AUDITING VALIDITY ON THE INTERNET WITH SPECIFIC REFERENCE TO FIREWALLS

BY

BRUCE CAMERON YOUNG

SHORT DISSERTATION

PRESENTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR

THE DEGREE

MASTER OF COMMERCE

IN

COMPUTER AUDITING

IN THE

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

AT THE

RAND AFRIKAANS UNIVERSITY

STUDY LEADER : PROF. A. DU TOIT

GAUTENG
NOVEMBER 1997

DECLARATION

I declare that this short dissertation hereby submitted to the Rand Afrikaans University for the degree of Master of Commerce, except to the extent acknowledged in the text, is my own unaided work and has not been submitted previously for any degree to any other university.

BRUCE CAMERON YOUNG

ACKNOWLEDGEMENTS

First and foremost, I would like to thank the Lord of my life, Almighty God, and the loves of my life, both Sharon and Honré, for their inspiration and support.

In addition, I would like to express my gratitude to :

Professor Anton du Toit and Professor Willie Boshoff for all their assistance and guidance;

Ernst & Young for sponsoring the research.

CONTENTS

OPSOMMING

GELDIGHEIDSOUDITERING OP DIE INTERNET, MET SPESIFIEKE VERWYSING NA KEERWALLE

DEUR

BRUCE YOUNG

OPSOMMING VAN DIE SKRIPSIE INGEDIEN VIR DIE GRAAD MAGISTER COMMERCII IN REKENAAROUDITERING IN DIE FAKULTEIT EKONOMIESE EN BESTUURWETENSKAPPE AAN DIE RANDSE AFRIKAANSE UNIVERSITEIT

STUDIELEIER : PROF A DU TOIT

GAUTENG

NOVEMBER 1997

GELDIGHEIDOUDITERING OP DIE INTERNET, MET SPESIFIEKE VERWYSING NA KEERWALLE

In hierdie opsomming word die agtergrond, metodiek en gevolgtrekking uiteengesit van die navorsing wat oor die ouditering van die Internet (met spesifieke verwysing na keerwalle), gedoen is. Dit word onder die volgende opskrifte bespreek:

1. **PROBLEEMOMSKRYWING EN DOEL VAN DIE NAVORSING**
2. **NAVORSINGSMETODIEK**
3. **BEPERKINGS EN UITSLUITINGS**
4. **RESULTATE**
5. **GEVOLGTREKKING**

Waar die Afrikaanse terminologie tekort skiet is die Engelse ekwivalent tussen aanhalingstekens aangedui.

1. PROBLEEMOMSKRYWING EN DOEL VAN DIE NAVORSING

As gevolg van die ekonomiese voordele van handeldryf wat besig is om op die Internet pos te vat, groei die Internetgebruik tans eksponensieel. Die gebruik van die Internet vir advertensiesdoeleindes, bestellings, die opsporing van goedere en betaling gaan 'n verandering teweeg bring in die

bestaande besigheidspraktyke. Die Internet het begin om kopers en verkopers op 'n internasionale vlak met mekaar in verbinding te bring. Tradisionele roetes soos winkelsentrums, katalogusse en selfs die verskyning van direkte televisiebemarking word vervang deur elektroniese kliëntesteun, elektroniese data uitruiling, elektroniese bankwese en finansiële dienste, elektroniese geld en produkverspreiding. Ten spyte van die gebruik van komplekse tegnologie, word daar steeds van ouditeure verwag om die beheeromgewing van organisasies te evalueer wat hulle oudit, sodat hulle 'n onafhanklike opinie oor die finansiële jaarstate kan gee. Dit beteken dat addisionele finansiële en elektroniese blootstellings deur die organisasie in ag geneem moet word soos byvoorbeeld: verandering van finansiële state; verduistering van fondse; vervalsing van geld; en identiteitsbedrog met die doel om finansiële transaksies te doen.

Bestuur bly verantwoordelik vir die implementering van voldoende, effektiewe beheer en ouditeure is verantwoordelik vir die evaluering daarvan. Bernstein beskryf die druk van 'n knoppie as 'n manier om 'n wêreldwye transaksie te inisieer wat òf as 'n winsgewende onderneming òf as 'n finansiële fiasko kan eindig. Die spoed van vandag se elektroniese kommunikasie sluit die moontlikheid uit dat iets per hand onderskep kan word. Dit alles verhoog die risiko wat die ouditeur in die gesig staar (Bernstein, et al.1996:21).

Schwartau beskryf die ouditering van die Internet as 'n nuwe probleem wat nuwe tegnieke vereis waarin baie ISACA (*Information Systems Audit and Control Association*) lede betrokke sal wees. Hy vra homself of waarmee hulle te kampe sal kry en wat die uitdagings is wat hulle sal teëkom. Schwartau is van mening dat wanneer die fases van ouditering, eksperimentering en pogings tot die inbou van sekuriteit op die Internet begin word, sal rekenaarouditeure en beheerspesialiste na vandag terugkyk en besef dat die huidige benadering veel eenvoudiger is. Hy bevraagteken rekenaarouditeure en beheerspesialiste se hantering daarvan, aangesien die reëls besig is om drasties te verander (Schwartau, 1996:10).

Die doelwit van hierdie skripsie is om riglyne te verskaf aan die rekenaarouditeur, met spesifieke beperkinge en uitsluitings. Dit word gedoen om hom in staat te stel om 'n ouditering te doen van die beheer wat deur bestuur geïmplementeer is, waar hulle gebruik maak van keerwal ("firewall") tegnieke. Sodoende word die geldigheid verseker van Internetpakkette ("Internet packets") waar dit versend word tussen eksterne netwerke en die organisasie se interne netwerke.

2. NAVORSINGSMETODIEK

'n Literatuurstudie van bestaande gesaghebbende handboeke en ander literatuur beskikbaar oor die Internet en keerwalle is onderneem. Met die inligting verkry uit die literatuurstudie, is omvattende riglyne ontwikkel om die rekenaarouditeur te help met die ouditering van so 'n omgewing.

3. BEPERKINGS EN UITSLUITINGS

Dié skripsie fokus op geldigheid, soos wat dit van toepassing is op eksterne gebruikers wat toegang verkry tot die Internet, van buite die organisasie. Die gebruik van anonieme Internetdienste, soos wanneer eksterne gebruikers toegang verkry tot 'n interne anonieme "File Transfer Protocol (FTP)" lêerbediener of 'n "Hipertext Transfer Protocol (HTTP)" lêerbediener, sowel as interne gebruikers wat toegang verkry tot die Internet van binne die organisasie, is binne die bestek van hierdie skripsie.

Hierdie skripsie handel nie oor die geldigheid van nie-anonieme dienste (of te wel gevalideerde dienste/ "authorised services") waar interne gebruikers toegelaat word om toegang te verkry tot die organisasie se stelsels en die gebruiker buite die organisasie, of elders op die Internet geleë is, nie.

Dié skripsie aanvaar dat die organisasie 'n goedgekeurde en gedokumenteerde sekuriteitsbeleid en riglyne het, wat 'n keerwalbeleid insluit. Die skripsie aanvaar ook dat die organisasie neergelegde riglyne het oor die Internetdienste wat hulle aan hulle gebruikers beskikbaar stel.

Hierdie navorsing is verder beperk tot die twee mees populêre keerwaltegnieke naamlik, pakketfiltrering ("packet filtering") en proksiedienste ("proxy services").

Bogenoemde uitsluitings en beperkings kan gebruik word vir toekomstige navorsing.

4. RESULTATE

Keerwalle is 'n meganisme wat beskerming kan verleen en skeiding tussen 'n organisasie se betroubare, interne netwerke en die onbetroubare Internet kan bewerkstellig. Die organisasie moet 'n beleid sowel as reëls en regulasies neerlê wat sal verseker dat slegs geldige en gemagtigde Internetverkeer toegelaat word om deur die keerwalle te beweeg. Die keerwalle is die organisasie se hoofinstrument om beleid af te dwing.

Keerwalle gebruik gewoonlik òf pakketfiltrering òf proksiedienste ten einde transmissie te beveilig. Hierdie twee metodes word in detail ondersoek.

'n Omvattende stel riglyne is vir die rekenaarouditeur ontwikkel, ten einde hom in staat te stel om die geldigheidsbeheer te evalueer wat geïmplementeer is met behulp van keerwaltegnieke. Die riglyne stel die rekenaarouditeur in staat om die komplekse omgewing van 'n keerwalinstallasie te evalueer om sodoende te verseker dat slegs geldige Inligtingspakkette ("information packets") versend word, konneksies met die Internet gemaak word en dienste, in ooreenstemming met die organisasie se Internet-sekuriteitbeleidsdokumente en prosedures, verskaf word.

Die riglyn ondersoek die volgende areas:

Riglyne met betrekking tot netwerktopologie word aangespreek om die rekenaarouditeur van hulp to wees t.o.v. waar die belangrike Internetkonneksies in verhouding tot mekaar geleë is, om die sekuriteitfilosofie in gebruik te verstaan, en om leemtes wat tot ongeldige aktiwiteite mag lei, te identifiseer.

Ten einde die geldigheidsdoelwit te verseker wanneer die Internet gebruik word, is dit nodig om streng beleid en riglyne neer te lê wat die raamwerk daarstel om omstandighede te beheer waarin die organisasie werksaam is. Om bogenoemde te bereik word riglyne verskaf om die organisasie se netwerksekuriteit te ondersoek ten einde vas te stel wat die organisasie se

beleid is met betrekking tot Internetdienste, sekuriteitsvereistes, private toegang, verantwoordelikheid, validasie en die monitor van oortredings.

'n Verdere area wat die rekenaarouditeur ondersoek, is die proses rondom die opstel van reëls vir pakketfiltrering. Riglyne is ontwikkel om met die verifikasie en die versekering behulpsaam te wees, sodat die kliënt se prosesse in ooreenstemming met goeie praktyk is.

'n Beheerlys is ontwikkel om vas te stel of die keerwal die vermoë het om die verlangde vlak van beheer en kontrole te verskaf.

Pakketfiltreringreëls word afgedwing om geldigheid te verseker en om die organisasie se netwerksekuriteitsbeleid te reflekteer en is daarom fundamenteel om te verseker dat alle netwerkverkeer geldig is. 'n Voorgestelde riglyn word aan die ouditeur verskaf om die pakketfiltreringreëls te verifieer, die toepaslikheid daar van te evalueer en te verseker dat slegs geldige inligting versend en slegs geldige dienste verskaf word.

Die rekenaarouditeur moet toesien dat 'n joernaal van die aktiwiteite van die keerwal bygehou word. Riglyne waarna die ouditeur moet oplet word in hierdie afdeling gelys.

5. GEVOLGTREKKING

Die Internet besit 'n fenomienale potentiaal om die wyse waarop organisasies besigheid doen, te verbeter. Bykomstige beheer- en risiko-oorwegings word egter ook teweeggebring.

Ter opsomming verskaf hierdie navorsing 'n stel riglyne 'n basis aan die rekenaarouditeur om die geldigheidsbeheerdoelwit te ouditeer soos wat dit geïmplementeer word met behulp van keerwaltegnieke.

Die riglyne is nie veronderstel om 'n allesomvattende lys van items te wees wat oorweeg behoort te word wanneer 'n oudit gedoen word nie. Die spesifieke omstandighede van die toepaslike Internetimplementering moet in ag geneem word.

Hierdie skripsie het die weg gebaan vir nuwe velde in akademiese navorsing. Moontlikhede vir verdere navorsing sluit in:

* Die ouditering van volledigheid en akkuraatheid van transaksies oor die Internet;
* Die ouditering van, en verifiëring van nie-anonieme dienste op die Internet;
* Die ouditeur se rol in die ontwikkeling en opstel van Internetsekuriteitbeleid t.o.v. prosedures; en

* Gedetailleerde analise van die risikos as gevolg van die gebruik van verskeie Internetdienste;

SYNOPSIS

1. PROBLEM DESCRIPTION AND OBJECTIVE OF THIS SHORT DISSERTATION

Use of the Internet is currently exploding, with the commercial benefits of trading on the Internet beginning to take off.

Management are still responsible for the implementation of adequate and effective controls, and auditors the evaluation thereof. To add to the risk that the auditor faces, at "the click of a button, we can initiate a worldwide transaction that will result in a profitable venture or a financial disaster. The speed of today's electronic communications precludes manual interception" (Bernstein, et al. 1996:21).

The objective of this dissertation is to provide guidelines to the information systems auditor (ISA), to audit the controls implemented by management using firewall techniques, and the policies and procedures controlling the firewalls, to ensure the validity of Internet packets passed between the external network and the enterprise's internal network with specific limitations and exclusions.

2. RESEARCH METHODOLOGY

A literature survey has been performed on existing authoritative textbooks and other literature available on the Internet and firewalls.

With all the information obtained from the literature survey, comprehensive guidelines were developed to assist the information systems auditor tasked with auditing the environment.

3. SCOPE AND LIMITATIONS

This short dissertation deals with validity, as it relates to external users accessing the Internet from outside the organisation. Included in this scope is the provision of anonymous Internet services.

Further, the research is limited to the two most commonly used firewall techniques, namely packet filtering and proxy services, and will not cover a specific firewall software product, but deal with the concept generically.

4. RESULTS

A firewall is a mechanism which protects and separates the organisation's trusted internal network, and the untrusted Internet. The enterprise needs to set up policies, procedures, and rules to ensure that only valid or authorised Internet traffic is allowed to pass through the firewall. The firewall is the chief instrument used to enforce the organisation's policy.

Firewalls typically use two techniques of securing the transmission, namely packet filtering and proxy services, and these two methods are examined in detail.

A comprehensive set of guidelines has been developed for the ISA to evaluate validity controls implemented by means of firewall techniques.

The guidelines provide the ISA with a means of evaluating the complex environment of a firewall implementation to ensure that valid and only valid information packets are transmitted, only valid connections are made to the

Internet, and only valid services provided in terms of the organisation's Internet security policies and procedures.

5 CONCLUSION

The potential the Internet offers as a means of improving and advancing the means of business is phenomenal. On the other hand, additional control and risk considerations have been introduced.

In summary, this research has provided a set of guidelines for the information systems auditor, as a basis for auditing the validity control objective, as implemented by firewall techniques.

The guidelines are not meant to be an all inclusive or exhaustive list of items to consider while auditing, and must be applied to the specific circumstances that prevail at each Internet implementation.

This dissertation has opened up new fields of academic research. Further fields for research include:

* Auditing accuracy and completeness on the Internet;

* Auditing the provision of authenticated or non-anonymous services on the Internet;
* The auditor's role in developing Internet security policies and procedures; and
* Detailed analysis of the risks resulting from the use of various Internet services.

CHAPTER 1

INTRODUCTION

CONTENTS PAGE

1.1 BACKGROUND

The "Internet" has proliferated dramatically over the past few years and months. It is seldom that one reads a newspaper or magazine, watches a television program or listens to the radio, without noting some reference to the Internet being made. Its use until recently has been limited, in the main, to posting information on the myriad of home pages which are available to the many who spend late nights "surfing the net". This passive use, however, is changing.

