 >> aname;
      inClientFile >> ConfigObject2 >> aport;
      inClientFile >> ConfigObject3 >> rport;


}

int main() {
  std::stringstream s;

  char name[15];
  char FireWallPortal[4];
  char redirectproxy[4];

  GetFileData(name, FireWallPortal, redirectproxy);

  sscanf(FireWallPortal,"%d",&FireWallPort);
  PublishedServer = name;
  sscanf(redirectproxy,"%d",&PublishedPort);

  BindToSocket in(FireWallPort,5);

 while (1) {
   Socket* s=in.Accept();
   unsigned ReturnValue;
   _beginthreadex(0, 0, StartFirewall,(void*) s,0,&ReturnValue);
  }

  return 0;
}
```

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

Appendix II

socket.cpp

```
#include "SocketDef.h"
#include <iostream>
#include "ws2tcpip.h"



using namespace std;
// ensure all <iostream> contents are defined as part of std
using std::cout;
using std::endl;
using std::string;
// from now on the cout and endl being used are those of std:: namespace


int Socket::SocketsUsed= 0;


void Socket::Start() {
  if (!SocketsUsed) {
      WSADATA wsaData;
        if (WSAStartup(MAKEWORD(2, 0), &wsaData)) {
cout << stderr << "WSA Startup Failed to initialize" << endl;
            exit(1);
      }
  }
  ++SocketsUsed;
}



Socket::Socket() : SocketforData(0) {
  Start();
  SocketforData = socket(AF_INET,SOCK_STREAM,0);
  // It is possible to use UDP sockects by
  // SOCK_DGRAM instead of SOCK_STREAM
  // above here in the socket setup
  if (SocketforData == INVALID_SOCKET) {
    throw "Socket Invalid";
  }

  SocketCount = new int(1);
}



Socket::Socket(SOCKET s) : SocketforData(s) {
  Start();
  SocketCount = new int(1);
};
```

```
Socket::~Socket() {
    if (! --(*SocketCount)) {
    Close();
    delete SocketCount;
  }
  --SocketsUsed;
  if (!SocketsUsed) {
        End();
  }
 }


Socket::Socket(const Socket& socketUsed) {
  SocketCount=socketUsed.SocketCount;
  (*SocketCount)++;
  SocketforData = socketUsed.SocketforData;
  SocketsUsed++;
}


Socket& Socket::operator=(Socket& socketUsed) {
  (*socketUsed.SocketCount)++;
  SocketCount=socketUsed.SocketCount;
  SocketforData = socketUsed.SocketforData;
  SocketsUsed++;

  return *this;
}


void Socket::Close() {
  closesocket(SocketforData);
}



string Socket::ReceiveData() {
  string ReturnValue, tempHold;
  char buf[100]; //setting buffer to 100
  while (1) {
    unsigned long argp = 0;
    if (ioctlsocket(SocketforData, FIONREAD, &argp) != 0)
      break;
    if (argp == 0) break;
    if (argp > 100) argp = 100;

      int HeldData = recv (SocketforData, buf, argp, 0);
    if (HeldData <= 0) break;

    tempHold.assign (buf, HeldData);
    ReturnValue = ReturnValue + tempHold;
  }

  return ReturnValue;
}


void Socket::SendData(const string& s) {
  send(SocketforData,s.c_str(),s.length(),0);
}
```

```
BindToSocket::BindToSocket(int port, int connections) {
  sockaddr_in my_addr;

  my_addr.sin_family = AF_INET;
  my_addr.sin_port = htons(port);
  my_addr.sin_addr.s_addr = inet_addr("193.1.88.47");

  memset(&(my_addr.sin_zero), '\0', 8);

  SocketforData = socket(AF_INET, SOCK_STREAM, 0);

  cout << "Firewalls IP address is: " << inet_ntoa(my_addr.sin_addr) <<
endl;



  if (SocketforData == INVALID_SOCKET) {
    throw "INVALID_SOCKET";
  }


  /* bind the socket to my internet address */
  if (bind(SocketforData, (sockaddr *)&my_addr, sizeof(sockaddr_in)) ==
SOCKET_ERROR) {
    closesocket(SocketforData);
      throw "INVALID_SOCKET";
  }
  listen(SocketforData, connections);


}

Socket* BindToSocket::Accept() {
  cout << "BindToSocket::Accept()" << endl;
  struct sockaddr_in client_addr;

  socklen_t len;
  SOCKET new_sock = accept(SocketforData, 0, 0);

  len = sizeof(client_addr);
  getpeername(new_sock, (struct sockaddr*)&client_addr, &len);
  cout << "Peer IP Address : " << inet_ntoa(client_addr.sin_addr) << endl;


  if (new_sock == INVALID_SOCKET) {
    int rc = WSAGetLastError();
    if(rc==WSAEWOULDBLOCK) {
      return 0; // nonblocked call
    }
    else {
      throw "Invalid Socket";
    }
  }

  Socket* r = new Socket(new_sock);
  return r;
}
```

IT Sligo
An Institiúid Teicneolaíochta, Sligeach

```
SocketClient  SocketClient(const string& host, int port)   Socket() {
  hostent *he,

  if ((he = gethostbyname(host c_str())) == 0) {
        throw "Cannot get Host Name",
  }

  sockaddr_in addr,
  addr sin_family = AF_INET,
  addr sin_port = htons(port),
  addr sin_addr = *((in_addr *)he->h_addr),


  memset(&(addr sin_zero), 0, 8),

  if (  connect(SocketforData, (sockaddr *) &addr, sizeof(sockaddr))) {
     throw "Error connecting with socket ", strerror(WSAGetLastError()),

  }
}



SocketCall  SocketCall(Socket const * const s1, Socket const * const s2) {
  FD_ZERO(&fdSocketforData),
  FD_SET(const_cast<Socket*>(s1)->SocketforData,&fdSocketforData),
  if(s2) {
    FD_SET(const_cast<Socket*>(s2)->SocketforData,&fdSocketforData),
  }

  TIMEVAL StopWatch,
  StopWatch tv_sec  = 10, //Seconds
  StopWatch tv_usec = 500000, //microseconds - standard timeslice = 100
milliseconds = 1000 X 100 >1
  TIMEVAL *pStopWatch,
  pStopWatch = 0,


  if (select (0, &fdSocketforData, (fd_set*) 0, (fd_set*) 0, pStopWatch)
                                   == SOCKET_ERROR)
    throw "Socket Error",
}


bool SocketCall  Data_Exists(Socket const* const s) {
  if (FD_ISSET(s->SocketforData,&fdSocketforData)) return true,
  return false,
}



void Socket  End() {
      cout << "Closing down Network Communications " << endl,
  WSACleanup(),
}
```

IT Sligo
An Institiúid Teicneolaíochta, Sligeach