SECURITY FEATURES IN A UNIX™ INTERNET FIREWALL WITH SPECIFIC REFERENCE TO GAUNTLET™ VERSION 3.1

by

WOUTER VAN DEN HEEVER

SHORT DISSERTATION

submitted in partial fulfilment of the requirements for the degree

MASTERS OF COMMERCE

in

COMPUTER AUDITING

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at the

RAND AFRIKAANS UNIVERSITY

STUDY LEADER: PROF A DU TOIT

JOHANNESBURG
NOVEMBER 1997

DECLARATION

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

Wouter van den Heever

ACKNOWLEDGEMENTS

I would like to thank Prof A du Toit and Prof WH Boshoff for their valuable ideas on the title of this dissertation as well as for their contributions in shaping my attitude and approach towards the science of Computer Auditing.

I would like to thank my wife and my son for their contribution in the successful completion of this dissertation.

I would like to thank God, without whom nothing is possible.

INDEX

SEKURITEITSEIENSKAPPE IN 'N UNIX™ INTERNET KEERWAL MET SPESIFIEKE VERWYSING NA GAUNTLET™ WEERGAWE 3.1.

DEUR

WOUTER VAN DEN HEEVER

OPSOMMING VAN DIE SKRIPSIE INGEDIEN VIR DIE GRAAD

MAGISTER COMMERCII IN REKENAAROUDITERING

IN DIE FAKULTEIT EKONOMIESE EN BESTUURSWETENSKAPPE

AAN DIE RANDSE AFRIKAANSE UNIVERSITEIT

STUDIELEIER: PROF A DU TOIT

JOHANNESBURG
NOVEMBER 1997

Die doel van die opsomming is om die agtergrond, metodiek en gevolgtrekkings van die navorsing oor die sekuriteitseienskappe van 'n Gauntlet™ weergawe 3.1 keerwal ("firewall") weer te gee. Hierdie opsomming is onder die volgende hoofde uiteengesit:

1. PROBLEEMOMSKRYWING EN DOEL MET HIERDIE NAVORSING
2. NAVORSINGSMETODIEK EN BEPERKINGS
3. RESULTATE
4. GEVOLGTREKKING

1. PROBLEEMOMSKRYWING EN DOEL MET HIERDIE NAVORSING

Die ouditeur moet tydens die uitvoering van 'n oudit 'n opinie uitspreek oor die redelikheid van die onderneming wat geoudit word se finansiële state. Die ouditeur se taak kan bemoeilik word indien die onderneming gebruik maak van tegnologies gevorderde rekenaartoerusting en toepassings. Die oudit van ondernemings wat toegang het tot die Internet en die Internet gebruik om sekere van hul besigheidsfunksies te vervul, kan addisionele eise aan die ouditeur stel, aangesien hy nou sy ouditprosedures moet aanpas om voorsiening te maak vir die moontlike impak wat die onderneming se Internetbedrywighede op die uitvoering van sy oudit het. 'n Belangrike voortvloeisel uit die feit dat 'n onderneming toegang het tot die Internet, is die feit dat alle ander instansies wat toegang het tot die Internet, nou ook toegang het (deur die Internet) tot die onderneming se rekenaarinfrastruktuur (en meer spesifiek, sy data).

'n Beproefde manier om sekuriteit te verleen aan 'n onderneming wat gekoppel is aan die Internet, is om gebruik te maak van 'n keerwal ("firewall"). 'n Keerwal dien as "buffer" tussen die onderneming se interne netwerke en alle ander netwerke buite die onderneming (Internet). 'n Keerwal se effektiwiteit word egter beperk tot die effektiwiteit waarmee dit opgestel en bedryf word.

'n Omvattende model moet dus vir die ouditeur ontwikkel word ten einde hom in staat te stel om (vanuit 'n sekuriteitsoogpunt) die keerwal se effektiwiteit en doeltreffendheid te kan beoordeel.

Daar is geen twyfel oor die belangrikheid van Internet keerwalle in die besigheidsomgewing nie. Die aantal besighede wat toegang het tot die Internet en besigheid bedryf op die Internet, het die afgelope paar jaar eksponensieel toegeneem. Die Gauntlet™ Internet keerwal ("firewall") is die keuse van duisende instansies regoor die wêreld, insluitende die Amerikaanse departement van verdediging.

Die hoofrede hoekom 'n studie van sekuriteitsfunksies van die Gauntlet™ Internet keerwal benodig word, is die feit dat die Gauntlet™ Internet keerwal nie outomaties veilig is nie. Daar is parameters wat gestel moet word om Gauntlet™ veilig te maak.

Die doel met hierdie navorsing is om die ouditeur behulpsaam te wees om die effektiwiteit van 'n Gauntlet™ Internet keerwal, met betrekking tot sekuriteit, te beoordeel.

2. NAVORSINGSMETODIEK EN BEPERKINGS

Die Gauntlet™ Internet keerwal sekuriteitsmodel is ontwikkel deur ouditdoelwitte wat op keerwalle van toepassing is, as basis te gebruik. Die sekuriteits-ouditdoelwitte is geldigheid en integriteit van data.

Metodiek:

1. 'n Literatuurstudie van bestaande gesaghebbende literatuur oor keerwalle, en in besonder die Gauntlet™ Internet keerwal, is uitgevoer; en
2. Al hierdie inligting is daarna verwerk om 'n sekuriteitsmodel vir Gauntlet™ weergawe 3.1 daar te stel.

Ten einde die studieveld af te baken en sodoende betekenisvolle studie te kon doen, is 'n aantal beperkings en uitsluitings, wat as volg opgesom kan word, gespesifiseer:

- Sekuriteitspakkette en derdeparty-bestuursagteware is geïgnoreer, want die doel van die studie was om Gauntlet™ te evalueer;
- Sekuriteitsfunksies van die konvensionele UNIX™ bedryfstelsel word slegs opgesom in hoofstuk 2, omdat Gauntlet™ sy eie "verharde" weergawe van UNIX™ gebruik;
- Ander toepassingsprogrammatuur (buiten Gauntlet™) is buite rekening gelaat;
- Die gebruik van die Gauntlet™ kriptografiese bord is uitgesluit van hierdie skripsie, aangesien dit slegs beskikbaar is vir sekere bedryfstelsels en in die algemeen net in die VSA en Kanada beskikbaar is; en
- Kwessies wat nie 'n direkte invloed op die effektiwiteit van die keerwal het nie, byvoorbeeld fisiese sekuriteit, is buite rekening gelaat.

3. RESULTATE

'n Sekuriteitsmodel vir 'n Gauntlet™ Internet keerwal is as gevolg van hierdie studie ontwikkel. Gauntlet™ verskaf sekuriteitsopsies vir die volgende beskikbare dienste:

- Terminaaldienste (TELNET and Rlogin);
- Elektroniese pos (SMTP and POP3);
- Lêeroordragdienste (FTP);
- Verwyderde uitvoering (Rsh);
- Gebruikersnet nuus (NNTP);

- Internet webdienste (HTTP, SHTTP, and SSL);
- Gopher dienste (Gopher, Gopher+);
- X Window dienste (X11); en
- Drukdienste (LP).

Die matriks in hoofstuk 4 beskryf, onder andere, die attribute en sintaks vir elk van die sekuriteitsfunksies in Gauntlet™. 'n Opsomming van hierdie matriks word hieronder gegee:

Gauntlet sekuriteitsfunksie	Attribute om te gebruik
SMTP	badadmin, baddir en userid
POP3	authenticate, authserver, destination, userid en hosts
TERMINAAL-DIENSTE	authenticate, authserver, destination, password change, hosts, timeout en userid
FTP	authenticate, authserver, destination, userid, hosts en timeout
RSH DIENSTE	hosts, timeout, userid en destination
GOPHER EN WWW	destination, hosts, timeout en userid
X WINDOWS	hosts, display, userid en timeout
LP DIENSTE	destination, userid, timeout, client en hosts
NNTP EN TCP	destination, userid, timeout en hosts
INLIGTINGS-DIENSTE	userid, timeout, hosts en destination

Voorts word algemene dienste wat deur Gauntlet™ verskaf word, ook in die matriks bespreek. Die algemene dienste wat bespreek word bestaan uit :

- Rekordhouding en verslagdoening;
- Verifikasie van integriteit; en
- Gebruikerbevestiging.

4. GEVOLGTREKKING

Die belangrikste probleem wat geïdentifiseer is, is die feit dat 'n Gauntlet™ Internet keerwal effektief en doeltreffend opgestel en bedryf moet word ten einde sekuriteit te verleen aan die onderneming wat aan die Internet gekoppel is. Die keerwal se sekuriteit word geoptimaliseer deur die model toe te pas.

Die model wat ontwikkel is, is nie bedoel as 'n plaasvervanger vir doeltreffende ouditprosedures nie, maar eerder as 'n hulpmiddel vir die onafhanklike ouditeur in sy aanslag van die effektiwiteit van 'n Gauntlet™ Internet keerwal om 'n onderneming se data te beskerm. Kliëntediens (waar die ouditeur advies gee aan 'n kliënt en nie net die oudit verrig nie) is vir baie ouditeure 'n belangrike funksie van hul take en hierdie diens kan uitgebrei word deur die gebruik van die model. 'n Voorbeeld van so 'n geval is waar die ouditeur genader word om sy kliënt te adviseer oor sekuriteitsaspekte, waar die kliënt beoog om 'n keerwal aan te koop en in die besigheid te implementeer.

Dit volg dat nuwe velde vir akademiese navorsing hierdeur geopen word - veral in die veld van die impak wat die gebruik van 'n Internet keerwal op die bereiking van ouditdoelwitte het. 'n Voorbeeld hiervan is die ontwikkeling en toetsing van spesifieke ouditprosedures vir die oudit van 'n Internet keerwal.