"This has been the year that the mainstream discovered the Internet. Demand for Internet-based services is exploding, and both large and small companies are getting into the act" (Ernst & Young, 1997:60).

It is estimated that there will be $186 billion in annual electronic commerce volume by the millennium. As organisations connect and take advantage of the opportunities made available by the information superhighway, they will find they are involved with a "threat multiplier." The network environment today involves heterogeneous networks, internal networks, different operating systems, LANs, WANs, routers, bridges, and a variety of equipment that has grown independently without necessarily any centralised thought. The enterprise networks of today have traditionally been fairly contained. When the enterprise takes advantage of the benefits which the Internet promises, the enterprise is automatically exposed to over forty

million people across the world . New buzz words abound, and add to the technical cloud which surrounds the Internet. GAN's, or global area networks, expand the geographical boundaries previously held by WAN's.

1.2 PROBLEM DESCRIPTION

Use of the Internet is currently exploding, with the commercial benefits of trading on the Internet beginning to take off. Using the Internet to advertise, order, track and pay for goods is going to change the face of how business is to be conducted. It is beginning to connect buyers and sellers directly on a world-wide basis. Traditional vehicles such as shopping malls, catalogues and the recent innovation of television direct marketing are being left behind, to be replaced by electronic customer support, electronic data interchange, electronic banking and financial services, electronic money and product dissemination, to name but a few of the uses.

Despite the use of this complex technology, auditors are still required to evaluate the control environment of the organisations they audit, which enables them to express their independent opinion on the annual financial statements. This means taking into account the additional financial and electronic commerce-related exposures that may entail an enterprise's financial statements being altered, funds being embezzled, money counterfeited, or someone impersonating an individual and performing

financial transactions in someone else's name, to list but a few of the additional risk factors to be considered.

As Ernst & Young (1997:61) put it:, "The public status of the Internet raises formidable issues regarding the security of information and payments", and "bank expenditures tied to the development and maintenance of Internet capabilities will rise more than 500% over the coming three years", which guarantees the existence of this risk, both presently, and increasingly in the future. Every transaction passes through a number of different servers, each of which can potentially be compromised. In addition, as the Internet is still so new, standards have yet to be developed and accepted by the business community.

The 1996 Business Week/Ernst & Young survey indicated that 8% of respondents experienced an attempted break-in via the Internet. The notorious hacker Kevin Mitnick, convicted twice, used the Internet to gain access to corporate networks and also to steal 30 000 credit card numbers (Bernstein, Bhimani, Schultz and Siegel, 1996:21).

Management are still responsible for the implementation of adequate and effective controls, and auditors the evaluation thereof. To add to the risk that the auditor faces, at "the click of a button, we can initiate a world-wide transaction that will result in a profitable venture or a financial disaster. The

speed of today's electronic communications precludes manual interception" (Bernstein, et al. 1996:21).

Auditing the information superhighway is a new problem that requires new tools and it is very likely that many ISACA (Information Systems Audit & Control Association) members are going to be involved in this task. After beginning to audit, look at, play with and secure the information superhighway, IS (Information systems) control professionals will look back and realise that it was far easier in the past to audit information system environments (Schwartau, 1996:10).

On the one hand businessmen have seen advances and improvements in the way they do business (Stair, 1992:644). On the other hand new and additional risk and control considerations and implications for audit professionals have been introduced (The Institute of Internal Auditors Research Foundation, 1994b:1-25).

1.3 OBJECTIVE OF THIS RESEARCH

The objective of this dissertation is to provide guidelines to the information systems auditor (ISA) to audit the controls implemented by management using firewall techniques, and the procedures controlling the firewalls, to ensure the validity of Internet packets passed between the external network and the enterprise's internal network with specific limitations and exclusions.

Chapter 5 provides the ISA with a guideline listing the issues to review. Upon performing an assessment following the guidelines, the ISA will be in the position to assess whether the risks relating to validity are reduced to an acceptable level, through the effective use of the techniques presented by firewalls.

1.4 SCOPE, LIMITATIONS AND EXCLUSIONS

This short dissertation deals with validity, as it relates to external users accessing the Internet from outside the organisation. Included in this scope is the provision of anonymous Internet services, such as users from the outside accessing an anonymous File Transfer Protocol (FTP) server, or a Hypertext Transfer Protocol (HTTP) server provided by an enterprise, as well as internal users accessing the Internet from inside the organisation.

This short dissertation does not address the validity as it relates to non-anonymous services (or "authenticated services"), where internal users are allowed to log onto the organisation's systems while situated externally, or elsewhere on the Internet.

This short dissertation assumes the organisation has in place an approved Internet Security Policies and Procedures Manual, which incorporates the firewall policy as a subset of the greater document. It is also assumed that

the organisation has established clear guidelines as to the Internet services they wish to allow their users access to.

The short dissertation addresses guidelines which the auditor must evaluate as a result of an existing firewall configuration, and does not attempt to prescribe how an Internet firewall should be configured. Neither does it address the risks relating to the development and implementation of an Internet firewall configuration.

A firewall technique is implemented as a combination of hardware and software, and involves administrative set-up (Cheswick and Bellovin, 1994:51-51), and therefore the resulting guideline includes aspects for review at both a hardware and software level as appropriate. The guidelines apply to firewall techniques in the generic sense, and will not be based on a particular proprietary firewall product supplied by a specific vendor.

Further, the research is limited to the two most commonly used firewall techniques, namely packet filtering and proxy services. Further, the dissertation is not based on any one particular firewall product, such as Gauntlet or Firewall-1, but rather the generic technique.

The above restrictions and exclusions can be used to provide the basis for further research in the future.

1.5 DEFINITIONS AND METHODOLOGY

As this short dissertation deals with **auditing validity** on the **Internet** with specific reference to **firewalls**, it is considered appropriate to define certain key terms in the title, namely auditing, validity, firewalls and the Internet.

"**Auditing** is a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users" (American Accounting Association Committee on Basic Auditing Concepts, 1972:Vol 47).

"The purpose of the **validity** check is to ensure that actions taken by the computer are valid actions. A valid action is one that conforms to a set of actions that are considered to be correct. The validity check compares each action with a set of valid actions to ensure that it is indeed valid" (Watne and Turney, 1990:242).

A comprehensive literature survey has not been carried out on the concept of validity as a control objective, as this has been proven through a number of research topics and publications. Instead, the research work published by Boshoff (1985,1990) and Damianides (1991, 9) will be assumed as correct.

The **Internet** was born about 25 years ago, as a U.S. Defence Department network called the ARPAnet (Krol, 1992:11). The story of its transition from birth as an experimental network to its current state is not within the scope of this research. However, an apt description is provided by Bernstein, et al. (1996:vii): "The **Internet**, often called the Information Superhighway by the media, connects computers all over the world to a degree not even anticipated by futurists".

A **firewall** is a mechanism used to protect a trusted network from an untrusted network. Typically, the two networks in question are an organisation's internal network (trusted) and the Internet (untrusted) (NCSA, 1996:3).

A **firewall** is an integral part of an organisation's security policy. It effectively manages the risks associated with networks by controlling and monitoring access between networks. Generally, firewalls filter inbound and outbound data, provide or manage public access to requested locations, deny all services except those explicitly permitted by the system administrator, log traffic and activity through the firewall, and activate alarms when prowlers are detected (Borderware, 1996:2).

A literature survey has been performed on existing authoritative textbooks and other literature available on the Internet and firewalls.

Based on the literature survey, all the relevant information was assimilated to complete this short dissertation.

1.6 RESEARCH APPROACH

The approach taken for this research essay has been to deal with the literature survey in chapters 2 through 4, with the development of guidelines in Chapter 5. More specifically:

1.6.1 The second chapter deals with the concept of validity. It also places into context, for the purposes of the short dissertation, how the validity control objective relates within the context of the Internet.

1.6.2 The third chapter deals with the technology, namely firewalls. The technology is understood, as it is the means by which the control objective is achieved.

1.6.3 Applying the Internet technology in practice results in risk, which is mitigated by controls which organisations must enforce. Chapter 4 deals with the risks which present themselves. The need for a sound Internet security policy is covered, as such a policy forms the basis of enforcing security by means of a firewall.

1.6.4 Chapter 5 presents the guidelines to achieve the overall objective of this short dissertation, namely to provide the ISA with guidelines to evaluate validity, with specific reference to firewalls. After considering the items listed, the ISA will be able to ensure that the risks relating to validity are reduced to an acceptable level.

1.7 SUMMARY OF RESULTS

The guidelines for auditing the validity of Internet traffic through a firewall, using firewall techniques, has been documented in chapter 5.

The primary objective of this research is to provide the ISA with assistance in auditing in an environment where the enterprise allows network traffic between the internal network and the external Internet, and firewall techniques have been utilised as a control mechanism. Using the guidelines provided, the auditor will be able to assess the adequacy of the controls implemented to ensure validity is achieved.

The guidelines examine the following areas:

1.7.1 Guidelines on examining the network topology are recommended in order to assist the ISA in obtaining an understanding of the existence and location of the important Internet components in relation to one

another; to understand the security philosophy deployed, and any weaknesses which may contribute to invalid activities.

1.7.2 In order to control the validity control objective while utilising the Internet, it is necessary to have stringent policies and procedures that define and control the conditions under which the enterprise should operate. To this end, guidelines are given in order that the enterprise network security policies are examined to determine the enterprise's policy with regard to Internet services, security requirements, privacy access, accountability, authentication, and monitoring violations.

1.7.3 A further area which the guidelines examine is the process used in dealing with the setting of packet filtering rules. Guidelines are developed to assist in the verification that the client process adheres to good practice.

1.7.4 A checklist of items is developed to determine the capability of the firewall to achieve the desired level of control.

1.7.5 Packet filtering rules are enforced to ensure validity and reflect the network security policy of the organisation (therefore fundamental in ensuring that all traffic is valid). Suggested guidelines are given for the auditor to verify that all these packet filtering rules are appropriate, and to ensure that only valid information is transmitted, and services offered.

1.7.6 The IT auditor must ensure that the activities of the firewall are logged. Guidelines of what the auditor must check are listed in this section.

1.8 CONCLUSION

The audit guidelines developed can be used by both external and internal ISA's faced with the task of auditing an environment where a firewall has been implemented to protect the internal network from the Internet. The objective of the research in this regard has therefore been met.

Further academic research may also be undertaken to address the issues relating to authenticated services, where internal users are allowed to log on to the organisations systems. Alternatively, an evaluation may be conducted on a specific firewall product.

CHAPTER 2

VALIDITY

CONTENTS PAGE

2.1 OBJECTIVE

The title of this short dissertation refers to auditing validity on the Internet with specific reference to firewalls.

2.1.1 Chapter 2

The objective of chapter 2 is to perform a limited literature survey on validity, in the context of the Internet. The objective is to expand on the control objective, but not to prove its accuracy, as this has already been achieved, as indicated in 2.3 below.

2.1.2 Chapter 3

The objective of chapter 3 is to perform a literature survey in order to understand the concept of a firewall and the typical methods of securing transmission to and from internal networks. Only once this has been established can the firewall technique be applied to the validity control objective. In order to derive the maximum benefit from the literature survey, the following objectives have been defined for this chapter:

2.1.2.1 To obtain authoritative definitions of Internet firewalls.

2.1.2.2 To detail what Internet firewalls do, what their capabilities are and what they cannot do.

2.1.2.3 Internet firewalls essentially contribute to validity through two major approaches to building firewalls, namely packet filtering

and proxy services. This section of the chapter will attempt to explain the technology, and the functionality with which these approaches strive to achieve the validity control attribute.

2.1.3 Chapter 4

The objective of chapter 4 is to understand the risks resulting from the use of the Internet. In order to derive the maximum benefit from the literature survey, the following objectives have been defined for this chapter:

2.1.3.1 The need for a sound Internet security policy will be researched, as such a policy forms the basis of enforcing security by means of a firewall.

2.1.3.2 To obtain authoritative facts relating to the risks.

2.1.3.3 To take a look at the types of incidents on the Internet which translate into risk.

2.1.3.4 To review the services that are available on the Internet, and the risks they bring to users of the services.

2.2 NATURE OF LITERATURE SURVEY

For the concept of validity, the literature surveyed is limited to explaining, defining and expanding on the already proven validity control objective, and related concepts in the context of the Internet.

A survey of literature was performed for aspects relating to the Internet and firewalls, from the authoritative references available.

2.3 SCOPE, LIMITATIONS AND EXCLUSIONS

Chapter 2 of the research essay focuses on the control objective pertaining to validity, and specifically excludes the control objectives relating to completeness, accuracy and maintenance.

The works of Boshoff (1985,1990) and Damianides (1991,9) will be assumed as correct in proving the validity control objective.

Specifically excluded from this short dissertation is the provision of so-called non-anonymous Internet services.

For non-anonymous services (or "authenticated" services, as they are commonly called), the user who is attempting to access the service initially needs to prove his identity to the server so that the server can decide whether the user is authorised to perform the request. Examples of authenticated services provided include:

* Allowing users to log on (via Telnet) from the Internet, e.g., while they're away at conferences or visiting other sites;

* Allowing researchers and collaborators from affiliated sites to log in to the systems; and
* Allowing selected customers or clients to logon to the enterprises systems (Chapman and Zwicky, 1995:35).

2.4 DEFINITIONS

User controls and **programmed procedures** are defined as all those controls and procedures designed to ensure that valid transactions, and only valid transactions, are processed, recorded and maintained completely and accurately in the accounting records (Jenkins, Perry and Cooke, 1996:173).

A **packet** is "a logical grouping of information that includes a header, control information, and a body that usually contains user data. Packets are used to transmit data across the Internet" (Bernstein, et al. 1996:434).

2.5 BACKGROUND

User and integrity controls are well documented by the institutes governing auditing standards, such as the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA) and the South African Institute of Chartered Accountants (SAICA).

The fundamental control and audit objectives and applicability of generally accepted auditing standards do not differ when financial information is processed in a computerised environment (SAICA, 1989:06).

2.6 VALIDITY

The components of the access path model are analysed in terms of the following objectives which are derived from Boshoff's (1985) original postulate and hypothesis on controls:

* **Completeness** of input and processing - all data is entered and processed;
* **Accuracy** of input and processing - data is correctly processed;
* **Validity** of input - only valid or authorised data is processed; and
* **Maintenance** - data is not altered after processing.

Proof of the validity of these controls is documented in Boshoff's research essays (1985,1990) and is assumed correct for the purpose of this short dissertation (Damianides, 1991, 9).

In many large installations, all transactions processed pass through a security "umbrella". This is provided by special security software which resides permanently in the system, sitting between the application programs and the operating system. When implementing this software, rights are

allocated to individual users and groups of users which specifically allow defined users to read, write, alter or delete items on the file as appropriate. The tables of users, rights and data elements are held in the system as the "security profiles" (Jenkins, et al. 1996:200).