SYNOPSIS

1. PROBLEM DESCRIPTION AND OBJECTIVE OF THIS SHORT DISSERTATION

Because of the increased number of businesses having access to and conducting business on the Internet, there is a need for security for those businesses conducting business in this way. A way widely accepted and used by organisations all over the world to achieve said security, is to make use of a firewall. In this short dissertation a specific firewall, the Gauntlet™ Internet Firewall, is studied.

A Gauntlet™ Internet Firewall is not secure by default. There is a need to configure and operate this firewall efficiently in order to utilise its security functions to the fullest.

The objective of this short dissertation is to help the auditor in his assessment of the efficiency (from a security point of view) of a Gauntlet™ Internet Firewall.

2. RESEARCH METHODOLOGY

1. A literature survey has been done on authoritative text books and other literature, such as users' manuals; and
2. With all the information obtained in the literature survey, a matrix for security functions, in Gauntlet™ ver. 3.1 has been developed.

3. SCOPE AND LIMITATIONS

This short dissertation focuses on the Gauntlet™ ver. 3.1 Firewall.

Certain exclusions apply to this dissertation:

- Security packages and security features of specific application programs were not considered, as the objective of this dissertation is to focus on the specified firewall software;

- Security functions of the conventional UNIX™ operating system have only been summarised in chapter 2, as Gauntlet™ uses its own "hardened" version of the UNIX™ operating system;
- Aspects not having a direct impact on security (for example LAN system speed) have been ignored, as the objective of this dissertation is to focus on the specified firewall software; and
- The use of the Gauntlet™ cryptographic board, which encrypts data for firewall-to-firewall communications, has been excluded from this dissertation as it is available for some operating systems only and is generally only available in the USA and Canada.

4. RESULTS

A security matrix for Gauntlet™ ver. 3.1 has been developed as a result of this study. Gauntlet™ provides security features for the following services:

- Terminal services (TELNET and Rlogin);
- Electronic mail (SMTP and POP3);
- File transfer services (FTP);
- Remote Execution (Rsh);
- Usenet news (NNTP);
- Web services (HTTP, SHTTP, and SSL);
- Gopher services (Gopher, Gopher+);
- X Window services (X11); and
- Printing services (LP).

In addition, it provides general management services (for example logging) which should form an integral part of the firewall's security.

5. CONCLUSION

The main problem identified is the fact that Gauntlet™ is not by default secure. The implementation and operation of a Gauntlet™ Firewall should be effectively managed in order to be able to utilise its security functions to the fullest.

In summary, this research has provided a basis for the understanding and optimising of security functions available in Gauntlet™ ver. 3.1.

The matrix that has been developed is not meant to be a replacement, but an enhancement for effective auditing procedures, for the auditor in assessing the effectiveness of a Gauntlet™ Internet Firewall in protecting an organisation's resources and, what is more important, its data.

CHAPTER 1: INTRODUCTION

This study intends to develop a matrix for the independent auditor with regard to the audit of an organisation linked to the Internet and using a firewall, with Gauntlet™ ver 3.1, as access control, with specific reference to the security features of Gauntlet™ ver 3.1. The objective of this chapter is to provide background information about research in the area of security features of Gauntlet™ ver 3.1. This chapter is presented under the following headings:

1.1 BACKGROUND
1.2 PROBLEM DESCRIPTION
1.3 OBJECTIVE OF THIS SHORT DISSERTATION
1.4 SCOPE, LIMITATIONS AND EXCLUSIONS
1.5 METHODOLOGY AND DEFINITIONS
1.6 RESEARCH APPROACH
1.7 SUMMARY OF RESULTS
1.8 CONCLUSION

1.1 BACKGROUND

With the dramatic increase in the number of businesses having access to and doing business on the Internet within such a short period of time, it comes as no surprise to read not only of the advantages of conducting business in this way, but also of the potential dangers involved if a business does not take adequate precautions to protect its valuable information technology resources.

The independent auditor is deeply involved with this technology advancement - not by choice, but by the need to keep up with technology. The auditor needs to have a basic understanding of all new information system technologies used by his clients in order to determine the extent of the impact it has on himself in the performance of his duties.

The independent auditor must issue an independent audit opinion on a set of financial statements. In order for the auditor to issue such opinion he must perform certain procedures (an audit). The result of these procedures will assist the auditor in deciding whether the desired audit objectives (see below) have been achieved.

Should the auditor decide to rely on existing internal accounting and system controls to ensure that the financial statements are a fair version of the financial affairs of a business at a certain date, he must investigate, analyse and test such internal controls before relying on them. The auditor must be convinced that the internal control systems are adequate and functioning properly and have been adequate and functioning properly during the entire period under the auditor's review.

According to Arens and Loebbecke (1988:509) the four audit objectives the auditor will wish to see achieved are as follows:

Completeness - to ensure that data is not lost or erroneously or maliciously deleted;
Accuracy - to ensure that data is reliable and not corrupt and that data is used in processing as it was intended;
Validity - to ensure that only authorised users, data and transactions are allowed; and
Maintenance - to ensure that programs, data, files and transactions are not subject to unauthorised changes or duplication.

Once an organisation does business on the Internet, it exposes itself to a whole array of risks. This happens as, in the same way that the organisation now has access to the Internet, anybody with access to the Internet now has access to the organisation's computer systems and data. A number of risks, stemming from the above-mentioned, for the organisation and its data, can be identified. External parties suddenly have unlimited access to business data. Physical access security is now rendered useless as outside parties are able to obtain access into the business by way of a telephone line.

The independent auditor now has to assess his position, the additional audit risks as well as the possible impact on desired audit objectives created by the fact that the company is linked to outside networks.

A typical configuration, showing the placement of an Internet Firewall, is given in Figure 1.1.

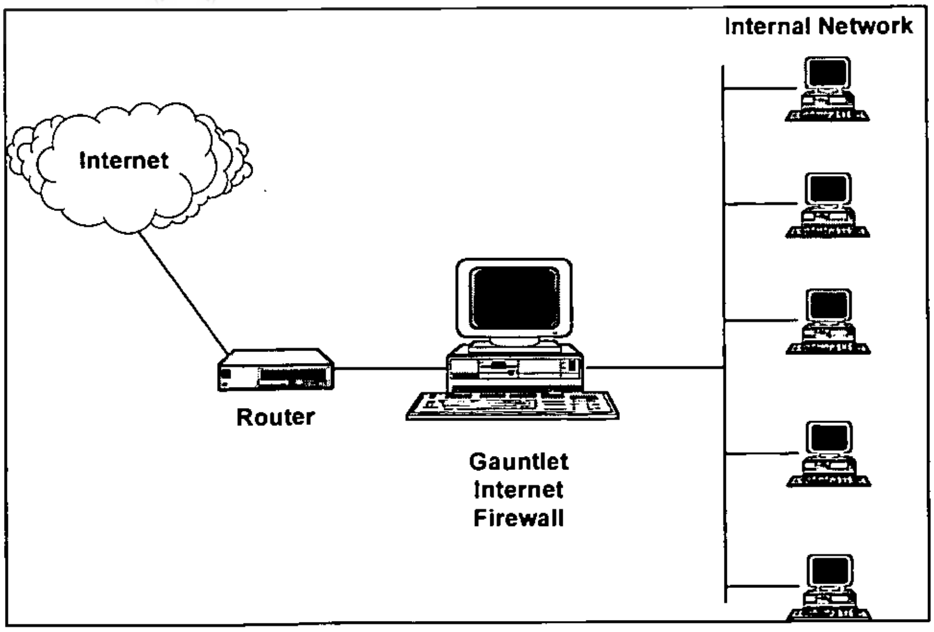

Figure 1.1 Gauntlet™ Internet Firewall Standard Configuration (Trusted Information Systems Incorporated, 1996:8).

The firewall is helping to establish a security perimeter to protect the internal network. It screens all requests that need to pass from one side of the firewall to the other. Using rules laid down by the organisation involved, based on their security policies, the firewall determines whether to accept or pass requests to the other side. To protect the inside network, the firewall must be able to see all the packets intended for hosts on the inside network (Trusted Information Systems Incorporated, 1996:141).

1.2 PROBLEM DESCRIPTION

Chapman and Zwicky (1995:4) state that when one is connected to the Internet, one is putting three things at risk, *vis-à-vis*:

- One's data;
- One's resources (the computers themselves); and
- One's reputation.

Cheswick and Bellovin (1994:9) recommend using firewalls to protect networks and minimise danger, while Chapman and Zwicky (1995:19) are of the opinion that firewalls can do a lot for the security of one's site.

Siyan and Hare (1995:119) are of the opinion that when intruders try to penetrate one's network, they usually try to subvert hosts on the system, which, if improperly configured, can easily be achieved. They further state that misconfigured systems account for a large number of network security problems.

According to Cheswick and Bellovin (1994:6), a key decision in the security policy is the stance of the firewall design of an organisation. The correct design and configuration of any firewall (including Gauntlet™) are therefore of cardinal importance.

It is evident, from the above-mentioned that security is an important issue when it comes to the design and implementation of a firewall in an organisation.

The problem that this dissertation tries to solve is which available security functions in Gauntlet™ ver 3.1 should be used (and, more important, how they should be configured) in order to maximise data security, that is the full achievement of the validity and integrity audit objectives for the independent auditor.

1.3 OBJECTIVE OF THIS SHORT DISSERTATION

The objective of this dissertation is to produce a matrix for the independent auditor to be used when performing an audit of a client using Gauntlet™ Firewall software, to evaluate the efficiency and effectiveness of the Gauntlet™ Firewall software insofar as achieving desired security audit objectives of validity and maintenance is concerned. Furthermore, an additional purpose of this matrix is to serve as source reference for the auditor to advise his clients on the set-up and parameter settings of the Gauntlet™ Firewall when implementing it at their organisations.

1.4 SCOPE, LIMITATIONS AND EXCLUSIONS

1.4.1 The Predefined Environment

This short dissertation focuses on the Internet Firewall, Gauntlet™ version 3.1. Although a specific version of the software has been used, the principles do not change, regardless of the version being used.

According to Trusted Information Systems Incorporated (1996:5-6), the components of a Gauntlet™ Internet Firewall are the following:

- **Hardware** (network interface cards and an optional cryptographic board); and
- **Software** (a "hardened" version of the UNIX™ operating system and application level security services).

1.4.2 Control objectives

The audit objectives of an audit remain unchanged, whether the system being audited is a manual or a computer system. According to Arens and Loebbecke (1988:509) the audit objectives are the following:

COMPLETENESS

To ensure that data is not lost or erroneously or maliciously deleted.

ACCURACY

To ensure that data is reliable and not corrupt and that data is used in processing as it was intended.

VALIDITY

To ensure that only authorised users, data and transactions are allowed.

MAINTENANCE

To ensure that programs, data, files and transactions are not subject to unauthorised changes and duplication.

The two audit objectives directly influenced by the use of a Gauntlet™ Internet Firewall are **validity** and **maintenance**, in other words, security.

1.4.3 Limitations / Exclusions

The following exclusions are noted:

- Security packages and security features of specific application programs were not considered, as the objective of this short dissertation is to focus on the specified firewall software;
- Security functions of the conventional UNIX™ operating system were only summarised in chapter 2, as Gauntlet™ uses its own "hardened" version of the UNIX™ operating system;
- Aspects not having a direct impact on the system (for example physical security) were ignored, as the objective of this short dissertation is to focus on the specified firewall software;
- The use of the Gauntlet™ cryptographic board, which encrypts data for firewall-to-firewall communications, was excluded from this dissertation as it is available for some operating systems only and is generally only available in the USA and Canada;
- Other considerations, such as LAN system speed and system versatility were ignored, as the objective of this short dissertation is to focus on the specified firewall software; and
- The achievement of the audit objectives of completeness and accuracy is specifically excluded, as they do not pertain to security.

1.5 METHODOLOGY AND DEFINITIONS

1.5.1 Methodology

The following methodology was used:

1. A literature survey was done of existing authoritative textbooks and other literature on UNIX™ and firewalls in general, and specifically on the Gauntlet™ Internet Firewall; and
2. With all the information obtained in the literature survey, a matrix for available security features in Gauntlet™ ver. 3.1, was developed.

In this chapter, seen from a security point of view, the need for the efficient set-up during implementation as well as the optimum operation thereafter of Gauntlet™ Internet Firewall software, has been established.

In chapter 2, security functions of the UNIX™ operating system, as they pertain to an Internet Firewall, are summarised. A detailed discussion on this topic was avoided, as it falls outside the scope of this dissertation. In chapter 3, the security features of the Gauntlet™ ver. 3.1 Internet Firewall are discussed. Each available service (proxy), as well as general firewall services (for example logging), are discussed in detail. Chapter 4 consists of a matrix for the independent auditor, detailing the available proxies and general firewall services. The matrix developed in this chapter may assist the auditor in determining the degree to which desired audit objectives have been met when auditing a client using a Gauntlet™ Internet Firewall. Chapter 5 concludes the short dissertation and indicates whether the objective of the dissertation has been met or not.

1.5.2 Definitions

Administrator

"The individual responsible for a system or network. The firewall administrator is responsible for the maintenance and administration of the firewall" (Trusted Information Systems Incorporated, 1996:137).

Audit objectives

Completeness - to ensure that data is not lost or erroneously or maliciously deleted;

Accuracy - to ensure that data is reliable and not corrupt and that data is used in processing as it was intended;

Validity - to ensure that only authorised users, data and transactions are allowed; and

Maintenance - to ensure that programs, data, files and transactions are not subject to unauthorised changes or duplication (Arens & Loebbecke, 1988:509).

Firewall

"A configuration of routers and networks placed between an organisation's internal network and a connection to an external network (Internet), to provide security" (Trusted Information Systems Incorporated, 1996:138).

Inside Network

"The network of machines protected by the firewall inside the defence perimeter" (Trusted Information Systems Incorporated, 1996:139).

Internet

"A three-tier hierarchy, which consists of networks for a common service channel, a middle tier and pieces of data. They connect several different physical networks, all over the world, by way of several protocols, including the Internet protocol" (Trusted Information Systems Incorporated, 1996:139).

Outside network

"The network of machines not protected by the firewall (outside the defence perimeter). When a firewall protects a network connected to the Internet, the outside network consists of the rest of the Internet" (Trusted Information Systems Incorporated, 1996:139).

Port

"A specific pathway for data and control information" (Trusted Information Systems Incorporated, 1996:140).

Proxy

"Specialised applications or programs that run on a firewall host. These programs take users' requests for Internet services (such as FTP and Telnet) and forward them according to the site's security policy. Proxies are replacements for actual services and serve as application-level gateways to the services" (Trusted Information Systems Incorporated, 1996:140).

Router

"A special purpose, dedicated machine that attaches to two or more networks and forwards packets from one to the other. An IP router forwards IP datagrams among the networks to which it is connected. An IP router uses the destination address on the datagram to choose the next hop to which it forwards a datagram" (Trusted Information Systems Incorporated, 1996:141).

Risk

"...a risk is merely the degree of loss...a person, thing, event, or idea that poses some danger to an asset" (Stang,1993:52).

Security

"Any measure taken to safeguard against unauthorised access, accidental or deliberate interference with operations, destruction, or unauthorised modification of information..." (Stang, 1993:1122).

Trusted network

"The network of machines protected by the firewall" (Trusted Information Systems Incorporated, 1996:142).

Untrusted network

"The network of machines not protected by the firewall, but from which the firewall accepts requests" (Trusted Information Systems Incorporated, 1996:142).

1.6 RESEARCH APPROACH

The research approach was as follows:

A literature study of authoritative literature on UNIX™, firewalls and Gauntlet™ was done. The results were used to develop a matrix for available security features in Gauntlet™.

In this chapter the need for the efficient set-up, during implementation, of Gauntlet™ Internet Firewall software, has been established.

In Chapter 2, security functions of the UNIX™ operating system, as they pertain to an Internet Firewall, are summarised.

In Chapter 3, the security features of the Gauntlet™ ver. 3.1 Internet Firewall will be discussed in detail.

Chapter 4 will consist of a matrix for the independent auditor of the available proxies and general firewall services in Gauntlet™.

Chapter 5 will conclude the short dissertation and indicate whether the objective of the dissertation has been met or not.

1.7 SUMMARY OF RESULTS

1.7.1 Introduction

Just as organisations should have a general security policy for their organisation, the Gauntlet™ Internet Firewall uses policies to summarise its rules. The policies are collections of rules about what the firewall can and cannot do in particular situations. They indicate which proxies can run, and whether they require authentication, special logging, or other general settings. The firewall policies the system administrator should create, should be based on the organisation's security policies.

By default, the Gauntlet™ Firewall includes one set of policies for requests from trusted networks and one set of policies for requests from un-trusted networks. The firewall determines which policy applies by the source IP address of the request. The default policy for trusted networks allows for a variety of services. It does not require users to authenticate. The default policy for untrusted networks allows for only a few services. It requires users to authenticate before accessing hosts inside the security perimeter. The system administrator can modify these default policies to match the security policy.

When the firewall is set up, the networks from which the firewall can accept requests, but which are not trusted, are explicitly configured. By default, after initial configuration, the un-trusted networks are all networks outside the inside security perimeter.

The firewall applies different policies (sets of rules) for requests from untrusted networks than it does for requests from trusted networks. For some types of requests the firewall may require additional authentication before processing the request.

1.7.2 Software

The software components of the firewall include a hardened operating system, application level security services, security programs, and other management utilities. A discussion is given below:

1.7.2.1 Operating System

The operating system is a hardened version of one of several UNIX™ systems. As part of the firewall, these operating systems have been tailored to provide support for only the services necessary to run the firewall.

1.7.2.2 Application Level Security Services (Proxies)

The software on the Gauntlet™ Firewall includes security services on a per application basis. On the firewall, proxy software relays information from one side of the firewall to the other. The proxy prevents the applications on outside networks from communicating directly with the applications on the inside network, and *vice versa*. No IP packets pass from one side of the firewall to the other. All data is passed at the application level.

Each application generally communicates through a different proxy that understands the protocol for that application. Gauntlet™ ver. 3.1 includes proxies for the following types of services:

- Terminal services (TELNET and Rlogin);
- Electronic mail (SMTP and POP3);
- File transfer services (FTP);
- Remote Execution (Rsh);
- Usenet news (NNTP);
- Web services (HTTP, SHTTP, and SSL);
- Gopher services (Gopher, Gopher+);
- X Window services (X11); and
- Printing services (LP).

All the proxies are configurable. The administrator can accept or reject requests to or from certain sites and networks, or set up other rules that the proxies use when passing requests through the firewall. The administrator can also enable or disable individual proxies and run only those needed. The proxies log all activities to and through the firewall. The administrator can use the logs to gather usage statistics or to look for potential attacks. In addition, several of the proxies support strong user authentication systems. These one-time passwords or security token systems provide additional security because users use a different password each time they access the network.

1.7.2.3 Security programs

The Gauntlet™ Firewall includes additional security software as an IP screening utility. This feature checks IP packets based on several criteria (for example, address) and processes or rejects the packets. It detects spoofed packets claiming to be from one network that are actually from another network. Using this utility, the firewall can be configured so that it is transparent to the users for most activities.

1.7.2.4 Management Utilities

In addition, the Gauntlet™ Firewall also contains several programs that ease the job of administering the firewall. These include management tools for configuring the firewall, scripts for reporting activity through the firewall and performing general administration.