Users are allocated individual passwords. When a user logs on to a system through a terminal, he is asked for his individual password. The system compares the password with the security profiles to see if the attempted access is valid, i.e. if the user is permitted to carry out the action proposed. Thus authorisation of individual transactions is no longer carried out, the validity of transactions relying not on authorisation but on pre-defined rules.

For such systems to be effective the following steps must be taken:

* The appropriate options must be selected in the security software. In practice this is complicated and it is an area where companies will often seek advice from the computer audit specialist;
* The security profiles must be carefully established so that the maximum independence of duties is maintained;
* Responsibility for ownership of data must be defined to appropriate persons;
* Security profiles must be kept secure and confidential;

* Passwords must be sensible, kept secret and be changed at regular intervals; and
* Attempted violations should be recorded and investigated (Jenkins, et al. 1996:200).

2.7 CONCLUSION

Control of access (validity) to an information asset is essentially done by describing what objects can access it and how they can access it (authorisation); and then by requiring that the accessing object identify and authenticate itself so that the privileged object is validated. Access control may also be considered as the means for enforcing authorisation.

Clearly, in the anonymous services category authentication of the packet is not important, as the identity of the requester is not important, as it is assumed that all the information is freely available, and the dilemma is to prevent access to the network and services not freely available.

As a result of the above literature survey, it can be concluded that the enterprise needs to ensure that rules are defined to ensure that only valid or authorised Internet traffic is allowed to access valid or authorised resources.

In the context of the Internet, this means that there must be programmed procedures and user controls applied to the Internet traffic passing between

the enterprise's internal and external Internet, so as to ensure valid packets, and only valid packets, are processed.

Furthermore, for anonymous services, such as accessing an anonymous FTP server, HTTP server, or Gopher server that is provided, the solution is clear: the enterprise protects the servers as well as it can to allow outsiders to access the information provided and prevent users from accessing anything else. In these anonymous services, all the information released is intended to be readable by anybody.

The firewall software must contains rules that restrict the users' ability to process transactions and ensure the validity of the traffic.

CHAPTER 3

INTERNET TECHNOLOGY

CONTENTS PAGE

3.1 INTRODUCTION

The auditor must ensure that only valid packets of information are allowed between the enterprise's internal network, and the external Internet. This chapter covers the technology which may be implemented to ensure the validity of the traffic passing between the networks. It is most often the role of the firewall to accomplish this, and it is traditionally placed between the organisation's network and the outside world (Cheswick, et al. 1994:53).

3.2 DEFINING AN INTERNET FIREWALL

In defining a firewall, an analogy can be made between the firewall built during the construction of a building and the computer version of this device (Siyan, 1995:81). The purpose of a building's firewall is typically to keep a fire from spreading from one part of the building to another. In theory, an Internet firewall serves a similar purpose: it prevents the dangers of the Internet from spreading to the internal network. In practice, an Internet firewall is more like a moat of a medieval castle than a firewall in a modern building. It serves multiple purposes:

* It restricts people to entering at a carefully controlled point;
* It prevents attackers from getting close to your other defences; and
* It restricts people to leaving at a carefully controlled point (Chapman, et al. 1995:17).

Logically, a firewall is a separator, a restricter, or an analyser. Typically, a firewall is a set of hardware components, including a router, a host computer, or some combination of routers, computers, and networks together with appropriate software. There are various ways to configure this equipment and this will depend upon a site's particular security policy, budget, and overall operations (Chapman, et al. 1995:17).

A firewall is a system or group of systems that enforces an access control policy between two networks. More specifically, a firewall is a collection of components or a system that is placed between two networks and possesses the following properties:

* all traffic from inside to outside, and vice versa, must pass through it; and
* only authorised traffic, as defined by the local security policy, is allowed to pass through it; and the system itself is immune to penetration (NCSA, 1996:3).

The major objective of a firewall is to protect one network from another. Usually, the network being protected belongs to you (or is your responsibility), and the network that you are seeking to protect yourself from is an external network that cannot be trusted and from which security attacks can originate. In general, a firewall is placed between the internal trusted

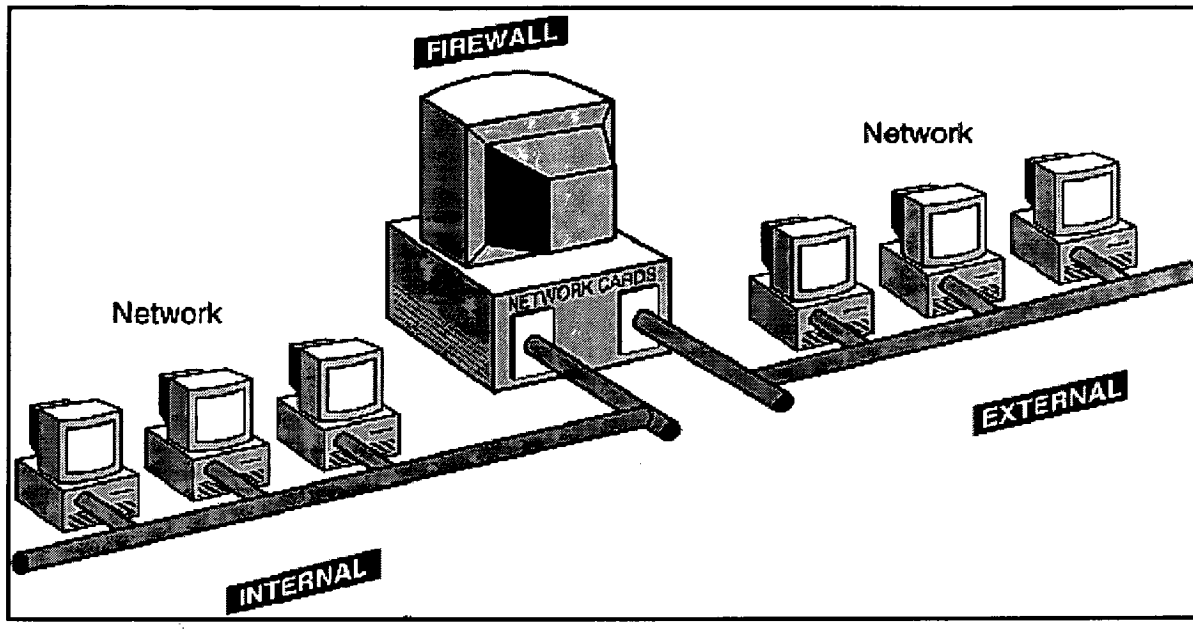
network and the external untrusted network. The firewall acts as a choke-point that can be used for monitoring and rejecting application-level network traffic. The firewall is the chief instrument used to implement an organisation's network security policy (Siyan, 1995:82).

Firewalls are barriers that exist between an organisation's internal network and any external network. The main objective of a firewall is to protect an internal network from unauthorised access by users on the external network. The external network can be the Internet, or may be another network belonging to the same organisation (Borderware, 1996:1).

3.3 TYPICAL FIREWALL COMPONENTS

The simple concept of a firewall is illustrated in figure 3.1. Simply illustrated, one sees the components of the internal network, typically belonging to the enterprise, the firewall, which may consist of numerous components, the external (Internet) network, from which protection is usually sought. A dual-homed host is a general purpose computer system that has at least two network interfaces as can be seen in Figure 3.1 (Chapman, et al.1995:58).

Figure 3.1: Dual-Homed Firewall (Borderware, 1996:5)



In reality, a firewall usually consists of many different components, and most robust firewall solutions make use of a combination of firewall techniques (Bernstein, et al. 1996:174).

Because of the location of the firewall between the two networks, it has the opportunity of ensuring that this traffic is acceptable. This means that whatever is being done, whether it be e-mail, file transfers, remote logins, or any kinds of specific interactions between specific systems, it has the ability to ensure that it conforms to the security policy of the site (Chapman, et al.1995:17).

3.4 CAPABILITIES OF FIREWALLS

3.4.1 A firewall is a focus for security decisions

A firewall is a choke-point. All traffic in and out must pass through this single, narrow checkpoint. A firewall allows an enterprise the ability to concentrate its security measures on this checkpoint: the point where the internal proprietary network connects to the Internet. By doing this, the enterprise effectively implements access control based on the connection's packets (Bernstein, et al. 1996:172).

3.4.2 A firewall can enforce security policy

Many of the services that people want from the Internet are inherently insecure. The firewall is the traffic cop for these services. It enforces the site's security policy, allowing only "approved" services to pass through and those only within the rules set up for them. For example, one site's management may decide that certain services such as Sun's Network File System (NFS) and Network Information Services are simply too risky to be used across the firewall. Still another site might decide to allow access from all systems of a certain type, or belonging to a certain group (Chapman, et al.1995:20).

3.4.3 A firewall can log Internet activity efficiently

Because all traffic passes through the firewall, the firewall provides a good place to collect information about system and network use and misuse. As a

single point of access, the firewall can record what occurs between the protected network and the external network (Chapman, et al.1995:20).

3.4.4 A firewall limits exposure

Sometimes a firewall will be used to keep one section of a site's network separate from another section. Firewalls have the ability to hide certain machines from others (Bernstein, et al. 1996:172).

3.4.5 Firewalls provide a single point of security administration

Instead of placing network security restrictions on thousands of individual hosts, a firewall configured in this manner will allow the security administrator to concentrate efforts on one area only (Siyan, 1995:82).

3.5 LIMITATIONS OF FIREWALLS

A firewall cannot do the following:

3.5.1 Protect the organisation against malicious insiders. This has lead to organisations implementing internal firewalls between subnetworks.

3.5.2 Protect the organisation against connections that don't go through it.

3.5.3 Protect against completely new threats.

3.5.4 Protect against viruses due to performance degradation.

3.5.5 Firewalls provide no authenticity of the source of the data. A firewall only gets to look at a "snapshot" of a packet. A resulting security risk is that one user can purport to be another.

3.5.6 Generally speaking, firewalls do not provide confidentiality. Although some firewalls provide encryption, to be effective, all communication parties would have to have the same firewall installation (Berstein, et al. 1996:173-174, Chapman, et al.1995:20, Siyan, 1995:173).

3.6 FIREWALL TECHNIQUES

Firewalls use two methods of securing transmission to and from internal networks, namely packet filtering and proxy services, and there are many variations of each of the two methods (Bernstein, et al. 1996:174, Realaudio, 1997:1).

The two methods will be investigated in order for the ISA to gain an understanding of how the organisation allows valid and blocks invalid connections from external hosts.

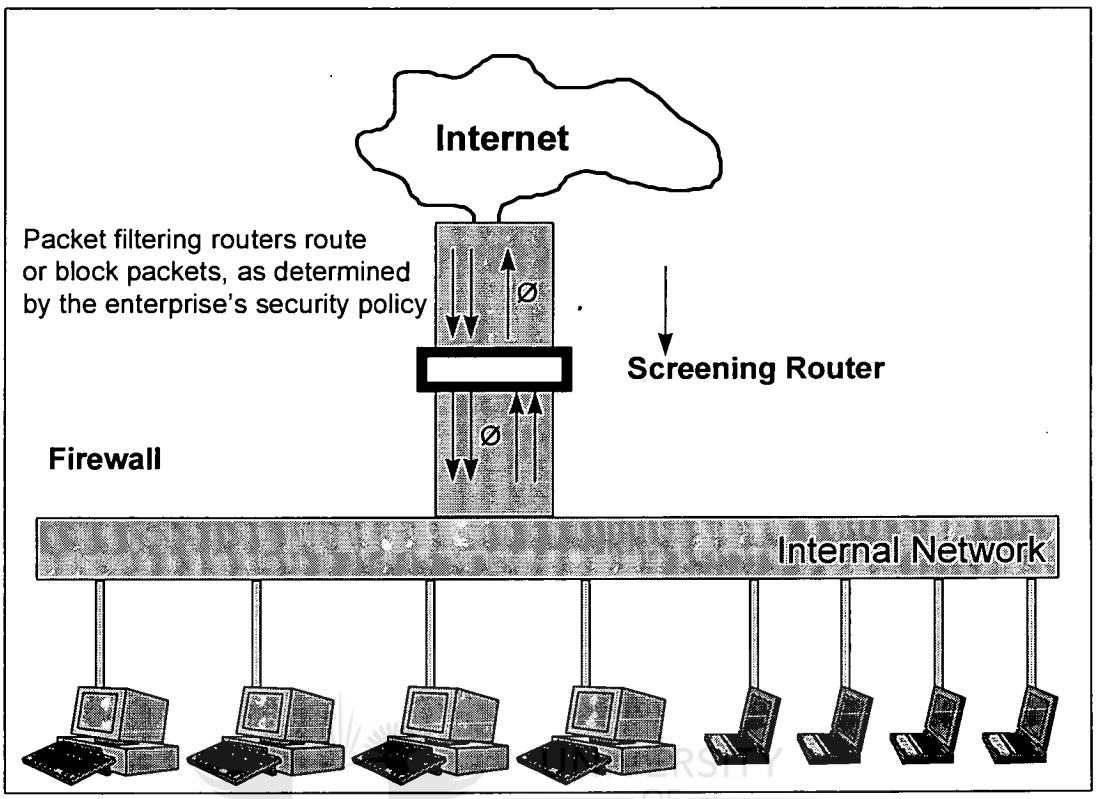
3.6.1 Packet filtering

Packet filtering systems route packets between internal and external hosts selectively (Siyan, 1995:87).

This principle is illustrated using Figure 3.2 and Figure 3.3. The basic operations are:

* Packet filter rules or criteria are stored for the packet filter device or screening router;
* Packet headers are parsed when they arrive at a port, and the fields in the Internet protocol (IP), Transmission control protocol (TCP), or User datagram protocol (UDP) headers are typically examined;
* Each packet filter rule is applied to the packet in the order in which the packet filter rule is stored;
* If a rule blocks the transmission or reception of a packet, the packet is not allowed;
* If the rule allows the transmission or reception of a packet, the packet is allowed to proceed; and
* If a packet does not satisfy a rule, it is blocked (Siyan, 1995:87).

Figure 3.2 Using a screening router to do packet filtering (Chapman, et al.1995:59, *adapted*).



A port is an interface on an internetworking device (such as a firewall), and in TCP/IP it refers to the number used to specify the receiving process in communication (Bernstein, et al. 1996:435). Both TCP and UDP make use of "ports" to identify the ultimate destination on a machine. Generally, each connection will be assigned (or bound to) a port on the machine. Most well known TCP/IP services, including Telnet, File transfer protocol (FTP), Simple mail transfer protocol (SMTP), Domain name server (DNS), and the Web, use ports for every system (Bernstein, et al. 1996:176).

Typical ports are illustrated in Table 3.1.

Table 3.1 Some Well-Known TCP Port Numbers (Siyan, 1995:91-92).

Description	Port Number
Remote Job Entry	5
ftp_data	20
ftp (Control)	21
telnet	23
smtp	25
time	37
Gopher	70
Finger	79
WWW HTTP	80
Kerberos	88
rlogin	513

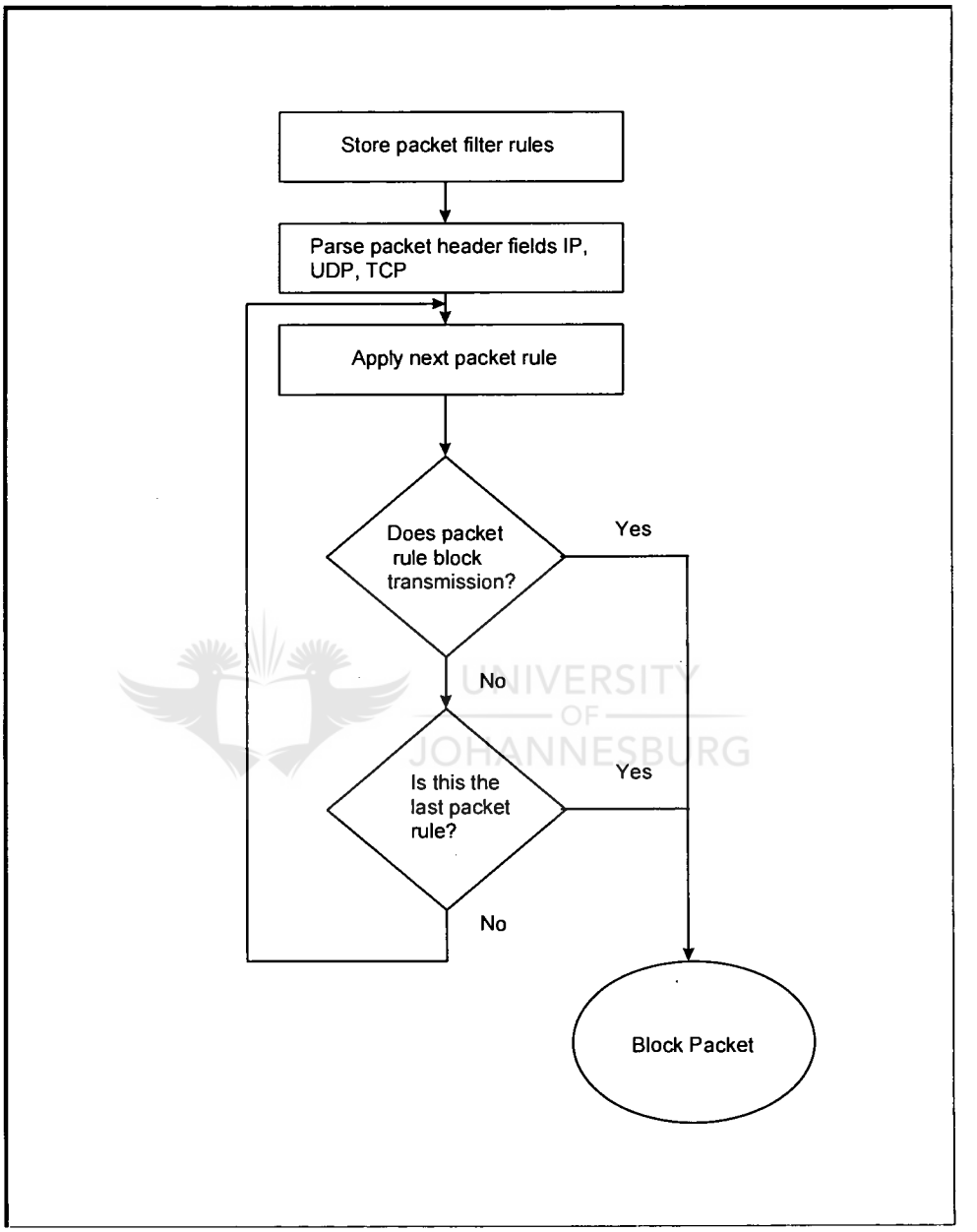
Most versions of TCP and UDP enforce a rule that only the superuser (root) is able to create a port with a number less than 1024. Thus ports 0 -1023 are considered privileged ports. The intention is that remote systems are able to trust the authenticity of information written to such ports. This is important when considering the packet filtering rules, and will be evident in Table 3.5 and Table 3.6 (Cheswick and Bellovin, 1994:24).

Parameters on which a packet filter can base decisions will vary depending on the firewall product, but usually include:

* traffic direction (in from the port, out to the port);
* port on which the traffic was received or to which it is destined;
* protocol type (e.g., IP, TCP, UDP);
* source and destination IP address;
* source and destination TCP or UDP port; and
* TCP "state" information (Bernstein, et al. 1996:177).

The rules are alternatively expressed in Figure 3.3. Here the process logic runs from top to bottom, where each header field is evaluated against the packet filter rule, and either denies or allows the packet.

Figure 3.3 Flow chart of packet filter operation (Siyan, 1995:89, *adapted*).



3.6.1.1 Validating by address

The simplest, although not the most common, form of packet filtering is filtering by address. Filtering in this way lets you restrict the flow of packets based on source and/or destination addresses of the packets, without having to consider what protocols are involved. Such filtering can be used to allow certain external hosts to talk to certain internal hosts, for example, or to prevent an attacker from injecting forged packets (packets handcrafted so they appear to come from somewhere other than their true source) into your network (Chapman, et al.1995:161).

This may be illustrated by an example. If the entity wishes to allow all IP traffic between a trusted external host (host 172.16.51.50) and host on the internal network (host 192.168.10.0), the rule may be set up as illustrated in Table 3.2.

Table 3.2 Telnet Summary (Chapman, et al.1995:167, *adapted*).

Rule	Direction	Source Address	Destination Address	ACK Set	Action
A	Inbound	Trusted external host 172.16.51.50	Internal	Any	Permit
B	Outbound	Internal	Trusted external host 172.16.51.50	Any	Permit
C	Either	Any	Any	Any	Deny

3.6.1.2 Validating by service

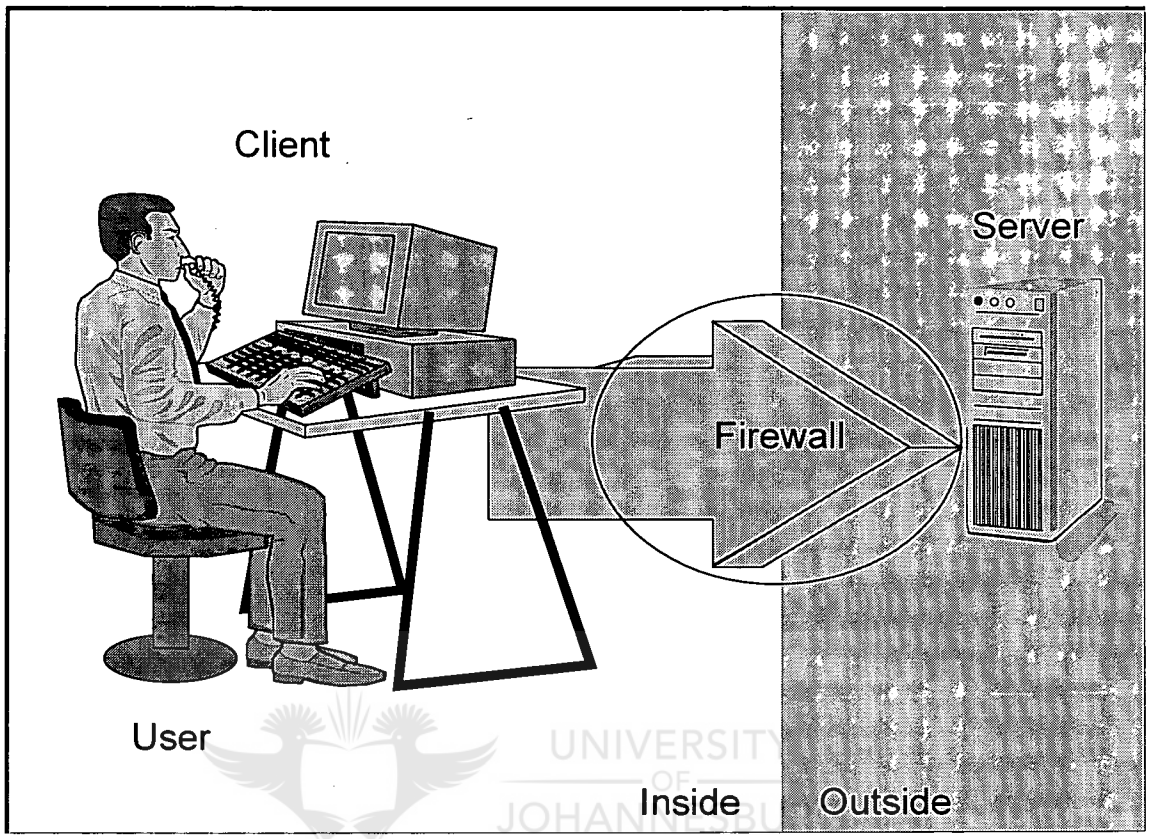
Blocking incoming forged packets, as discussed previously, is virtually the only common use of filtering solely by address. Most other uses of packet filtering involve filtering by service, which is somewhat more complicated.

The next example includes a detailed look at Telnet. Telnet allows a user to log in to another system, as if the user had a terminal directly connected to that system. Telnet is used as an example because it is fairly common, fairly simple, and from a packet filtering point of view representative of several other protocols such as (SMTP) and Network news transfer protocol (NNTP). The focus will be on the outbound Telnet service (Chapman, et al.1995:164).

3.6.1.3 Outbound Telnet service

A local client (a user) is talking to a remote server. One needs to handle both outgoing and incoming packets. Figure 3.4 illustrates the Telnet service.

Figure 3.4 Outbound Telnet (Chapman, et al.1995:164, *adapted*).



The outgoing packets for this outbound service contain the user's keystrokes and have the following characteristics:

* The IP source address of the outgoing packets is the local host's IP address;
* The IP destination address is the remote host's IP address;
* Telnet is a TCP-based service, so the IP packet type is TCP;

* The TCP destination port is 23; that is the well-known port number Telnet servers use;
* The TCP source port number (which is called "Y" in this example) is some seemingly random number greater that 1023. (BSD UNIX reserves ports from 0 to 1023 for local use only by root. These ports are normally used only by servers, not clients); and
* The first outgoing packet, establishing the connection, will not have the ACK bit set; the rest of the outgoing packets will.

The incoming packets for this outbound service contain the data to be displayed on the user's screen (for example, the "login:" prompt) and have the following characteristics:

* The IP source address of the incoming packets is the remote host's IP address;
* The IP destination address is the local host's IP address;
* The IP packet type is TCP;
* The TCP source port is 23; that's the port the server uses;
* The TCP destination port is the same "Y" used as the source port for the outgoing packets; and
* All incoming packets will have the ACK bit set (again, only the first packet, establishing a connection, does not have the ACK bit set; in this example

that first packet was an outgoing packet, not an incoming packet) (Chapman, et al.1995:162-163).

3.6.1.4 Inbound Telnet Service

The inbound Telnet service will not be illustrated. There are similarities between the headers of the incoming and the outgoing packets; the source and destination addresses and ports are exchanged (Chapman, et al.1995:166).

3.6.1.5 Telnet summary

Table 3.3 illustrates the various types of packets involved in inbound and outbound Telnet services.

Table 3.3 Telnet Summary (Chapman, et al. 1995:166).

Service Direction	Packet Direction	Source Address	Dest. Address	Packet Type	Sourc Port	Dest. Port	ACK Set
Outbound	Outgoing	Internal	External	TCP	Y	23	*
Outbound	Incoming	External	Internal	TCP	23	Y	Yes
Inbound	Incoming	External	Internal	TCP	Y	23	*
Inbound	Outgoing	Internal	External	TCP	23	Y	Yes

* The TCP ACK bit will be set on all but the first of these packets, which establishes the connection. Note that Y is both random (from the packet filtering system's point of view) port numbers above 1023.

To allow outgoing Telnet, but nothing else, the rules would be set up as illustrated in table 3.4.

Table 3.4 Telnet Summary (Chapman, et al.1995:167).

Rule	Direc-tion	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	ACK Set	Action
A	Out	Internal	Any	TCP	>1023	23	Either	Permit
B	In	Any	Internal	TCP	23	>1023	Yes	Permit
C	Either	Any	Any	Any	Any	Any	Either	Deny

3.6.2 Proxy services

Proxy services are specialised application or server programs that run on a firewall host. Instead of taking a transparent approach that packet filters take, proxy servers adopt a "store-and-forward" approach. They do this by terminating the inbound connection from the source, and initiating a second connection to the destination. Because of the need to have multiple network interfaces, they are often referred to as dual-homed hosts. These programs take users' requests for Internet services (such as FTP and Telnet) and forward them, as appropriate according to the site's security policy, to the actual services (Bernstein, et al. 1996:177, Chapman, et al.1995:61).