1.7.2.5 Summary

A summary of the matrix, illustrating security functions and relevant attributes as set out in chapter 4, is given in Table 1.1.

Table 1.1 Security functions and attributes of Gauntlet™ ver. 3.1

GAUNTLET™ SECURITY FUNCTION	ATTRIBUTE(S)
SMTP	badadmin, baddir and userid
POP3	authenticate, authserver, destination, userid and hosts
TERMINAL SERVICES	authenticate, authserver, destination, password change, hosts, timeout and userid
FTP	authenticate, authserver, destination, userid, hosts and timeout
RSH SERVICES	hosts, timeout, userid and destination
GOPHER AND WWW	destination, hosts, timeout and userid
X WINDOWS	hosts, display, userid and timeout
LP SERVICES	destination, userid, timeout, client and hosts
NNTP AND TCP	destination, userid, timeout and hosts
INFORMATION SERVICES	userid, timeout, hosts and destination

General firewall services in Gauntlet™ are also discussed in the matrix. These services include:

- Logging and reporting;
- Verifying integrity; and
- User authentication.

1.8 CONCLUSION

A matrix depicting the relative importance as well as preferred settings for a Gauntlet™ Internet Firewall, seen from a security point of view, was developed as a result of this study.

Gauntlet™ provides security functions for the following services (the name of the proxy it uses, is indicated in brackets):

- Terminal services (TELNET and Rlogin);
- Electronic mail (SMTP and POP3);
- File transfer services (FTP);
- Remote Execution (Rsh);
- Usenet news (NNTP);
- Web services (HTTP, SHTTP, and SSL);
- Gopher services (Gopher, Gopher+);
- X Window services (X11); and
- Printing services (LP).

All the above services influence, though some to a lesser degree, the audit objectives of validity and maintenance. The developed matrix serves as an enhancement to thorough auditing procedures. Its aim is to guide the independent auditor in his assessment of the adequacy of internal control in an organisation. It also aims to educate the independent auditor as to the possible impact that the use of a Gauntlet™ Firewall has on the validity and maintenance audit objectives.

The research opens new fields for academic research in the area of the impact on desired audit objectives by security features in an Internet Firewall environment, such as the design and testing of specific audit procedures for the audit of an Internet Firewall.

CHAPTER 2: SUMMARY OF UNIX™ INTERNET SECURITY FEATURES

This chapter covers the actual literature study of UNIX™ Internet security features. Chapter 3 covers the literature study of Gauntlet™ ver. 3.1 in order to determine the available security features in Gauntlet™ ver. 3.1, which would then be used to prepare the matrix in Chapter 4. This chapter is presented under the following headings:

2.1 OBJECTIVE
2.2 NATURE OF LITERATURE STUDY
2.3 SCOPE, LIMITATIONS AND EXCLUSIONS
2.4 DEFINITIONS
2.5 DISCUSSION OF SECURITY FEATURES IN UNIX™
2.6 CONCLUSION

2.1 OBJECTIVE

The objective of the literature study in this chapter, is to summarise the available security functions in the UNIX™ operating system.

2.2 NATURE OF LITERATURE STUDY

To ensure credibility and acceptance of the findings (in chapters 2 and 3) and proposals of this short dissertation, it is essential that the underlying concepts should be based on authoritative views and be generally accepted among computer auditing professionals. Theory based on an individual's experience, without taking generally accepted professional views into account, may be subject to personal bias. Other factors which may introduce bias are the individual's background and the absence of formal research. To avoid these problems, references have been restricted to authoritative technical books and manuals by information technology experts and auditing specialists. The main categories of authors/publishers are:

- IDG Books Worldwide, Inc;
- O'Reilly and Associates, Inc. publishing company;
- Addison-Wesley publishing company;
- New Riders Publishing;
- Prentice-Hall, Inc. publishing company; and
- Trusted Information Systems Incorporated, developer of the Gauntlet™ Firewall; the firewall used by, amongst others, the United States Department of Defence.

The reasons for choosing these authors/publishers are the following:

- They represent an internationally accepted view of auditing; and
- They represent an internationally accepted view of firewalls and firewall security.

2.3 SCOPE, LIMITATIONS AND EXCLUSIONS

2.3.1 Scope

For this chapter, existing authoritative textbooks had to be surveyed to obtain an in-depth understanding of firewalls and, specifically, UNIX™ firewall security.

2.3.2 Limitations and exclusions

To achieve the objectives of the literature survey in this chapter, it was necessary to examine and analyse all security features of the UNIX™ operating system. The following limitations and exclusions were consequently placed on the scope of the literature survey:

- Only issues which dealt with UNIX™ Internet Firewall security were included. Sections in the references that dealt with non-related issues were thus excluded; and
- Inferior references and opinions of individuals were ignored, as the objectives of this survey require authoritative references.

2.4 DEFINITIONS

Definitions of terms used in this dissertation are set out below (Trusted Information Systems Incorporated, 1996:137-142):

- ***APOP***: A version of Post Office Protocol (POP) which uses non-reusable passwords for authentication.
- ***ARP***: Address Resolution Protocol: Allows a host to find the physical address of a target host on the same physical network, given only the target's IP address. The protocol used to dynamically bind an IP Address to a physical hardware address. The use of ARP is restricted to a single physical network and is limited to networks that support hardware broadcast.
- ***Authentication***: Method to guarantee that the sender of information is whom the sender purports to be.
- ***Bastion host***: A secure computer that forms part of a security firewall and runs applications that communicate with computers outside an organisation.
- ***Chroot***: The chroot mechanism allows a program to irreversibly change its view of the file system by changing where the root of the file system is. When a program chroots to a particular portion of a given file system, that portion becomes the whole file system and, in effect, the rest of the file system ceases to exist, from the program's point of view.

- ***Defence perimeter**:* The mechanisms used to protect a network of machines.
- ***Domain***: A part of the DNS naming hierarchy. Domain names consist of a sequence of names (labels) separated by full stops (dots).
- ***Dual-homed***: A dual-homed host has two network interfaces, hence addresses and acts as a router between the subnetworks to which those interfaces are attached.
- ***Encryption***: A mechanism for changing the appearance of data. Encryption allows the creation of secure connections over insecure channels. Encrypting network traffic provides both privacy and authentication.
- ***Ftp***: File Transfer Protocol: The TCP/IP standard, high-level protocol for file transfer from one machine to another. FTP uses TCP.
- ***Ftpd***: FTP daemon. One of the programs that implement ftp.
- ***Gated*** (Gateway Daemon): A program run on a host or router that collects routing information from within one autonomous system and advertises the information to another autonomous system.
- ***Gateway***: Dedicated host that interconnects two different services or applications (for example an e-mail gateway).
- ***Group***: A collection of users with a common security concern.
- ***Hardened***: An analogy indicating that an operating system or application has been modified to eliminate elements that make it vulnerable to failure.
- ***HTML*** (HyperText Meta Language): The language used to implement network resource pages.
- ***HTTP*** (HyperText Transfer Protocol): The primary application protocol that underlies the World Wide Web.
- ***Inetd***: The program that listens for requests for services specified in the */etc/inetd.conf* configuration file. When it

hears such a request, it starts the proper server to process the request.

- ***IP Address*** (Internet address): A 32-bit integer address assigned to each host on the Internet.
- ***Mail exchanger***: A host that accepts e-mail; some mail exchangers forward the mail to other hosts. DNS has a separate address type for mail exchangers (MX records).
- ***Mail gateway***: A host that connects to two or more dissimilar electronic mail systems and transfers mail messages among them.
- ***Netacl***: A program that provides the capability of a TCP Wrapper.
- ***Netperm table***: The network permissions table that contains Gauntlet™ configuration information used by the kernel, proxies, and other applications. The configuration information is in the form of policy or applications rules.
- ***NIC***: Network Interface Card.
- ***Packet filter***: A method to select or deselect traffic from given network addresses.
- ***Packet filtering gateway***: A system that gateways protocols, using simple packet content rules.
- ***POP*** (Post Office Protocol): A client-server protocol for handling user electronic mailboxes. The user's mailbox is kept on the server, rather than on the user's personal machine.
- ***Protocol***: A formal description of message formats and the rules that must be followed to exchange those messages.
- ***Rlogin*** (Remote LOGIN): The remote login protocol developed for UNIX™ by Berkeley. Rlogin offers a service similar to Telnet.
- ***Security perimeter***: The mechanisms used to protect a network of machines.

- ***Smap***: A small program intended solely for dealing with incoming SMTP connections. The relative simplicity of smap allows it to be easily examined and considered in its entirety for security problems.
- ***Smapd***: A second program that is invoked regularly (typically once a minute) to process the files queued in the queue directory, normally by handing them to Sendmail for delivery.
- ***SMTP*** (Simple Mail Transfer Protocol): The TCP/IP standard protocol for transferring electronic mail messages from one host to another. SMTP specifies how two hosts interact and the format of control messages they exchange to transfer mail.
- ***Strong authentication system***: A system for verifying users. It uses one-time, non-reusable passwords.
- ***TCP/IP***: Transmission Control Protocol and the Internet Protocol refer to an entire suite of data communications protocols.
- ***TCP wrapper***: The TCP Wrapper package monitors incoming network traffic and controls network activity. It is a simple but effective piece of publicly available software set up to run whenever certain ports (corresponding to certain services) are connected.
- ***UDP*** (User Datagram Protocol): The TCP/IP standard protocol that allows an application program on one host to send a datagram to an application program on another. UDP uses IP to deliver datagrams but UDP includes a protocol port number, allowing the sender to distinguish between application programs on a given remote host.
- ***URL*** (Uniform Resource Locator): A string that gives the location of information. The string begins with a protocol type (for example, FTP, HTTP) followed by the domain name of a server and the path name to a file on that server.

- ***WWW*** (World Wide Web): The large-scale information service that allows a user to browse information. WWW offers a hypermedia system that can store information as text, graphics, audio, etc.