Figure 3.5 Application-level proxy services (Realaudio, 1997:2, *adapted*)

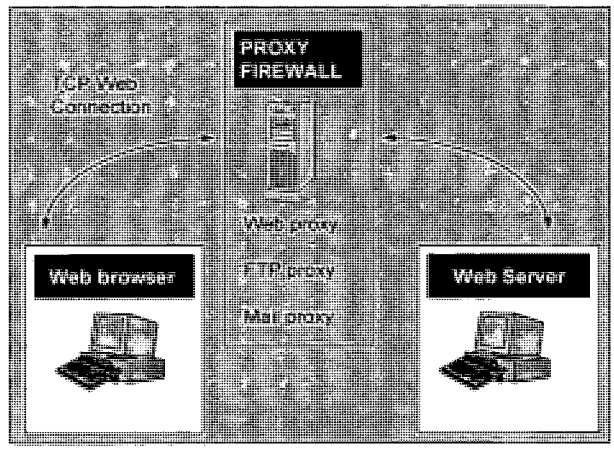
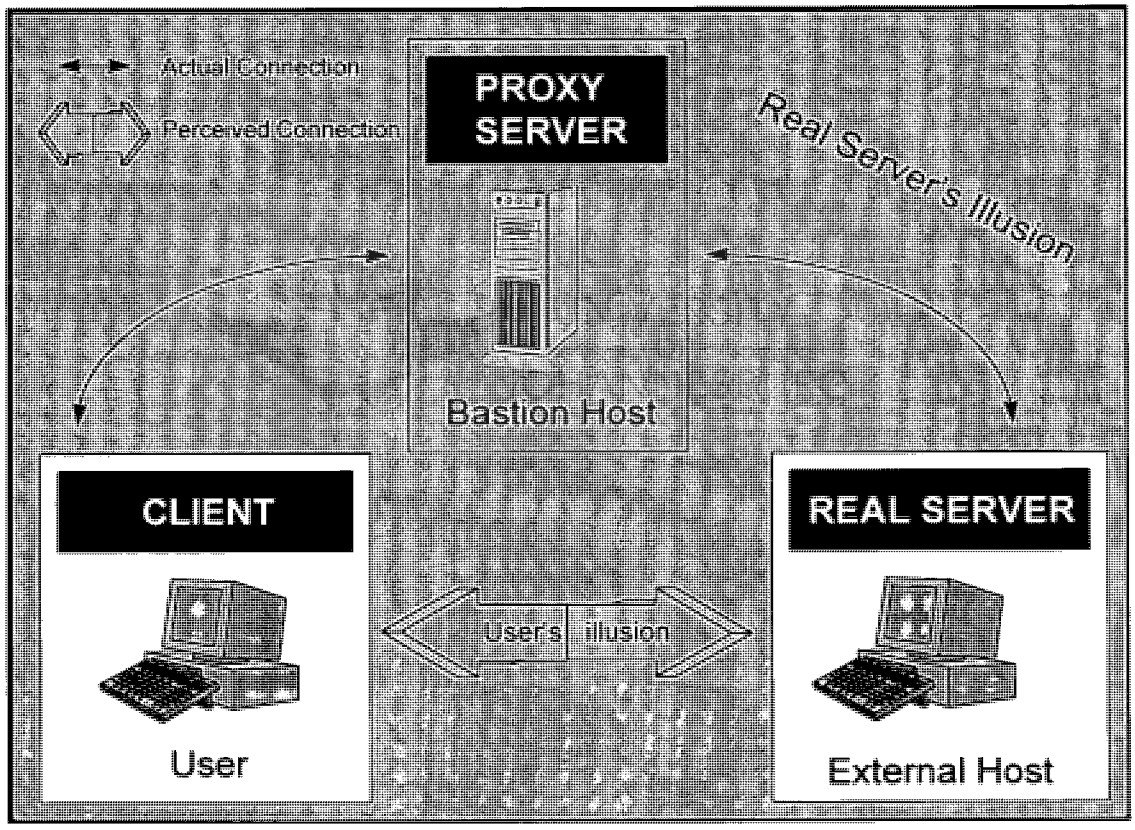


Figure 3.5 illustrates an implementation of a proxy server, which provides application support for Web, FTP and mail services (SMTP). A proxy server for a particular protocol or set of protocols runs on a dual-homed host or a bastion host: some host that the user can talk to, and which can, in turn, talk to the outside world. The user's client program talks to this proxy server instead of directly to the "real" server out on the Internet. The proxy server evaluates requests from the client and decides which to pass on and which to disregard. If a request is approved, the proxy server talks to the real server on behalf of the client (thus the term "proxy"), and proceeds to relay requests from the client to the real server, and to relay the real server's answers back to the client (Chapman, et al.1995:189).

Figure 3.6 illustrates the illusion that is created for the user. As far as the user is concerned, talking to the proxy server is just like talking directly to the real server. As far as the real server is concerned, it's talking to a user on the host that is running the proxy server; it does not know that the user is

really somewhere else. The security advantage is that proxy servers "hide" the internal host from the destination server. This is an advantage for organisations who do not wish their internal networks to be visible to the outside world. Proxying doesn't require any special hardware, although it does require special software for most services. This principle is illustrated in the Figure 3.6 (Bernstein, et al., 1996:190).

Figure 3.6 Proxies-reality and illusion (Chapman, et al. 1995:191,*adapted*)



3.6.2.1 Benefits of proxy servers

The use of proxy servers has a number of benefits. They contribute to validity in a number of ways, ensuring that when connection is made,

unauthorised access to other parts of the network and services is disallowed. Typical benefits include:

* Users are not given access to the operating system;
* They do not require users to make multiple connections across different machines;
* The internal network is hidden from the destination server;
* Application specific restrictions can be made: for example, using FTP, the ability to restrict file uploads while allowing file downloads, or the ability to restrict submission of information via the WEB forms while allowing unlimited retrieval of information via the WEB;
* They have the capability to log and control all incoming and outgoing traffic. Because all data between the client and server is intercepted by the application proxy, it has full control over the session, and can perform detailed logging; and
* A disadvantage of application gateways is that a custom program has to be written for each application. This is an advantage as well from a security viewpoint because a user cannot go through the firewall unless an explicit application gateway has been provided (Bernstein, et al. 1996:189, Siyan, 1995:103).

3.7 LOGGING FIREWALL ACTIVITY

If logging routines are attached to ports, there is some assurance that invalid connections will be detected (Cheswick, et al. 1994:133).

An example of such a log may look as follows (line numbers have been added):

1: May 29 00:00:58 localhost wn[27194] : noc.nca.or.bv - - [] "GET/long/consulting.html HTTP/1.0"200 1074 <Sent file: >

2: May 29 00:02:38 localhost ftpd[26086] : : 05/29/95 0:02:38 spoke.cst.cnes.vg(gupta@) retrieved

3: May 27 01:13:38 mv-gw.longitude.com user: host naismith.longitude.com admin login failed

4: May 27 01:13:47 mv-gw.longitude.com last message repeated 2 times

5: May 27 01:15:17 mv-ge.longitude.com user: host naismith.longitude.com admin login succeeded

6: May 27 01:19:18 mv-gw.longitude.com 16 permit: TCP from 192.168.20.35.2591 to 172.16.1.3.53 seq 324EE800, ,ack 0x0, win 4096, SYN.

7: May 29 16:26:46 mv-gw.longitude.com 8 deny: UDP from 192.168.186.11.20 to 192.168.20.34.1937 (Chapman, et al.1995:401).

A number of facts can be gleaned from such reporting, and the ISA must ensure that the client follows similar principles, or investigates the following situations, in an attempt to determine whether invalid activities are being attempted:

* Log entries must be viewed in context. E.g., "login succeeded for user hacker" is acceptable, unless it's proceded by three "login failed" messages for every user above "hacker" in the password file; and
* The message on line 6, shows an unexceptional outbound TCP connection, logged under normal principles. This message would not be a problem, but for the messages on lines 3 to 5. Interpreting the scenario, one can discern that someone made three invalid tries at logging in as "admin", finally succeeded, and then immediately started up an outbound connection (Chapman, et al. 1995 : 400-401).

Such activity may well represent a security breach, and as such, should be followed up.

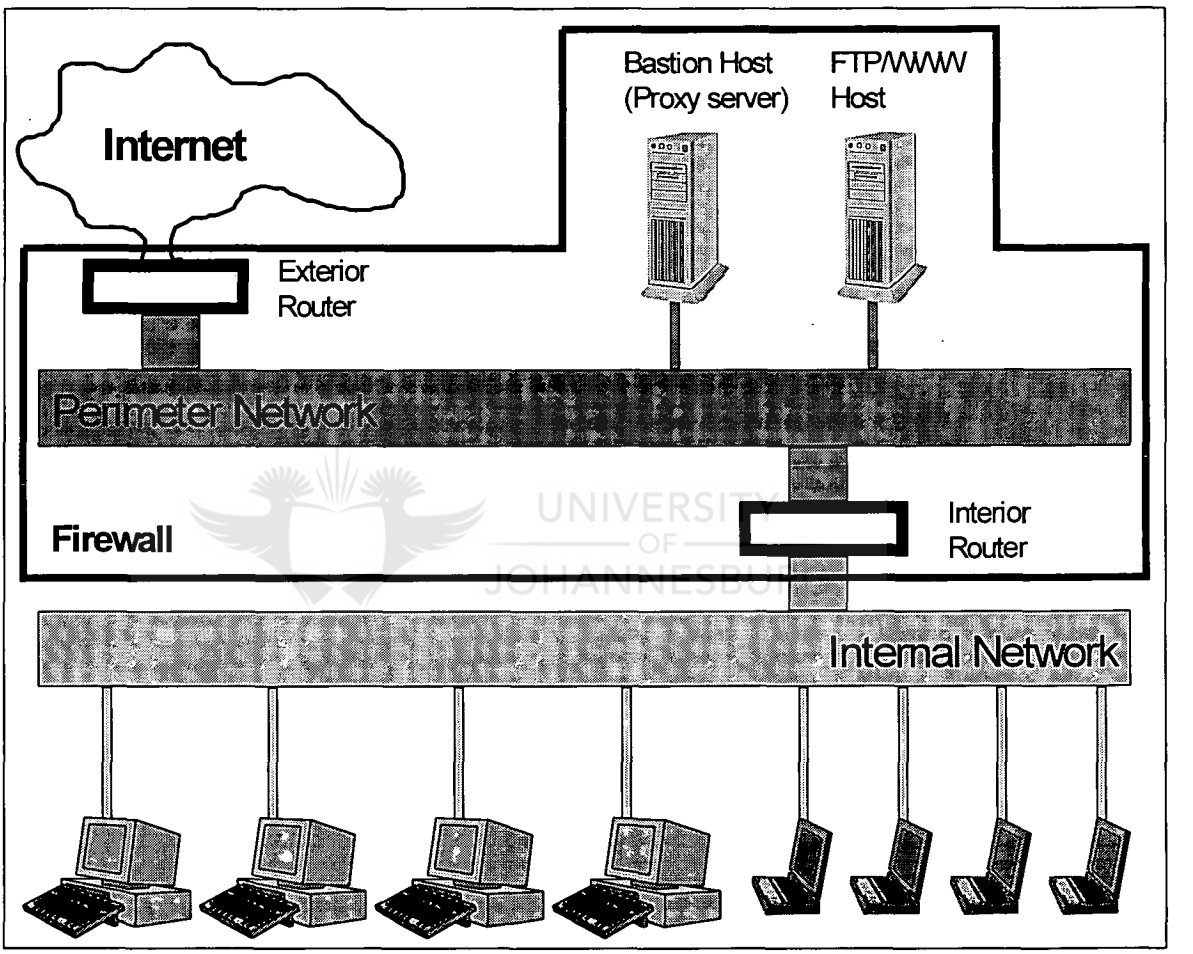
3.8 A TYPICAL FIREWALL CONFIGURATION

It is important to illustrate possible firewall components and their functions in one diagram that will illustrate their interaction with each other. This will serve to integrate all the concepts and issues within one diagram. The ISA,

tasked with auditing validity, will be able to refer to this architecture as a point of reference and departure, from which other architectures and configurations can be understood. With that in mind, one of the most commonly used firewall architectures has been chosen to explain the concepts.

The firewall architecture is commonly referred to as the screened subnet architecture, and is illustrated in figure 3.7.

Figure 3.7 Screened subnet architecture (using two routers) (Chapman, et al.1995:68,*adapted*).



3.8.1 Explanation of a screened subnet architecture

In summary, in the simplest configuration of a screened subnet architecture, there are two screening routers, each connected to the perimeter network. The exterior router is placed between the external (Internet) and the perimeter network, and the interior router is placed between the internal (protected) network and the perimeter network. In between these one has the bastion host (usually acting as a proxy server, of which there can be more than one machine). The layered security eliminates a single point of failure (Berstein, et al. 1996:196-202, Cheswick and Bellovin, 1994:74-80, Chapman, et al. 1995:66-77).

The components of this type of firewall configuration and their functions are:

* **Perimeter network**. This is a further layer of security, an additional network between the external Internet and the protected internal network. Isolating the bastion host on a perimeter network can reduce the impact of a break-in on the bastion host. Should a hacker break into the bastion host, because no corporate internal traffic passes over the perimeter network, the internal traffic will be safe from the eyes of intruders. In typical networks which do not have such a perimeter network, snoopers may succeed in picking up passwords by watching for those used during

Telnet, FTP, and rlogin sessions. In addition, the contents of sensitive files and e-mail may be compromised. By isolating the bastion host on the perimeter network, because it is the most vulnerable machine on the network, an enterprise can reduce the impact of a break-in (Berstein, et al. 1996:196-202, Cheswick and Bellovin, 1994:74-80, Chapman, et al. 1995:66-77);

* **Exterior router**. It is the first point of entry from the outside world to the corporate network, and will provide protection to the bastion host, interior router, and finally the internal network. This access router may be located and administered by an external service provider, which raises issues such as the level of trust, willingness to implement the enterprise's needs, and the process over changes to packet-filtering rule sets. An important task of the exterior router is the blocking of incoming packets from the Internet that have forged source addresses, and that claim to have come from the internal network (Berstein, et al. 1996:196-202, Cheswick and Bellovin, 1994:74-80, Chapman, et al. 1995:66-77);
* **Bastion Hosts**. This may consist of more than one machine, and is the main point of contact for incoming connections from the outside world. A bastion host is any firewall host critical to the network security. It typically provides the first line of defence (Siyan, 1995, 101). The bastion host will act as a proxy server, either by running specialised proxy server software for particular protocols (such as HTTP or FTP), or by running standard servers for self-proxying protocols (such as SMTP). It is easier to

implement "stripped down" hosts in this manner, that is, each host on the subnet can be configured to run only those services it is required to serve, thus providing an intruder with fewer potential targets. This has security, performance and redundancy advantages (Berstein, et al. 1996:196-202, Cheswick and Bellovin, 1994:74-80, Chapman, et al. 1995:66-77); and

* **Interior router**. The interior router or choke router serves to protect the internal network from the machines on the external and perimeter network. It provides packet filtering for selected services outbound from the internal network. These services must be in terms of what is considered valid and may include outbound Telnet, FTP and others. The services allowed between the bastion host and the internal network are likely to be different, and the enterprise will wish to limit the number of services made possible should the bastion host be compromised: e.g., should there be an anonymous FTP server on the perimeter network, the internal router should not allow any FTP requests to the internal network, however, it should allow internal requests to the greater Internet. One of the best security features of a router is its ability to filter on the origin and destination address (Ernst and Young, 1994:8).

3.8.2 Examples of filtering rules for routers

Typical sample printouts of the filtering rules for both an interior and exterior routers are given in Table 3.5 and Table 3.6, together with explanations, to illustrate how these may be set up.

Table 3.5 Interior router (Chapman, et al.1995:329-333).