2.5 DISCUSSION OF SECURITY FEATURES IN UNIX™

2.5.1 Password file

The first line of defence against unauthorised access to the system is the */etc/password* file. Unfortunately it is also often the weakest link. Access is only granted after entering a correct password. The password file consists of lines or records in which each line is split into seven fields with a colon, as illustrated in the following example (Siyan & Hare, 1995:59):

1) Syntax
   username:encrypted password:UID:GID:comment:home directory:login shell - (one line).

2) Actual example
   chare:u7mHuh5R4UmVo:105:100:Chris Hare:/u/chare:/bin/ksh - (one line); and

2.5.2 Trusted Computing Base

The trusted computing base is comprised of a collection of software including the UNIX™ kernel and the utilities that maintain the trusted computing base. These utilities include *authchk* for verifying and correcting problems in the password database and integrity for verification of the accuracy of the system files. The trusted computing base implements the security policy on the system. This policy is a set of operating rules that govern the interaction between subjects such as processes, and objects such as files, devices, and interprocess communication objects (Siyan & Hare, 1995:72).

2.5.3 Permissions

The permissions that UNIX™ uses on each file determine how access to the files and directories is controlled. The permissions applied to a file are based upon the UID and GID (Group ID) stamped on the file and the UID or GID of the user trying to access the file. According to Siyan & Hare (1995:77) the three sets of permissions are as follows:

- Those applicable to the owner of the file;
- The users who have the same GID as that on the file; and
- All other users.

For each category of users, there are three permissions bits: read, write and execute (Siyan & Hare, 1995:77).

2.5.4 Kerberos Authentication

Kerberos is an authentication system that validates a principal's identity. A principal can be either a user or a service. According to Siyan and Hare (1995:84), in either case, the principal is defined by the following three components:

- Primary name;
- Instance; and
- Realm.

2.6 CONCLUSION

The UNIX™ operating system provides basic security features. It is very important, however, to implement a firewall once an organisation is connected to the Internet.

CHAPTER 3: DETAILED ANALYSIS OF GAUNTLET™ VER. 3.1 INTERNET FIREWALL SECURITY FEATURES

This chapter covers the actual literature study of Gauntlet™ ver. 3.1 in order to determine its available security features, which would then be used to prepare the matrix in chapter four. This chapter is presented under the following headings:

3.1 OBJECTIVE
3.2 SCOPE, LIMITATIONS AND EXCLUSIONS
3.3 BACKGROUND
3.4 DISCUSSION OF SERVICES (PROXIES) IN GAUNTLET™ VER. 3.1
3.5 DISCUSSION OF GENERAL GAUNTLET™ VER. 3.1 FIREWALL SERVICES
3.6 CONCLUSION

3.1 OBJECTIVE

The objective of this literature study is to analyse, in detail, the available security functions in Gauntlet™ ver. 3.1 and, by analysing it, determining the relevant importance of said security features for the independent auditor. Furthermore, the ultimate goal of this analysis is to use it as a basis to produce a matrix for the independent auditor, reflecting the relevant importance and ideal settings of each available security function.

3.2 SCOPE, LIMITATIONS AND EXCLUSIONS

3.2.1 Scope

Existing authoritative textbooks had to be surveyed to obtain an in depth understanding of firewalls and, specifically, firewall security in general. This, in turn, had to be applied to the Gauntlet™ Internet Firewall.

As none of the above-mentioned textbooks are product specific, reliance was placed on the Gauntlet™ Internet Firewall administrator's guide for guidance, as it relates to specific security issues in Gauntlet™ version 3.1.

3.2.2 Limitations and exclusions

To achieve the objectives of the literature survey, it was necessary to examine and analyse all security features of a Gauntlet™ Internet Firewall. The following limitations and exclusions were consequently placed on the scope of the literature survey:

- Only issues which dealt with Gauntlet™ ver. 3.1 Internet Firewall security were included. Sections in the references that dealt with non-related issues were thus excluded;
- Inferior references and opinions of individuals were ignored, as the objectives of this survey require authoritative references;
- As this short dissertation principally deals with Gauntlet™ ver. 3.1, references to application controls and risks and other integrity controls and risks have not been included; and
- As there are no books on Gauntlet™ available in the public press, the Gauntlet™ Internet Firewall administrator's guide was the only available source for the literature study in this chapter.

3.3 BACKGROUND

The physical placement of a firewall in an organisation's network, can be graphically depicted as in figure 3.1.

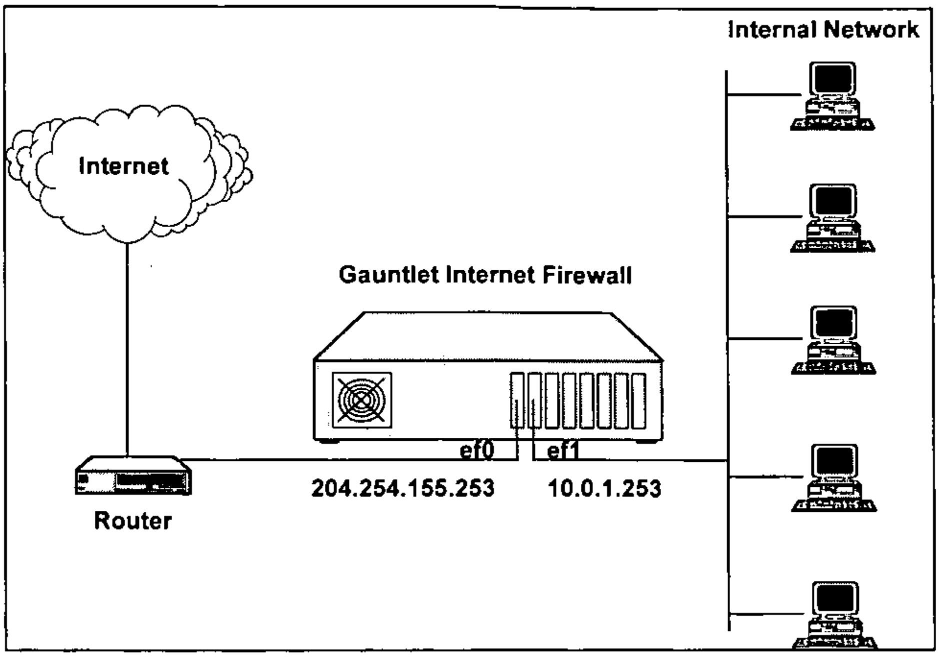

Figure 3.1 Placement of an Internet Firewall as a Dual Homed Bastion Host (Trusted Information Systems Incorporated, 1996:9).

As a dual-homed bastion host (which is the supported configuration of this dissertation), the firewall machine has two network interface cards, thus two connections, one to the internal network and one to outside networks (Internet). **All** outside network traffic must enter and exit the firewall through one network interface, such as ef0 (see figure 3.1 above). Similarly, **all** inside network traffic must enter and exit through a network interface, such as ef1 (see figure 3.1 above). To accomplish this, each interface has a separate IP address. An IP address can be defined as a 32-bit integer address assigned to each host on the Internet. The organisation was assigned the 204.254.155 network and chose 204.254.155.253 as the outside IP address (see figure 3.1 above). It chose 10.0.1.253 (see figure 3.1 above) for the inside IP address (Trusted Information Systems Incorporated, 1996:141).

Assuming the organisation is using Ethernet and the BSD/OS version of the Gauntlet™ Internet Firewall, the interface is known as *ef0*. Other operating systems and other topologies may use other interface names, such as *lan0* or *le0* (Trusted Information Systems Incorporated, 1996:141).

Once a firewall is in place and the auditor is convinced that it is functioning effectively, the auditor can rely on the internal control provided by the firewall as a basis for assuming that the integrity and validity audit objectives, insofar as the connection to outside networks is concerned, have been achieved.

It is, however, problematic for the independent auditor to actually determine if a firewall is functioning effectively because, amongst other reasons, it is a highly technical information technology issue and not all auditors have adequate technical knowledge regarding firewalls.

The Gauntlet™ Internet Firewall exemplifies a minimalist and reductionist approach. It follows the paradigm: that which is not expressly permitted is prohibited. The firewall must explicitly allow activities; either through system defaults or through the organisation's own configurations. New services cannot slip through the firewall, unless they are allowed through the firewall. The organisation must be able to identify and remove any "backdoors" that may be grand-fathered into place (Trusted Information Systems Incorporated, 1996:3).

The network permissions table (*netperm table*) contains configuration information for the Gauntlet™ Internet Firewall. The kernel, proxies and other applications read their configuration information from this table. The rules in the table include two types of information: policy rules and application-specific rules (Trusted Information Systems Incorporated, 1996:111).

3.3.1 Policy Rules

Policies are collections of general configuration information. These allow one to closely map the organisation's security policy to policies for the Gauntlet™ Firewall. According to Trusted Information Systems Incorporated (1996:111) Gauntlet™ configuration policies include information such as:

- Types of proxies that the firewall can start;
- Permitted (or denied) destinations for requests; and
- Authentication requirements.

The **source address** of a request is the basis for **a** policy. The default Gauntlet™ configuration defines two policies: an inside policy and an outside policy (Trusted Information Systems Incorporated, 1996:111).

The inside policy defines the general policies for requests from the inside (trusted) networks. This policy indicates that proxies can send requests to any destination. This policy also allows users to change their passwords for strong authentication systems from the inside networks (Trusted Information Systems Incorporated, 1996:111).

The outside policy defines the general policies for requests from the outside (untrusted) networks. This policy indicates that proxies can send requests to any destination. It requires strong authentication for all outside requests with the authentication server that is on the firewall (Trusted Information Systems Incorporated, 1996:111).