Rule	Direc -tion	Source Address	Destination Address	Protocol	Source Port	Dest Port	ACK Set	Action
Spoof	In	Internal	Any	Any	Any	Any	Any	Deny
Telnet-1	Out	Internal	Any	TCP	>1023	23	Any	Permit
Telnet-2	In	Any	Internal	TCP	23	>1023	Yes	Permit
FTP-1	Out	Internal	Any	TCP	>1023	21	Any	Permit
FTP-2	In	Any	Internal	TCP	21	>1023	Yes	Permit
FTP-3	Out	Internal	Any	TCP	>1023	>1023	Any	Permit
FTP-4	In	Any	Internal	TCP	>1023	>1023	Yes	Permit
FTP-5	Out	Internal	Bastion	TCP	>1023	21	Any	Permit
FTP-6	In	Bastion	Internal	TCP	21	>1023	Yes	Permit
FTP-7	In	Bastion	Internal	TCP	Any	6000-6003	Any	Deny
FTP-8	In	Bastion	Internal	TCP	>1023	>1023	Any	Permit
FTP-9	Out	Internal	Bastion	TCP	>1023	>1023	Yes	Permit
SMTP-1	Out	Internal	Bastion	TCP	>1023	25	Any	Permit
SMTP-2	In	Bastion	Internal	TCP	25	>1023	Yes	Permit
SMTP-3	In	Bastion	Internal NNTP Server	TCP	>1023	25	Any	Permit
SMTP-4	Out	Internal	Bastion	TCP	25	>1023	Yes	Permit
NNTP-1	Out	Internal NNTP Server	NNTP Feed Server	TCP	>1023	119	Any	Permit
NNTP-2	In	NNTP Feed Server	Internal NNTP Server	TCP	119	>1023	Yes	Permit
NNTP-3	In	NNTP Feed Server	Internal NNTP Server	TCP	>1023	119	Any	Permit
NNTP-4	Out	Internal NNTP Server	NNTP Feed Server	TCP	119	>1023	Yes	Permit
HTTP-1	Out	Internal	Bastion	TCP	>1023	80	Any	Permit
HTTP-2	In	Bastion	Internal	TCP	80	>1023	Yes	Permit
DNS-1	Out	Internal DNS Server	Bastion	UDP	53	53	a	Permit
DNS-2	In	Bastion	Internal DNS Server	UDP	53	53	a	Permit
DNS-3	Out	Internal DNS Server	Bastion	TCP	>1023	53	Any	Permit
DNS-4	In	Bastion	Internal DNS Server	TCP	53	>1023	Yes	Permit
DNS-5	In	Bastion	Internal DNS Server	TCP	>1023	53	Any	Permit
DNS-6	Out	Internal DNS Server	Bastion	TCP	53	>1023	Yes	Permit
Default-1	Out	Any	Any	Any	Any	Any	Any	Deny
Default-2	In	Any	Any	Any	Any	Any	Any	Deny

Explanation of the packet filtering rules in Table 3.5

As can be seen in the table, the UDP protocol does not have the ACK bit, unlike the TCP protocol. This ACK bit is important, as it is not set for the first packet, thus allowing the packet filter to distinguish which packet is the first, and thereby enabling filtering on all TCP packets.

* **Spoof**

  Blocks incoming packets that claim to have internal IP addresses.

* **Telnet-1 and Telnet-2**

  Allow outgoing Telnet connections;

* **FTP-1 and FTP-2**

  Allow outgoing connections to FTP servers, for use by passive-mode internal clients that are interacting with those servers directly;

* **FTP-3 and FTP-4**

  Allow the FTP data channel connections from passive-mode internal clients to external FTP servers. These rules actually allow all connections from internal TCP ports above 1023 to external TCP ports above 1023;

* **FTP-5 and FTP-6**

  Allow normal (nonpassive-mode) internal FTP clients to open an FTP command channel to the proxy FTP server on the bastion host. Note that these rules are actually redundant if you have rules FTP-1 and FTp-2 in place earlier in the list, because "Bastion" as a source or destination (covered by rules FTP-5 and FTP-6) is a subset of "All" (covered by rules FTP-1 and FTP-2). Having these redundant rules is going to impose a

slight performance cost, but makes the rule set easier to understand. It also makes it possible to change rules FTP-1 and FTP-2 (e.g., if you decide you don't want to support passive mode clients) without accidentally breaking normal-mode client access to the proxy server;

* **FTP-6 through FTP-9**

  Allow FTP data connections from the proxy server on the bastion host to non-passive internal clients. The FTP-7 rule prevents an attacker who has gained access to the bastion host from attacking internal X11 server via the hole generated by rules FTP-8 and FTP-9. If you have other servers internally listening for connections on TCP ports above 1023, you should add similar rules for them. Note that trying to list things that should be denied (as in rule FTP-7) is generally a losing proposition, because your list will almost always be incomplete somehow;

* **SMTP-1 and SMTP-2**

  Allow outgoing mail from internal hosts to the bastion host;

* **SMTP-3 and SMTP-4**

  Allow incoming mail from the bastion host to your internal mail server;

* **NNTP-1 and NNTP-2**

  Allow outgoing Usenet news from your news server to your service provider's news server;

* **NNTP-3 and NNTP-4**

  Allow incoming Usenet news from your service provider's news server to your news server;

* **HTTP-1 and HTTP-2**

  Allows internal HTTP clients to connect to the HTTP proxy server on your bastion host;

* **DNS-1**

  Allows UDP-based DNS queries and answers from the internal DNS server to the bastion host DNS server;

* **DNS-2**

  Allows UDP-based DNS queries and answers from the bastion host DNS server to the internal DNS server;

* **DNS-3 and DNS-4**

  Allow TCP-based DNS queries from the bastion host DNS server to the internal DNS server, as well as answers to those queries. Also allow zone transfers in which the bastion host DNS server is the secondary server and internal DNS server is the primary server;

* **DNS-5 and DNS-6**

  Allow TCP-based DNS queries from the internal DNS server to the bastion host DNS servers, as well as answers to these queries. Also allow zone transfers in which the bastion host DNS server is the primary server and the internal DNS server is the secondary server; and

* **Default-1 and Default-2**

  Block all packets not specifically allowed by one of the proceeding rules (Chapman, et al.1995:329-337).

Table 3.6 Exterior router (Chapman, et al.1995:333-337).

Rule	Direc -tion	Source Address	Desti- nation Address	Proto- col	Source Port	Desti- nation Port	ACK Set	Action
Spoof-1	In	Internal	Any	Any	Any	Any	Any	Deny
Spoof-2	In	Perim.	Any	Any	Any	Any	Any	Deny
Telnet-1	Out	Internal	Any	TCP	>1023	23	Any	Permit
Telnet-2	In	Any	Internal	TCP	23	>1023	Yes	Permit
FTP-1	Out	Internal	Any	TCP	>1023	21	Any	Permit
FTP-2	In	Any	Internal	TCP	21	>1023	Yes	Permit
FTP-3	Out	Internal	Any	TCP	>1023	>1023	Any	Permit
FTP-4	In	Any	Internal	TCP	>1023	>1023	Yes	Permit
FTP-5	Out	Bastion	Any	TCP	>1023	21	Any	Permit
FTP-6	In	Any	Bastion	TCP	21	>1023	Yes	Permit
FTP-7	In	Any	Bastion	TCP	20	6000-6003	Any	Deny
FTP-8	In	Any	Bastion	TCP	20	>1023	Any	Permit
FTP-9	Out	Bastion	Any	TCP	>1023	20	Yes	Permit
FTP-10	In	Any	Bastion	TCP	>1023	21	Any	Permit
FTP-11	Out	Bastion	Any	TCP	21	>1023	Yes	Permit
FTP-12	Out	Bastion	Any	TCP	20	>1023	Any	Permit
FTP-13	In	Any	Bastion	TCP	>1023	20	Yes	Permit
FTP-14	In	Any	Bastion	TCP	>1023	>1023	Any	Permit
FTP-15	Out	Bastion	Any	TCP	>1023	>1023	Any	Permit
SMTP-1	Out	Bastion	Any	TCP	>1023	25	Any	Permit
SMTP-2	In	Any	Bastion	TCP	25	>1023	Yes	Permit
SMTP-3	In	Any	Bastion	TCP	>1023	25	Any	Permit
SMTP-4	Out	Bastion	Any	TCP	25	>1023	Yes	Permit
NNTP-1	Out	Internal NNTP Server	NNTP Feed Server	TCP	>1023	119	Any	Permit
NNTP-2	In	NNTP Feed Server	Internal NNTP Server	TCP	119	>1023	Yes	Permit
NNTP-3	In	NNTP Feed Server	Internal NNTP Server	TCP	>1023	119	Any	Permit
NNTP-4	Out	Internal NNTP Server	NNTP Feed Server	TCP	119	>1023	Yes	Permit
HTTP-1	Out	Bastion	Any	TCP	>1023	Any	Any	Permit
HTTP-2	In	Any	Bastion	TCP	Any	>1023	Yes	Permit
HTTP-3	In	Any	Bastion	TCP	>1023	80	Any	Permit
HTTP-4	Out	Bastion	Any	TCP	80	>1023	Yes	Permit
DNS-1	Out	Bastion	Any	UDP	53	53	a	Permit
DNS-2	In	Any	Bastion	UDP	53	53	a	Permit
DNS-3	In	Any	Bastion	UDP	Any	53	a	Permit
DNS-4	Out	Bastion	Any	UDP	53	Any	a	Permit
DNS-5	Out	Bastion	Any	TCP	>1023	53	Any	Permit
DNS-6	In	Any	Bastion	TCP	53	>1023	Yes	Permit
DNS-7	In	Any	Bastion	TCP	>1023	53	Any	Permit
DNS-8	Out	Bastion	Any	Any	Any	Any	Any	Permit
Default-1	Out	Any	Any	Any	Any	Any	Any	Deny
Default-2	In	Any	Any	Any	Any	Any	Any	Deny

Explanation of the packet filtering rules in Table 3.6

The exterior router is often managed by an external service provider, and as such, the organisation may not have the ability to maintain it. It is the first point of contact to the organisation's network.

* **Spoof**

  Blocks incoming packets that claim to have internal or perimeter net IP addresses--that is, forged packets presumably sent by an attacker. Rule Spoof-1 is the same as the Spoof rule on the interior router; rule Spoof-2 is unique to the exterior router;

* **Telnet-1 and Telnet-2**

  Allow outgoing Telnet connections. These are identical to the corresponding rules on the interior router (as are the rules on the exterior router that involve internal and external hosts, but nothing on the perimeter net);

* **FTP-1 through FTP-4**

  Allow outgoing passive-mode FTP connections and are identical to the corresponding rules on the interior router;

* **FTP-5 and FTP-6**

  Allow the proxy server on the bastion host to open an FTP command channel to FTP servers on the Internet. Note that, unlike the corresponding rules on the interior router, these rules are not redundant if you have rules FTP-1 and FTP-2 in place earlier in the list. This is

because "Bastion" as a source or destination (covered by rules FTP-5 and FTP-6) is not a subset of "Internal" (covered by rules FTP-1 and FTP-2);

* **FTP-7 through FTP-9**

  Allow FTP data connections from external FTP servers to the proxy server on the bastion host. The FTP-7 rule prevents an attacker from attacking X11 servers on the bastion host via the hole created by rules FTP-8 and FTP-9. If you have other servers on the bastion host listening for connections on TCP ports above 1023, you should add similar rules for them;

* **FTP-10 through FTP-15**

  Allow passive and normal mode FTP from external clients to the anonymous FTP server on the bastion host. There are no equivalent rules on the internal router because there are no FTP servers on the internal network that external clients can access;

* **SMTP-1 and SMTP-2**

  Allow outgoing mail from the bastion hosts to the outside world;

* **SMTP-3 and SMTP-4**

  Allow incoming mail from the outside world to the bastion host;

* **NNTP-1 to NNTP-4**

  Allow Usenet news both ways between our Usenet news server and your service provider's news server. These rules are identical to the corresponding rules on the interior router;

* **HTTP-1 and HTTP-2**

Allow the bastion host HTTP proxy server to connect to the HTTP servers on any machine on the Internet. Actually these rules allow any TCP client program on the bastion host using a port above 1023 to contact any server program on any host on the Internet using any port. This is done so that the HTTP proxy server can contact HTTP servers on non-standard port numbers (i.e., other than port 80). As broad as these rules are, it's important that they allow only outgoing connections, by examining the ACK bit;

* **DNS-1**

  Allows UDP-based DNS queries and answers from the bastion host DNS server to DNS servers in the outside world;

* **DNS-2**

  Allows UDP-based DNS queries and answers from Internet DNS servers to the bastion host DNS Server;

* **DNS-3 and DNS-4**

  Allow external UDP-based DNS clients to query the DNS server on the bastion host and it to answer them;

* **DNS-5 and DNS-6**

  Allow TCP-based DNS queries from the bastion host DNS server to DNS servers on the Internet, as well as answers to those queries. Also allow zone transfers in which the bastion host DNS server is the secondary server and an external DNS server is the primary server;

* **DNS-5 and DNS-6**

Allow TCP-based DNS queries from the outside world to the bastion host DNS servers, as well as answers to these queries. Also allow zone transfers in which the bastion host DNS server is the primary server and the internal DNS server is the secondary server; and

* **Default-1 and Default-2**

  Block all packets not specifically allowed by one of the proceeding rules, just as the corresponding rules do on the interior router (Chapman, et al.1995:329-337).

3.9 SETTING OF PACKET FILTERING RULES

The previous section dealt with possible packet filtering rules. In order for these to be effective, and remain effective, the enterprise should follow certain best practices when setting the packet filtering rules. These include:

* The filtering rules should be edited off-line should they need to be changed. The editing tools provided with the system are usually not very robust, and do not allow easy deletion of rules or modification of specific rules. The organisation should keep the filters in a text file, so they can be edited with a familiar word processor, and merely loaded when required. An added advantage is achieved, as one can add comments to the rules, which are usually stripped off and discarded by the filtering system once loaded;

* The rules should be reloaded from scratch every time. Each time the rules are loaded, a complete new file should be loaded. This prevents the situation where the entity is unsure of how the new rule inserted interacts with the existing rule set;
* The entity should always use IP addresses, never hostnames in the ruleset. The entity should never use actual host names, as the filtering could be subverted if an individual accidentally or intentionally corrupts the name-to-address translation (e.g., by feeding false data to the DNS server);
* The entity should be aware of the implicit defaults. Should a packet not match any of the filtering rules, a default action might be taken. Certain systems deny all such packets, while others make the default the opposite of the last rule, e.g., if the last rule was a "deny", then the system will default to a "permit". The auditor should ensure that the entity puts an explicit default rule at the end of the list of packet filtering rules; and
* The entity should log certain events which occur. The packet filtering router essentially either forwards a packet or drops it. The entity may wish to log all packets which are dropped. This will allow the entity to determine what is being tried that is not allowed (Chapman, et al. 1995:159).

3.10 CONCLUSION

The concept of a firewall is now clearly defined, together with the capabilities and limitations of firewalls. This chapter has explained the two commonly used methods of implementing firewalls, namely packet filtering and proxy services. Further, it has sketched a scenario of a common firewall configuration, namely the screened subnet architecture, and illustrated the setting of packet filtering rules, by giving possible settings in response to an organisation's Internet security policy.

The chapter has equipped the ISA with the requisite technical knowledge necessary to proceed with the audit required. Next, the risks which the ISA faces are explained.

CHAPTER 4

INTERNET RISKS

CONTENTS PAGE

4.1 INTRODUCTION

The Internet presents marvellous opportunities. Millions of people are out there exchanging information. The risks should also be obvious: when you get millions of people together, you get crime; it's true in a city, and it's true on the Internet (Chapman, et al.1995:18).

In order to audit the validity of services provided by the Internet, it is necessary to understand the typical services provided on the Internet, and the risks pertaining to these services. The need for a sound Internet security policy will be researched, as such a policy forms the basis of enforcing security by means of a firewall. The explanation of Internet services has been restricted to include only the common Internet services.