3.3.2 Application-specific rules

The *netperm-table* also includes configuration information for proxies and other firewall applications. According to Trusted Information Systems Incorporated (1996:112) these include:

- Userid and groupid under which a proxy should run;
- Directories the proxies should use as their root directories;
- Text files proxies should display when denying or accepting requests;
- Length of idle time before the proxies should terminate the connection; and
- More specific lists of permitted and denied destination networks for a particular proxy.

Because the proxies and applications read the *netperm-table* from top to bottom, the system administrator must place proxy-specific rules before the generic policies. When the relevant proxy parses the configuration information, it uses the proxy-specific rule rather than the more general policy rule (Trusted Information Systems Incorporated, 1996:112).

3.3.3 Applications

Other Gauntlet™ applications such as the authentication server, *gauntlet-gui* interface and IP screening utility also read configuration information from the *netperm-table.* (Trusted Information Systems Incorporated, 1996:112).

3.3.4 How Gauntlet™ uses the information contained in the Netperm table

As part of the start-up process a proxy or application reads the *netperm-table* looking for applicable configuration rules. It parses the table from top to bottom, looking for rules that match its name. It also matches wildcard rules that apply to all applications. (Trusted Information Systems Incorporated, 1996:113).

The proxy first uses these rules to determine if it can accept the request from the source address. It then determines whether the requested service is an explicitly permitted service. If it is not, the proxy denies the request. If it can accept the request, it uses the other rules to determine whether it needs to authenticate the request, and whether it can send the request to the specified destination. The application also finds and uses rules for that specific application (Trusted Information Systems Incorporated, 1996:113).

3.3.5 Trusted and untrusted network tables

The Gauntlet™ Internet Firewall uses a simple policy of trusted and untrusted networks. The following paragraphs explain the purpose, format and precedence of the tables the Gauntlet™ Firewall uses to specify these networks.

3.3.5.1 Trusted Networks Table

The trusted networks table contains a list of all networks that the Gauntlet™ Firewall trusts. This means that the Gauntlet™ Firewall does not require requests from hosts on these networks to provide authentication. The proxies and other applications can trust their requests (Trusted Information Systems Incorporated, 1996:107).

This table should be used to implement the organisation's basic security policy. Many policies indicate the firewall can trust hosts behind the firewall (on the inside network). In this scenario, administrators can add the addresses for their inside networks to this table (Trusted Information Systems Incorporated, 1996:107).

3.3.5.2 Untrusted Networks Table

The untrusted networks table contains a list of all networks that the Gauntlet™ Firewall does not trust. This means that the Gauntlet™ Firewall requires requests from hosts on these networks to provide authentication. The proxies and other applications will process these requests only after authenticating the user (Trusted Information Systems Incorporated, 1996:107).

By default, the untrusted table includes the wildcard '*'. This indicates that the firewall will accept requests from any other network after authenticating the user (Trusted Information Systems Incorporated, 1996:107).

This table should also be used to implement the organisation's basic security policy. Some policies do not allow any outside access, while others allow access only after authentication. (Trusted Information Systems Incorporated, 1996:107).

3.3.5.3 How Gauntlet™ ver. 3.1 uses the information contained in these tables

The proxies and other Gauntlet™ Firewall applications use the information in the trusted and untrusted network tables when determining whether to accept a request, and whether to authenticate the request. However, they do not read these tables directly. Instead, an update script takes the information in the trusted and untrusted tables and creates rules in the *netperm-*

table. This update script runs when one updates the configuration information using the Gauntlet™ administration tools. When the proxies start, they read these rules from the *netperm-table* (Trusted Information Systems Incorporated, 1996:107).

It is now necessary to analyse, in detail, the steps the firewall takes for packets it receives on either interface.

3.3.6 Receives Packet

Routing information on outside hosts directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertise the outside IP address of the firewall as the **ONLY** way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall (Trusted Information Systems Incorporated, 1996:10).

3.3.7 Checks Source and Destination

Once the firewall receives a packet it must determine what to do with it. First, the operating system kernel examines the destination of the packet and determines whether it needs to deliver the packet locally. Local delivery includes packets destined for hosts inside the firewall. The firewall absorbs these packets and redirects them to an appropriate proxy. If there is no proxy configured to accept a packet, the firewall drops the packet and drops the failed access (Trusted Information Systems Incorporated, 1996:10).

Next, the firewall examines the source address of the packet and the interface on which it received the packet. If this check indicates that this request could not possibly have come in through this interface, it rejects the packet and logs it. (Trusted Information Systems Incorporated, 1996:137).

3.3.8 Checks Request Type

If the firewall is configured to deliver the packet locally, it examines the contents of the packet. The operating system checks various tables on the firewall to determine if it offers the requested service on the requested port. If it does not, it logs the attempt as a potential security alert and rejects the request (Trusted Information Systems Incorporated, 1996:10).

3.3.9 Runs Appropriate Program

If the firewall is configured to offer the requested service, the operating system uses other configuration information to start the appropriate program. (Trusted Information Systems Incorporated, 1996:10).

3.3.10 Processes the Request

The proxy or application now processes the request. It first checks its configuration information. The proxy determines how to handle the request based on the source (IP address) of the request. By default, it uses one policy (set of rules) for trusted networks and another policy for untrusted networks (Trusted Information Systems Incorporated, 1996:11).

Once configured, the proxy processes the requests as the standard application would. Requesting applications think they are communicating with an actual server, not a proxy (Trusted Information Systems Incorporated, 1996:11).

The proxies also check to determine if the request is permitted for the destination. For some services, the proxies can perform the additional step of authenticating the user. This verification provides additional assurance that the users are really who they say they are. The proxy then passes the request to the appropriate program on the other side of the firewall, using the standard protocol for that service (Trusted Information Systems Incorporated, 1996:11).

3.4. DISCUSSION OF SERVICES (PROXIES) IN GAUNTLET™ VER. 3.1

3.4.1. SMTP SERVICES

The protocol for transferring mail around the Internet is the Simple Mail Transport Protocol (SMTP). A message transfer agent, such as the sendmail program used on many UNIX™ systems handles the transfer requests. The design of reductionism does not allow the use of *sendmail* as a critical security component of the Gauntlet™ Firewall. The Gauntlet™ Firewall includes a two-part proxy that securely handles the transfer of SMTP mail between the inside and outside networks (Trusted Information Systems Incorporated, 1996:15).

The proxy for SMTP is actually two processes: a client (*smap*) and daemon (*smapd*). Together, they provide configurable access control and logging mechanisms. The processes running on the firewall transfer mail between internal and external mail servers, based on supplied rules. The proxies also prevent versions of *sendmail* on the inside network from communicating with versions of *sendmail* on the outside network. The proxies log all successful and unsuccessful mail connections, and the number of bytes transferred (Trusted Information Systems Incorporated, 1996:15).

The firewall runs the client proxy (smap) as a daemon listening for requests on the standard SMTP port (25). When the firewall receives requests for SMTP services on this port, the *smap* client collects the mail from the sender, logs the message and places the mail in a temporary directory. Periodically, based on a configurable value (by default every 1 minute), the daemon (*smapd*) wakes up and checks to see if there is any new mail. The *smapd* daemon checks the headers of the mail for formatting problems. It then calls the configured message transfer agent (usually *sendmail* in delivery mode) for final delivery (Trusted Information Systems Incorporated, 1996:15).

A common policy is to have one mail hub for the inside network. In this scenario, outside networks know (by way of DNS) that they should send all mail for the domains (****.com*) on the inside networks to the firewall (*firewall.***.com*) itself for processing. An outside host informs the firewall it has mail. The firewall checks the appropriate configuration files (*/etc/services and /etc/rc.local*) and determines that it needs to start (or call) the *smap* client. The *smap* client collects the mail from the outside host and writes it to a directory (*/var/spool/smap*) on the firewall (Trusted Information Systems Incorporated, 1996:16).

3.4.2 POP3 SERVICES

Employees and companies are expanding the places in which and the types of machines on which they need to read their electronic mail. For a variety of reasons, it may not be convenient to run a full mail transfer system using SMTP on these systems. The Post Office Protocol Version 3 (POP3) is one of the protocols that allows a workstation to access a mail server. The POP3 proxy included with the Gauntlet™ Firewall allows administrators to selectively allow outside hosts to exchange mail with a POP3 mail server through the firewall. The POP3 server must use APOP for authenticating the user (Trusted Information Systems Incorporated, 1996:19).

The Gauntlet POP3 proxy is an application level gateway that provides configurable access control, authentication and logging mechanisms. According to Trusted Information Systems Incorporated (1996:19) the POP3 proxy, which runs on the firewall, transfers mail between external workstations and internal mail servers, based on:

- Source IP address;
- Source host name;
- Destination IP address;
- Destination host name; and
- User name.

The POP3 proxy can be configured to allow inside workstations to exchange mail with POP3 servers outside the perimeter. According to most security policies (including the Gauntlet™ Firewall default), it's just not a good idea. The POP3 protocol assumes that the SMTP proxy has already checked the formatting in the headers of incoming mail messages. In addition, allowing POP3 clients to communicate with outside mail servers adds another level of complexity. It bypasses the central control centre of the inside mail hub, which rewrites addresses and enforces other company policies. The mail server should be behind the firewall on the inside network. All POP3 clients on the inside network can collect their mail from this mail server (Trusted Information Systems Incorporated, 1996:19).

The firewall runs the POP3 proxy (pop3-gw) as a daemon listening for requests on the standard POP3 port (110). When the firewall receives requests for POP3 services on this port the proxy checks its configuration information (in the *netperm-table*) and determines whether the initiating host has permission to use POP3 services. If the host does not have permission, the proxy logs the connection and displays an error message (Trusted Information Systems Incorporated, 1996:20).

If the host has permission, the POP3 proxy authenticates the user using APOP and logs the connection. The proxy then passes the message on to the POP3 server on the internal mail hub, and authenticates on behalf of the user using APOP. The proxy remains active until either side terminates the connection (Trusted Information Systems Incorporated, 1996:20).