4.2 INTERNET SECURITY POLICY

As Bernstein (1996:208) puts it, "one of the foremost principles to remember is that a firewall should enforce an organisation's policy". The question the ISA is tasked with answering, while auditing validity, is whether or not the firewall's implementation adequately reflects the organisation's Internet policy. Compliance with the policy will ensure that only valid services in terms of the policy are allowed. This means that the auditor must:

* Evaluate whether the current firewall/packet filter is able to enforce the policies;
* Ensure that the process of setting packet filtering rules ensures compliance with the policy; and
* Verify that the current packet filtering rules are appropriate (Bernstein, et al. 1996:211).

A comprehensive Internet security policy should contain the following subjects:

* **Internet services:** The definitions about which Internet services are allowed and detailed guidelines on how to use these services;
* **Security:** The definitions of security implementations, like firewalls that will be used and the standards for these implementations;
* **Privacy** : The definition of reasonable expectations of privacy regarding issues such as monitoring and logging;
* **Access:** Policy statements about access rights and privileges for users, administrators and management; guidelines of how access will be provided using Internet connection types;
* **Accountability:** The definition of responsibilities of users, administrators and management;
* **Authentication:** The definition of policies about the use of authentication devices and remote location authentication;

* **Availability:** The definition of users' expectation for the availability of Internet services like recovery issues and operating hours; and
* **Violation:** The indication of which violation (e.g. privacy, security, internal and external) must be reported and to whom; guidelines on how to handle violation incidents (Ernst and Young, 1996).

The firewall is the chief instrument used to implement an organisation's network security policy (Siyan, 1995:82).

4.3 INTERNET RISKS WHICH TRANSLATE INTO RISK FOR THE ORGANISATION

Invalid users gaining access to your network from the Internet, or internal or external users having use of invalid or unauthorised Internet services all pose a risk to the organisation, and will result in the validity control objective not been achieved.

4.3.1 Types of attacks

There are many types of attacks on systems, and many ways of categorising these attacks.

4.3.1.1 Unauthorised access

The most common attacks on systems are intrusions; with intrusions, people are actually able to use the enterprise's computers. Most attackers want to access an enterprise's computers as if they were legitimate users. They range from social engineering attacks, to simple guesswork, to intricate ways to get in without needing to know an account name and password. One means of unauthorised access is the use of another user's account to access the system without prior permission (Fowler, Huddelston, Tidrow, Robinson, Le Valley and Ringo, 1995:282).

4.3.1.2 Denial of service

A denial of service attack is one that's aimed entirely at preventing you from using your own computers. Although some cases of electronic sabotage involve the actual destruction or shutting down of equipment or data, more often they follow the pattern of flooding. An intruder floods a system or network with messages, processes, or network requests so that no real work can be done. The system or network spends all its time responding to messages and requests, and cannot satisfy any of them.

Most often, the risk of denial of service attacks is unavoidable. If you accept things from the external universe-electronic mail, telephone calls, or packages, it is possible to get flooded. A "packet flood" can overwhelm the capacity of the network or system, rendering it unavailable (Bernstein, et al. 1996:189, Chapman, et al.1995:7).

4.3.1.3 Information theft

Some types of attacks allow an attacker to get data without ever having to directly use the enterprise's computers. Usually these attacks exploit Internet services that are intended to give out information, inducing the services to give out more information than was intended, or to give it out to the wrong people.

Network sniffing is much easier than tapping a telephone line. Traffic that crosses the Internet may cross any number of local area networks, any one of which can be a point of compromise (Chapman, et al.1995:7).

4.3.1.4 Repudiation

With the implementation of electronic commerce, there comes the risk that one or more of the users participating in a transaction will deny participation, which poses a critical threat for electronic financial transactions and electronic contractual agreements (Bernstein, et al. 1996:28).

4.4 TYPICAL SERVICES AND THE RISKS THEY POSE TO USERS WHO ALLOW THEIR USE

The following is a list of only the typical services which are available on the Internet, together with certain risks. These are listed to demonstrate the

need for control over the validity checking of Internet services, and by no means is it an exhaustive list. Should the risks not be controlled in the services listed, this will result in the validity control objective not been achieved.

4.4.1 Electronic mail

Electronic mail is one of the most popular and basic network services. It's relatively low risk, but that doesn't mean it's risk free. Forging electronic mail is trivial, and forgeries facilitate two different types of attacks: attacks against the enterprise's reputation and social manipulation attacks (e.g., attacks in which users are sent mail purporting to come from an administrator and advising them to change to a specific password). Accepting electronic mail ties up computer time and disk space, opening the enterprise up for denial of service attacks (Chapman, et al.1995:254).

4.4.2 File transfer

File Transfer Protocol (FTP) is the Internet standard protocol for file transfer. The primary worry at most sites is that users will bring in Trojan horse software. Although this can happen, actually the larger concern is that users will bring in computer games, pirated software, and pornographic pictures,

which tend to take up an annoying amount of time and disk space, but don't represent a major security risk.

Allowing people to use FTP to transfer files from the computer system is somewhat riskier. To get access to the files an enterprise has made available, users log into the system using FTP with the special login name "anonymous". In setting up an anonymous FTP server, the enterprise will need to ensure that people who use it can't get access to other areas or file on the system, and that they can't use FTP to get shell-level access to the system itself. Writable directories in the anonymous FTP area are a special concern. The enterprise will also need to ensure that its users don't use the server inappropriately (Chapman, et al.1995:254).

4.4.3 Remote terminal access and command execution

Programs that provide remote terminal access allow users to use a remote system as if it were a directly attached terminal.

Telnet is the standard for remote terminal access on the Internet. Telnet was once considered a fairly secure service because it requires users to authenticate themselves. Unfortunately, Telnet sends all of its information undecrypted, which makes it extremely vulnerable to sniffing and hijacking attacks. For this reason, Telnet is now considered one of the most

dangerous services when used to access an enterprise's site from remote systems.

There are various kinds of authentication schemes for doing remote logins, but although authentication protects the password, the session can still be tapped or hijacked.

There are programs besides Telnet that can be used for remote terminal access and remote execution of programs - most notably rlogin, rsh, etc. These programs are used in a trusted environment to allow users remote access without having to re-authenticate themselves. The host they're connecting to trusts the host they're coming from to have correctly authenticated the user. The trusted host model is simply inappropriate for use across the Internet, because one generally cannot trust hosts outside the enterprise's network. In fact, one cannot even be sure the packets are coming from the host they say they are (Chapman, et al.1995:254).

4.4.4 Usenet news

News groups are the Internet counterpart to bulletin boards, and are designed for many-to-many communication.

The risks of news are much like those of electronic mail: users might foolishly trust information received; they might release confidential information; and the enterprise may get flooded.

Network News Transfer Protocol (NNTP) is used to transfer news across the Internet. The biggest security issue with news is what to do with private newsgroups. Many sites create private local newsgroups to facilitate discussions among their users; these private newsgroups often contain sensitive, confidential, or proprietary information. Someone who can access the NNTP server can potentially access these private newsgroups, resulting in disclosure of this information (Chapman, et al.1995:254).

4.4.5 The World Wide Web

The World Wide Web (WWW) is a new, entirely Internet-based concept, based in part on existing services, and in part on a new protocol, HyperText Transfer Protocol (HTTP).

There are two basic sets of security concerns regarding HTTP, namely what a malicious client can do to an enterprises HTTP server, and what a malicious HTTP server can do to the enterprise's clients (Chapman, et al.1995:254).

4.5 CONCLUSION

This chapter has demonstrated that very real risks exist, and has validated the need to ensure validity controls are in place to assist in the mitigation of the risks prevailing, and help ensure that only the services in terms of the enterprise's security are allowed, and in the manner intended.

In addition, the chapter has given an insight into the common Internet services available, and demonstrated the need for a sound Internet security policy.

Together with the preceding chapters, a basis has been formed to set up guidelines for performing specific audit procedures relating to auditing to ensure validity on the Internet.

CHAPTER 5

AUDIT GUIDELINES

CONTENTS PAGE

5.1 INTRODUCTION

Given that the control objective relating to validity is now clearly defined, as well as the related firewall technology, together with the risks prevailing as a result of their application using the Internet, guidelines can be formulated to audit the controls implemented through the use of firewall techniques to mitigate the risks of validity, to a level considered acceptable.

In addition to the review of controls at the detail level, such as the correct packet filtering rules, the ISA also needs to verify that the applicable IT processes implemented by the enterprise are sound, as they contribute to ensuring the overall validity control objective. This includes processes over setting up of the packet filtering rules, selection of a packet filtering router and the monitoring of activities.

5.2 OBJECTIVE

The objective of this chapter is to provide the ISA with guidance as to elements that need to be reviewed, in order that he/ she will be able to assess the level of risk of invalid packets being allowed, or unauthorised use of Internet services. This will include a review of certain general and specific controls. It is necessary to verify certain general aspects such as security policies, as these will contribute indirectly to the specific validity control

implemented by means of the firewall. References to the preceding chapters are made within parenthesis.

5.3 AUDIT GUIDELINES

5.3.1 Network diagram (3.8)

In preparation for the audit, the ISA must request a current copy of the enterprise's most recent network diagram. This will assist in obtaining an understanding of the existence and location of the following important Internet components:

* Location of the designated firewall in relation to the other network components;
* All hosts present, the function and purpose, together with details of the operating system and software products running on each host;
* All routers, taking note of their position in the network;
* All defined networks, identifying internal, perimeter and external networks; and
* Individuals in the organisation who are assigned responsibilities for the various components in the network.

The auditor must perform the following steps using the network diagram:

* Using the network diagram/topology, gain an understanding of the security philosophy deployed, and identify any possible weaknesses in the configuration, which may contribute to invalid entry points, and possible single points of failure which can be reported upon;
* Identify the firewall components (firewalls, routers etc.) to be relied upon to ensure validity, and therefore to be reviewed;
* Document the individuals in the enterprise who are responsible for updating the diagram;
* Enquire as to the process by which the network diagram is updated, and note the version control and the date on which the diagram was last updated. Verify that this process is effective; and
* During the review, note any differences between the actual configuration audited, and that reflected by the network diagram.

5.3.2 Security policy (3.4.2)

A security policy should serve as a foundation for the implementation of security. Although developing a policy will not tangibly ensure validity, the effect of the policy will be reflected in the effectiveness of the security implementation. In order to control the validity control objective via the Internet, it is necessary to have stringent policies and procedures that define and control the conditions under which the enterprise should operate. The ISA should perform the following procedures with regard to security policies:

* Request a copy of the enterprise's security policy, and verify that it clearly specifies the necessary aspects relating to Internet services, security requirements, privacy access, accountability, authentication, and monitoring violations;
* During the review, report on any deviations from the above attributes, specifically in the areas of which services are to be allowed, and the security component;
* Determine whether management has ratified and agreed the policy; and
* Review the process by which the policy is reviewed and updated. Ensure this is performed periodically, and is effective.

5.3.3 Setting of packet filtering rules (3.6.1, 3.9)

The ISA must ensure that the organisation has an effective process to deal with the setting of packet filtering rules. Verify that the process adheres to the following good practice:

* The filtering rules should be edited off-line should they need to be changed;
* The organisation should keep the filters in a text file, so they can be edited with a familiar word processor, and merely loaded when required;
* Ensure that comments are entered, explaining the purpose of each rule. This will ensure that they are easily understood;

* Check that the process requires the rules to be reloaded from scratch every time. This will help ensure the correct rules are loaded;
* Verify that the entity uses IP addresses, and never hostnames in the ruleset;
* Verify that the implicit defaults are understood. Check that in all instances in which a packet does not match any of the filtering rules the correct default action is taken; and
* Validate that the process ensures the correct events are logged.

5.3.4 Evaluating the current firewall/packet filter (3.6)

After examining the network diagram, and the security policies in place, the ISA should document details relating to the enterprises policy with regard to Internet services, security requirements, privacy access, accountability, authentication, and monitoring violations. With this complete, the ISA must verify whether the packet filter used by the enterprise has the capability of implementing the desired policy.

The remainder of this section is a checklist of items to determine the capability of the firewall to achieve the desired level of control:

* For all the requirements listed in terms of the policy, ensure that the packet filter can achieve the control, by ascertaining whether the firewall is configured to implement the specific control;
* Ensure through enquiry of users that the router is fast enough for the entity's needs. If it is not adequate, users may be tempted to gain invalid access through alternative means, which may compromise the enterprises network;
* Verify that the device used to run the firewall is used exclusively for this purpose. Using the device to run other non-security-related software may compromise the network security. Ensure that a dedicated packet filtering router is used;
* Ensure that the enterprise is able to specify the rules for the packet filtering in a simple manner. In this way the packet filtering system will not add more complexity, and increase the inherent risk that invalid connections will be allowed;
* Verify that the packet filtering implementations do not treat packets as simply an unstructured array of bits and require the entity to state rules in terms of the offset and state of particular bits;
* Enquire whether the facility exists to download the rules from another machine. Evaluate whether the current procedure lends itself to easy modification and update of the rules;
* Verify that the system administrator is able to specify rules based on the header information or meta-packet information available for the packets.

Meta-packet information consists of information that the router knows about the packet, but is not contained in the header. An example of this may be the interface the packet came in or is going out on. This will enable the entity's security administrator to specify rules based on combinations of the header and meta-packet information. Ensure that the filter is able to filter on the following header information:

- IP source and destination address;
- IP options;
- Protocol, such as TCP, UDP, or ICMP;
- TCP or UDP source and destination port;
- ICMP message type; and
- Start of connection (ACK bit) information for TCP packets.

* Document the methodology the packet filter uses to apply the rules, and ensure that it applies them in the order specified. Some systems attempt to merge and re-order rules to achieve greater efficiency. This can increase the risk of invalid packets being allowed;
* Verify that the system has the capability and flexibility to specify a separate rule set for incoming and outgoing packets on each interface. If the packet filter only looks at outgoing packets, for example, then the filtering will not protect the router itself from incoming packets. In addition, if the filter only examines outgoing packets, it is difficult, if not impossible, to detect forged packets being inserted from the outside (i.e. packets

coming in from the outside, but which claim to have internal source addresses);

* Determine whether the packet filter has the facility to log all the packets that are dropped. The rules set up reflect the security policy of the entity; therefore should a packet be dropped, by examining it one is able to determine when someone attempts to violate the policy;
* Enquire as to whether the packet filter provides the facility to test and validate the capabilities. This will allow the system administrator to determine whether the router is filtering as intended;
* Verify that the system is configured on the principle of least privilege. Application of this principle as an example is where SMTP is configured so that outgoing mail is routed via the bastion host, rather than directly to the remote systems;
* In reviewing the network diagram, a choke-point should be obvious, so that all traffic between the internal clients and the Internet are channelled through the perimeter network. If this is not apparent, document reasons for this, and satisfy yourself as to the appropriateness of the alternate configuration;
* Establish whether a fail-safe stance is apparent and applied through the packet filtering rules. In general this is achieved through specifically allowing only what is valid, and denying all the remaining options. This will assist in protecting against new services which may be invalid, as they

will not be allowed unless specifically granted through the existing rule set; and

* The ISA must ensure that the setup ensures universal participation. This will ensure that all users must go through the single point of access to the firewall. There should be no other points of access, and the ISA must ensure that the policies in place prohibit individual users from accessing the Internet via a modem, and in this manner compromise the overall security.