The default policy allows outside hosts to connect to an internal mail server to collect mail. The firewall itself cannot run a POP3 server, because the POP3 proxy is running on the standard POP3 port (Trusted Information Systems Incorporated, 1996:20).

3.4.3 TERMINAL SERVICES

Terminal service access to other computers can be a vital part of many network activities. The TELNET and Rlogin protocols are used for making these terminal connections, and they are not without risk. The Gauntlet™ Firewall includes proxies for both the TELNET and Rlogin protocols, which securely handle terminal services between the inside and outside networks (Trusted Information Systems Incorporated, 1996:23).

The Gauntlet™ TELNET and Rlogin proxies are application level proxies that provide configurable access control, authentication and logging mechanisms. The TELNET and Rlogin proxies, which run on the firewall, pass TELNET and Rlogin requests through the firewall, using rules the system administrator configured. According to Trusted Information Systems

Incorporated (1996:23) the proxies can be configured to allow connections based on:

- Source IP address;
- Source host name;
- Destination IP address; and
- Destination host name.

Using these options, the firewall can be configured to allow specific hosts on outside networks to connect to inside hosts or *vice versa*. The strong authentication features of the proxies allow administrators to require users to authenticate before connecting. The proxies log all successful and unsuccessful connection attempts, and the amount of data transferred. (Trusted Information Systems Incorporated, 1996:23).

TELNET and Rlogin proxies can be invoked in two ways: using a network access control daemon, or on their own. The permissions can be modified to match the security policy. Whichever way is chosen, the proxies provide the same services: passing requests through the firewall, with access control, authentication and logging (Trusted Information Systems Incorporated, 1996:24).

3.4.4 FTP SERVICES

Sometimes the easiest way to transfer information from one machine to another is to actually transfer the relevant files. The Gauntlet™ Firewall includes a proxy that securely allows the transfer of files from the outside network to the inside network as well as the transfer of files from the inside network to the outside network (Trusted Information Systems Incorporated, 1996:29).

The Gauntlet™ FTP proxy is an application level proxy that provides configurable access control, authentication and logging mechanisms. The FTP proxy, which runs on the firewall, passes FTP requests through the firewall, using rules supplied by the system administrator. According to Trusted Information Systems Incorporated (1996:29) the FTP proxy can be configured to allow file transfer activity based on:

- Source IP address;
- Source host name;
- Destination IP address;
- Destination host name; and
- FTP command (for example, STOR and RETR).

Using these options, the firewall can be configured to allow specific hosts on outside networks to transfer files to and from inside hosts. The firewall can be configured to permit users on the inside network to copy files (using the FTP daemon RETR command) from hosts on the outside network, but not place files (using the FTP daemon STOR command) on these outside hosts. The strong authentication feature of the FTP proxy allows administrators to require users to authenticate before transferring files. The FTP proxy logs all successful and unsuccessful file transfer attempts, and the number of bytes transferred. Used together, these access controls and log files allow the organisation to have much more control over the files entering and leaving their system than using the standard UNIX™ FTP programs (Trusted Information Systems Incorporated, 1996:29).

The FTP proxy can be invoked in two ways: using a network access control daemon, or on its own. The permissions and rules can be modified to match the business security policy. Whichever way the business chooses the FTP proxy provides the same services: passing requests through the firewall, with access control, authentication and logging (Trusted Information Systems Incorporated, 1996:30).

3.4.5 RSH SERVICES

Administration and support activities can be made easier if one can just execute a shell on a remote machine. The Rsh service allows users to do this. The Rsh program is not without risks: it runs programs on another machine and requires some privileges to login. The Gauntlet™ Firewall includes a proxy that securely handles the execution of Rsh requests from machines inside the network to machines outside the network (Trusted Information Systems Incorporated, 1996:35).

The Gauntlet™ *Rsh* proxy is an application level gateway that provides configurable access control, authentication and logging mechanisms. The *Rsh* proxy, which runs on the firewall, passes *Rsh* requests through the firewall, using supplied rules. According to Trusted Information Systems Incorporated (1996:35) the *Rsh* proxy can be configured to allow remote shell activity based on:

- Source IP address;
- Source host name;
- Destination IP address; and
- Destination host name.

Using these options, the firewall can be configured to allow specific hosts on the inside network to start remote shells on outside hosts. The *Rsh* proxy logs all successful and unsuccessful remote shell attempts, and the number of bytes transferred (Trusted Information Systems Incorporated, 1996:35).

In this default configuration, the UNIX™ system runs the *Rsh* proxy (*rsh-gw*) as a daemon listening for requests on the standard Rsh port. Whenever the system receives a *Rsh* request on this port, the *Rsh* proxy checks its configuration information (in the *netperm-table*) and determines whether the initiating host has permission to use *Rsh*. If the host has permission, the proxy logs the transaction and passes the request to the outside host. The *rsh-gw* remains active until either side closes the connection (Trusted Information Systems Incorporated, 1996:35).

3.4.6 WORLD WIDE WEB SERVICES

There is a vast wealth of information stored on machines connected the Internet. The graphical interfaces of browsers and web pages make it much easier to access and digest this information. WWW (World Wide Web) services allow for the transfer of a wide variety of file types and for running a number of different programs. This complexity means a greater potential for problems. These services are generic file transfer mechanisms and require logging and access control consistent with FTP and terminal services (Trusted Information Systems Incorporated, 1996:39).

The HTTP proxy included with the Gauntlet™ Firewall securely handles requests for information by way of hypertext, Gopher and file transfer (Trusted Information Systems Incorporated, 1996:39).

The HTTP proxy is an application level proxy that provides configurable access control and logging mechanisms. The HTTP proxy, which runs on the firewall, passes HTTP, SHTTP, SSL and Gopher requests as well as FTP URLs and selectors through the firewall, using supplied rules. According to Trusted Information Systems Incorporated (1996:39) the proxy can be configured to allow connections based on:

- Source IP address;
- Source host name;
- Destination IP address; and
- Destination host name.

Using these options, the firewall can be configured to allow clients on the inside network to access Gopher sites on the outside network. The system administrator can also limit the web sites that employees can access from machines on the inside network. The proxies log all successful and unsuccessful connection attempts, and the amount of data transferred (Trusted Information Systems Incorporated, 1996:39).

The HTTP proxy can be configured to allow outside hosts to access web and Gopher servers behind the firewall on inside networks. According to most security policies (including the Gauntlet™ Firewall default), this is not a good idea (Trusted Information Systems Incorporated, 1996:40).

The default configuration for HTTP requests allows all inside hosts to access any WWW sites. In this scenario, the web browser on the inside host passes a request with a URL for a particular web page to the firewall on port 80. The firewall starts the *http-gw* proxy. The proxy examines the request and determines that it is a basic request for HTTP service. The proxy checks the source and destination ports in the *netperm-table*. It then sends the request on to the web server specified in the

URL. When it receives the requested data, it passes the data back to the requesting web browser. If the request is for Gopher or FTP services (from a Web or Gopher client), the firewall still calls *http-gw* proxy and still uses the *http-gw* rules (Trusted Information Systems Incorporated, 1996:40).

3.4.7 X WINDOW SYSTEM SERVICES

The X Window System provides many features and functions that allow machines to share input and output devices. A user running the X Window System on one machine can display the results of a graphical program on another machine running an X Window client. This flexibility is also the source of a number of well-known security problems. When someone allows access to his/her display, he/she is essentially allowing access to his/her screen, mouse and keyboard. Most sites do not want to provide this sort of free access to their machines, but administrators recognise that these services can be useful. The X11 proxy included with the Gauntlet™ Firewall allows administrators to selectively allow X11 services through their firewall (Trusted Information Systems Incorporated, 1996:45).

The Gauntlet™ X11 proxy is an application level proxy that provides configurable access control. The proxy, which runs on the firewall, passes X11 display requests through the firewall, using supplied rules. According to Trusted Information Systems Incorporated (1996:45) the system administrator can configure the proxy to allow display requests based on:

- Display name; and
- User.

Using these rules, the firewall can be configured to allow only certain machines on the inside network to display information from machines on an outside network. The firewall can be configured to permit only certain users to use the X11 proxy (Trusted Information Systems Incorporated, 1996:45).

Because the X11 proxy works in conjunction with the TELNET and Rlogin proxies, access can still be configured based on the source or destination host name or IP address. The strong authentication feature is also available. The TELNET and Rlogin proxies also log X requests and connections (Trusted Information Systems Incorporated, 1996:45).

Unlike some of the other Gauntlet™ proxies, the firewall does not start the X11 proxy when it receives display requests. Instead, users must explicitly start the X11 proxy from either the TELNET or Rlogin proxy (Trusted Information Systems Incorporated, 1996:46).

The default policy is to allow both inside and outside hosts to start the X11 proxy. The firewall itself cannot run an X server because the firewall does not allow requests to the standard X port (Trusted Information Systems Incorporated, 1996:46).

3.4.8 LP SERVICES

Printing continues to be a widely used feature of most computer networks. In some circumstances, users need to print information using printers connected to other machines, on other networks. Users behind a firewall might want to print to printers on systems on the outside, or behind other firewalls. The Gauntlet™ Firewall includes an *LP* proxy that securely handles the transfer of print requests (Trusted Information Systems Incorporated, 1996:51).

The Gauntlet™ *LP* proxy is an application level gateway that provides configurable access control and logging mechanisms.

The *LP* proxy, which runs on the firewall, passes *LP* requests through the firewall, using supplied rules. According to Trusted Information Systems Incorporated (1996:51) the *LP* proxy can be configured to allow file transfer activity based on:

- Source IP address;
- Source host name;
- Destination IP address;
- Destination host name;
- *Lp* commands (for example, number and priority); and
- Printer queue.