5.3.5 Evaluating the current packet filtering rules (3.8.2)

The packet filtering rules are enforced to ensure validity and reflect the network security policy of the organisation, and are therefore fundamental in ensuring that all traffic is valid. The auditor should obtain a printout of the packet filtering rules, and verify that they are appropriate.

Often the auditor is faced with the situation that the exterior router is maintained by the Internet service provider, and thus it is difficult to audit. In these circumstances, such an audit is not achievable, and in all likelihood, the auditor will not be able to audit it as the service provider will be unwilling to allow this. At a minimum, the ISA should examine the contract with the service provider, and review the content for any weaknesses that might exist

in terms of what the enterprise is relying on the service provider to have in place. This makes auditing the interior router even more important, as the exterior router merely becomes a backup to the interior router.

A methodology has been suggested by means of which all rules can be audited. This does not attempt to dictate a specific rule design for all possible services and the permutations possible. Each situation is different, and to prescribe rules would be dangerous. Imperative to the task is a good understanding of the network security policies to be implemented by the packet filter, against each service.

* The ISA must obtain a printout of the current packet filtering rules for the interior, exterior and all other relevant packet filters, and ensure that they represent the actual rules used in production, and validate that they are not an old version;
* The ISA must use the already documented details relating to the enterprises policy with regard to Internet services, security requirements, privacy access, accountability, authentication, and monitoring violations. With this information, the ISA will be able to verify the implementation of the network security policy by means of the filtering rules. The ISA must ensure that each relevant policy is represented by a specific rule, in the rule set, ensuring its enforcement;

* The auditor needs to perform the review on an iterative basis for each rule in the printout, verifying the accuracy of the following information:

  - The nature of the service which is to be allowed or disallowed. This may be FTP or HTTP for example;
  - The direction of the connection. "In" usually refers to traffic from the external Internet, with its destination being the internal enterprise network and will apply to external users accessing the enterprise's internal network. "Out" usually refers to internal users of the enterprise requiring access to the external Internet;
  - The full association, consisting of the source (local) address, the destination (remote) address, the protocol type, the source (local) port and the destination (remote) port;
  - Other additional information such as ACK bit; and
  - Whether or not the service is to be allowed or denied.

* In addition to the rules relating to specific known services, verify that there is a rule covering spoofing, or forged packets from the outside purporting to be an internal user. The rule should be similar to the following:

Rule	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK Set	Action
Spoof-1	In	Internal	Any	Any	Any	Any	Any	Deny

* There should be a rule, usually at the end of the list, which deals with blocking all packets not specifically allowed by any of the proceeding rules. This may be illustrated as follows:

Rule	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK Set	Action
Default-1	Out	Any	Any	Any	Any	Any	Any	Deny
Default-2	In	Any	Any	Any	Any	Any	Any	Deny

Clearly all packets not satisfying any previous rule are denied, regardless of direction, source address, destination address, protocol type, source port, destination port or ACK bit setting;

* The following is given as an illustration of how the ISA may approach a policy implementation. Should the enterprise network security policy indicate that, in relation to Telnet, they have trustworthy users and proper IP addresses, and that proxying for Telnet does not have an advantage over packet filtering, they will allow all outgoing Telnet, but block all incoming Telnet, and the rule would be as follows:

Rule	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK Set	Action
Telnet-1	Out	Internal	Any	TCP	>1023	23	Any	Permit
Telnet-2	In	Any	Internal	TCP	23	>1023	Yes	Permit

Note that no incoming Telnet sessions are allowed as the ACK bit must not be set for the first packet. As the rule for incoming traffic requires the ACK bit to be set, it is in response to the outgoing connection already set-up. The incoming request for a Telnet session would be denied by the default rule usually at the end of the access list; and

* The ISA must evaluate each rule in turn, ensuring that it reflects the security policy and wishes of management.

5.3.6 Evaluating the monitoring/logging of firewall activities, as a detection control to ensure validity (3.7)

The IT auditor must ensure that the activities of the firewall are logged. This will contribute to the validity control objective by ensuring that all services allowed or disallowed are in line with the security policy of the organisation. During the audit/evaluation of the monitoring, the auditor must ensure that the entity is logging the following, at a minimum:

* All dropped packets;
* All denied connections;
* All rejected attempts;
* For every successful connection to or through the bastion host:
    - Time;
    - Protocol; and
    - User name.
* All error messages from the routers, bastion host, and any proxying programs;
* Multiple failed attempts to log in to valid accounts on the machines, particularly accounts that are used across the Internet, or attempts on accounts in the order in which they appear in the password file;

* Unusual accepted packets or commands which appear mysterious or illogical;
* Successful logins from an unexpected site;
* Deleted or modified log files;
* Programs that abruptly omit expected information (this tends to suggest that the programs have been replaced with versions that ignore the intruder's files and programs);
* New log files containing password information or packet traces that are unexplainable;
* Directories that contain more administrative entries than expected. On Unix machines, a directory that contains more than two files with name made out of periods ("." And "..") should not be duplicated. If there is an extra entry, it is likely to have spaces in it, and may be used to conceal the file or directory from casual observation;
* Unexpected logins as privileged users (such as root), or unexpected users who suddenly are able to become privileged users;
* Apparent probes or attacks coming from the entity's own machines;
* Extra processes with names that are variants of common system processes (e.g., both sendmail and Sendmail are running, or *init* and *initd*; this is a way of trying to conceal invalid or modified services); and
* An unexpected change in the login prompt for a machine.

In addition, the auditor must ensure that the following client activities/management controls are in place:

* Most of the logging will probably be done via the UNIX syslog facility. The client should have developed scripts (or obtained them with their firewall), which facilitates the analysis and summarising of the logs;
* The auditor should ask for copies of such logs as evidence of the client's review;
* Ensure that the client writes scripts to filter out messages to be ignored. If this is not done, the log file will prove too verbose, and will not be effective for reviewing;
* The auditor must examine the filter scripts to ensure that the correct rules and filters are in place;
* For security reasons, the client should not log passwords that were used in failed attempts. However, the failed attempt should be logged. Because users frequently mistype their own passwords, logging these mistyped passwords would make it easier for an intruder to break into a user's account; and
* The auditor must validate that there is a process in place to review the packet filtering rules on a regular basis, to ensure they are current, and continually reflect the network security policy, and thereby the wishes of management;

5.4 CONCLUSION

In the opinion of the author, the objective of this chapter has been achieved. A comprehensive set of guidelines has been developed for the ISA to evaluate validity controls implemented by means of firewall techniques.

CHAPTER 6

CONCLUSION

6.1 INTRODUCTION

The main problem stems from the astounding rate at which the Internet has grown, coupled with the increasing use of the Internet by businesses in re-engineering and speeding up their business processes.

With the use of this new technology arises the need to audit the business processes, and the resulting accounting information. Management are still responsible for the implementation of adequate and effective controls, and auditors for the evaluation thereof.

6.2 CONCLUSION

The research has provided a basis for understanding the problem, together with the enabling Internet technology, and the risks they present.

The objective set for this dissertation has been met. The objectives were to provide the information systems auditor with guidelines, identifying what needs to be audited to assist in determining whether an entity has achieved

the control objective relating to validity, with specific reference to firewall techniques.

The guidelines developed are not meant to be an all-inclusive set of issues to audit; they should however, cover the important aspects. An approach has been suggested for the evaluation of the packet filtering rules; however it does not attempt to prescribe what the rules should reflect in any given situation. It is emphasised that the example firewall configurations in Table 3.5 and Table 3.6 are merely examples. The ISA should not blindly compare these to the client-specific rules. Instead, the ISA should first take the time to understand the needs of the client, the environment, and the implications and complications of the services they wish to offer, in terms of their Internet security policy. A comprehensive discussion on all the possible Internet services available, together their unique and specific risks, is outside the scope of this dissertation.

The investigation has opened up new fields of academic research. Further fields for research include:

* Auditing accuracy and completeness on the Internet;
* Auditing the provision of authenticated or non-anonymous services on the Internet;

* The auditor's role in developing Internet security policies and procedures; and
* Detailed analysis of the risks resulting from the use of various Internet services.

BIBLIOGRAPHY

BERSTEIN, T; BHIMANI, A; SCHULTZ, E; SIEGAL, C 1996: Internet Security for Business. John Wiley & Sons, Inc.

BOSHOFF, WH 1985: The interface between application and integrity controls in modern computer systems. Johannesburg: Rand Afrikaans University (M. Comm dissertation).

BOSHOFF, WH 1990: A Path Context Model for computer security phenomena in potentially non-secure environments. Johannesburg: Rand Afrikaans University (D. Comm thesis).

CHAPMAN, DB & ZWICKY, ED 1995 : Building Internet Firewalls. Sebastopol CA : O'Reilly & Associates.

CHESWICK, R & BELLOVIN, S 1994 : Firewalls and Internet Security, Repelling the Wily Hacker. Massachusetts : Addison-Wesley Publishing Company.

DAMIANIDES, M 1991: A control model for the evaluation and analysis of control facilities in a simple path context model in a MVS/XA environment. Johannesburg: Rand Afrikaans University (M. Comm dissertation).

ERNST & YOUNG 1994 : Building Network Firewalls with Routers and Bridges : Technical Briefing Series.

ERNST & YOUNG 1997 : 1997 Special Report Technology in Banking & Financial Services, Managing the Value Network .

The INSTITUTE OF INTERNAL AUDITORS RESEARCH FOUNDATION 1994b: Systems audibility and control. Module1. Executive summary. Almonte Springs. 27 p.

JENKINS, B; PERRY, R; COOKE, P 1986 : An Audit Approach to Computers, Third addition. Great Britain : Staples Printers St Albans Limited at The Priory Press.

KROL, E 1992 : The Whole Internet User's Guide & Catalog. Sebastopol CA : O'Reilly & Associates.

NATIONAL COMPUTER SECURITY ASSOCIATION 1996 : NCSA Firewall Policy Guide.

REALAUDIO. 1997. Firewall Support. [Online]. Available URL address: http/www.realaudio.com/help/firewall/info.html.

SAICA 1989: Auditing in a computer environment. Audit and accounting guide. Johannesburg. 37 p.

SCHWARTAU, W 1996 : Information Warfare : Chaos on the Electronic Superhighway. IS Audit & Control Journal - The Journal of Information Systems Audit & Control Association, Volume I, 1996 : 10-12.

SCHWARTAU, W 1996 : Creating Boundries, Protecting Companies and Employees on the Information Superhighway. IS Audit & Control Journal - The Journal of Information Systems Audit & Control Association, Volume I, 1996 : 28-32.

SECURE COMPUTING. 1996. The BorderWare Firewall Server 4.0. [Online]. Available URL address: http:/www/sctc/com/borderware/white.html.

STAIR, RM 1992: Principles of information systems. A managerial approach. Boston: Boyd and Fraser. 701 p.

SIYAN, K; 1995 : Implementing Internet Security, New Riders Publishing : Indianapolis, Indiana.

WATNE, D; TURNEY, PB 1984 : Auditing EDP Systems, Second addition. New Jersey : Prentice-Hall.

FURTHER READING

BORN, E 1996 : Enforcing Legal Ownership Rights by an Access Control System. Computers & Security - Official Journal of IFIP TC 11, Volume 15, No. 3, 1996 : 212-220.

COBB, S 1996 : The Internet : A Technical Primer. IS Audit & Control Journal - The Journal of Information Systems Audit & Control Association, Volume I, 1996 : 36-39.

CURRY, DA 1992 : Unix® System Security, A Guide for Users and System Administrators. Massachusetts : Addison-Wesley Publishing Company, Inc.

DELOITTE & TOUCHE : Information Proctection, Your Business and The Internet, New approaches for new environments.

DEVON SOFTWARE CORP. 1996. KyberPassTM. [Online]. Available URL address: http://www.magi.com/~devon/table.html.

ERNST & YOUNG 1993 : A Practical Approach to Logical Access Control. Berkshire England : McGRAW-HILL Book Company Europe.

FIREWALL SECURITY CORPORATION. 1997. Firewall Security Corporation Home Page : Authentication. [Online]. Available URL address: http:/www/frus.com.

HUDOBA, S 1995 : Why the Internet?. IS Audit & Control Journal - The Journal of Information Systems Audit & Control Association, Volume I, 1996 : 11-13.

INTERNET SECURITY INCORPORATED. 1996. The Normal Firewall, Serious Internet Protection. [Online]. Available URL address: http://www.inter-secure.com/prod01.htm.

INTERNET SECURITY INCORPORATED. 1993. Connecting to the Internet : Security Considerations. [Online]. Available URL address: http://www.inter-secure.com/csl9307.htm.

INTERNET SECURITY INCORPORATED. 1993. Security Program Mangement. [Online]. Available URL address: http://www.inter-secure.com/csl9308.htm.

INTERNET SECURITY INCORPORATED. 1993. Connecting to the Internet : Security Considerations. [Online]. Available URL address: http://www.inter-secure.com/csl9307.htm.

INTERNET SECURITY INCORPORATED. 1993. People : An important asset in computer security. [Online]. Available URL address: http://www.inter-secure.com/csl9310.htm.

KOGAN, A; SUDIT, E; VASARHELYI M 1996 : Implications of Internet Technology : On-Line Auditing and Cryptography. IS Audit & Control Journal - The Journal of Information Systems Audit & Control Association, Volume III, 1996 : 42-27.

KRÜGER, WJ 1993 : Authorisation as audit risk in an information technology environment. Vanderbijlpark : Rand Afrikaans University (M Com dissertation).

KOGAN, A; SUDIT, E; VASARHELYI M 1996 : Auditor, Firefighter, Lumberjack. IS Audit & Control Journal - The Journal of Information Systems Audit & Control Association, Volume I, 1996 : 24-27.

RANUN, MJ. 1996. Thinking About Firewalls. [Online]. Available URL address: mjr@tis.com.

SUN MICROSYSTEMS, INC. 1997. Solstice™ Firewall-1™ 2.1. [Online]. Available URL address: http://www.sun.com/solstice/Networking-products/fw-1v2.html.

US DEPARTMENT OF DEFENSE. 1997. Orange Book Summary. [Online]. Available URL address: http://www.dmu.ac.uk./~chl/orange.html.

WANG, S; CHANG, J 1996 : Smart card based secure password authentication scheme. Computers & Security - Official Journal of IFIP TC 11, Volume 15, No. 3, 1996 : 231-237.