Using these options, the firewall can be configured to allow specific hosts on the inside network to print files on outside hosts. Access to LP commands can be restricted, allowing users to print, but not allowing them to restart or remove print jobs. The *LP* proxy logs all successful and unsuccessful file transfer attempts and the number of bytes transferred (Trusted Information Systems Incorporated, 1996:51).

The default policy allows inside hosts to use *LP*. Users on inside hosts can continue to print to outside hosts as they did before the firewall was put into place. The default policy does not allow outside hosts to connect to inside hosts for printing (Trusted Information Systems Incorporated, 1996:52).

3.4.9 NNTP AND GENERAL TCP SERVICES

Usenet news continues to be one of the most widely used features on the Internet. Many sites rely on Usenet news for information on the latest technology. The Network News Transfer Protocol (NNTP) must be configured carefully to protect internal news groups that may contain sensitive proprietary information (Trusted Information Systems Incorporated, 1996:55).

The plug proxy included with the Gauntlet™ Firewall allows administrators to tunnel NNTP-based news feeds through their firewall. The NNTP connections come from known sites (as opposed to the multitude of sites that may connect by way of SMTP to deliver mail). NNTP can be proxied using the generic plug proxy (Trusted Information Systems Incorporated, 1996:55).

Allowing proprietary protocols through the firewall is risky. Because the protocols are proprietary, the firewall and the proxy have no idea what sorts of data or requests the applications are sending. The plug proxy should not be used for proprietary protocols without first performing a risk assessment (Trusted Information Systems Incorporated, 1996:55).

According to Trusted Information Systems Incorporated (1996:56) for each version of the plug proxy, the proxy can be configured to allow connections based on:

- Source IP address;
- Source host name;
- Source port;
- Destination IP address;
- Destination host name; and
- Destination port.

Using these options, the firewall can be configured to allow the service provider's host on the outside to connect to the firewall and pass news by way of NNTP to the business news machine on the inside network. The system administrator can also route all internal requests for *whois* lookups to a specific *whois* server on the outside network. The proxies log all successful and unsuccessful connection attempts, and the amount of data transferred (Trusted Information Systems Incorporated, 1996:56).

The default policy for NNTP transfer is to allow requests to and from one internal news server and one external news server. The firewall itself cannot run an NNTP news server, or any other service that is passing through the plug proxy, because the plug proxy is using the standard port for these services. The firewall is simply acting as the tunnel, by way of the plug proxy (Trusted Information Systems Incorporated, 1996:56).

3.4.10 INFORMATION SERVICES ON THE FIREWALL

Sometimes it is not feasible to run a separate WWW or Gopher server outside the business firewall. Because of hardware or other constraints, a separate machine cannot be devoted to be the WWW server. Alternatively, not enough traffic is expected to justify another machine, but the business still wants to offer WWW services to its customers. Instead, the business wants to run the WWW server securely on the firewall itself. The Info Server included with the Gauntlet™ Internet Firewall securely services requests for HTTP, Gopher and FTP services (Trusted Information Systems Incorporated, 1996:61).

The server, which runs on the firewall, works with a set of management tools to service HTTP, Gopher and FTP requests. According to Trusted Information Systems Incorporated

(1996:61) the server can be configured to allow connections based on:

- Source IP address; and
- Source host name.

The Gauntlet™ Info Server implements a minimalist design, in which the server handles only the file requests. A variety of management tools (on a per service basis) actually provides the data. (Trusted Information Systems Incorporated, 1996:61).

3.5 DISCUSSION OF GENERAL GAUNTLET™ VER. 3.1 FIREWALL SERVICES

3.5.1 LOGGING AND REPORTING

Logging is an important part of a properly configured firewall. Administrators can use the information in logs to gather usage statistics, monitor activities and investigate potential attacks. The logging features of the Gauntlet™ Internet Firewall provide administrators with a wealth of information about activities to and through the firewall. The system administrator should configure both the logging and reporting features to match the organisation's security policy (Trusted Information Systems Incorporated, 1996:89).

The components of the Gauntlet™ Firewall log a wide variety of activities and attributes, which are set out in Table 3.1 (Trusted Information Systems Incorporated, 1996:89).

Table 3.1 Attributes logged by components of a Gauntlet™ Internet Firewall

Components	**Attributes Logged**
• Firewall kernel • Proxies • Authentication management system • DNS • Sendmail	• Source IP address • Destination IP address • Source port • Destination port • User name • Session date and time • Number of bytes transferred • Individual commands (for some activities) • Successful access attempts • Unsuccessful access attempts

The proxies, kernel and authentication management system automatically write information to the logs. Even if the organisation chooses not to do anything with the information in the logs, the programs still write the information. (Trusted Information Systems Incorporated, 1996:89).

By default, the firewall keeps seven days of logs in ASCII format and the previous seven days in compressed format. It is therefore critical that all log files be checked on a regular basis (Trusted Information Systems Incorporated, 1996:90).

3.5.2 VERIFYING INTEGRITY

Even though only one account was created on the firewall for the administrator, he still wants to ensure that no person or process has modified the system. The Gauntlet™ Internet Firewall includes procedures for verifying system integrity (Trusted Information Systems Incorporated, 1996:101).

The Gauntlet™ integrity database is a collection of cryptographic checksums or message digests for most files on the file system. The database contains a checksum for each file, using information about the file size, date, userid, groupid, and mode (Trusted Information Systems Incorporated, 1996:101).

To verify the integrity of the system, a new checksum database can be created and its values can be compared with the values of the existing database. Changes in the checksums for a file indicate that someone or something has modified the file in some manner. Unless the Gauntlet™ Firewall is specifically instructed to ignore a particular item, it provides information on that item. This is a very important function to check for file modifications and should be carried out frequently by the system administrator (Trusted Information Systems Incorporated, 1996:101).

3.5.3 USER AUTHENTICATION (PASSWORDS)

The Gauntlet™ Firewall can permit or deny access based not only on host name, but also on user name. In addition, the security policy may require that users use some form of strong authentication (see 3.5.4) each time they access a particular host or service within their perimeter. To ease the integration of users, the Gauntlet™ Firewall provides a user authentication management system. The use of the authentication management system is optional. It must be used, however, any time the system administrator has configured the FTP, TELNET, Rlogin and POP3 proxies to require authentication from untrusted networks (the default for the Gauntlet™ Firewall) (Trusted Information Systems Incorporated, 1996:77).

The Gauntlet™ user authentication management system acts as a piece of "middleware" to provide a unified interface for several strong authentication systems and the Gauntlet™ Firewall (Trusted Information Systems Incorporated, 1996:77).

The various proxies use the information in the user authentication management system any time the organisation has configured the proxies to require authentication. Using the default Gauntlet™ policies, this occurs any time a user from an untrusted network tries to access a service inside the perimeter. (Trusted Information Systems Incorporated, 1996:77).

Using the default policy, the proxies do not authenticate requests from trusted networks. The proxies operate under the assumption that users coming from trusted networks are who they say they are (Trusted Information Systems Incorporated, 1996:78).

3.5.3.1 REUSABLE PASSWORDS

This system, a part of the user authentication system included with the Gauntlet™ Firewall, has a reusable password option. It is designed for administrator testing only. Every time a user needs to authenticate he/she uses the same password. The use of reusable passwords should be avoided at all cost (Trusted Information Systems Incorporated, 1996:81).

3.5.4 MAKING USE OF USERS, GROUPS AND ADMINISTRATORS

3.5.4.1 USERS

User names created in the user authentication management system are used only for strong authentication. The user names must match the user names for the strong authentication system the organisation is using. By default, no user accounts are created on the firewall. The exception to this rule is the *login-sh* authentication wrapper program (Trusted Information Systems Incorporated, 1996:78).

The user names in the user authentication management system do not need to match any user names on the internal network. The system administrator may wish to use the same names for the convenience of the users (Trusted Information Systems Incorporated, 1996:78).

3.5.4.2 GROUPS

The Gauntlet™ user authentication management system also makes use of groups. Groups allow the organisation to permit or deny services based on groups of user names, rather than individual user names. (Trusted Information Systems Incorporated, 1996:79).

Just as is the case with user names, the groups created in the Gauntlet™ user authentication management system are not necessarily the same as the groups created on the firewall. The same names can, of course, be used for easier administration (Trusted Information Systems Incorporated, 1996:79).

3.5.4.3 ADMINISTRATORS

Global administrators can create both groups and users. Initially, root is the only global administrator. Creating another global administrator is part of the configuration process for the user authentication system. Within each group, group administrators who can create and modify users only within their own group, can be designated (Trusted Information Systems Incorporated, 1996:79).

3.6 CONCLUSION

The references in this chapter seem to be voluminous, but they are necessary to enable the achievement of the objectives of the literature survey.

Some references relate indirectly to the objectives, but they are necessary to understand and appreciate the scope of security features available in Gauntlet™ ver. 3.1

In the writer's opinion, the objectives of the literature survey have been achieved. No further security areas, that have not been specifically excluded, should be exposed with more reading.

Having completed the literature study and analysis of the security features of Gauntlet™ ver. 3.1 in this chapter, the results will be now be disclosed in the form of a matrix in chapter 4.

CHAPTER 4: GAUNTLET™ VER. 3.1 DECISION MATRIX FOR THE INDEPENDENT AUDITOR

The configuration settings (attributes) that influence security for Gauntlet™ ver. 3.1 services, as well as general services, to obtain maximum security in the firewall, are presented as a matrix in this chapter. This chapter is presented under the following headings:

4.1 INTRODUCTION

The objective of this chapter is to provide the independent auditor with a matrix for use in his assessment (from a security point of view) of a Gauntlet™ Internet Firewall.

4.2 DECISION MATRIX FOR GAUNTLET™ VER. 3.1

This matrix, set out as Table 4.1, was developed using the detailed literature study in Chapter 3 as a basis. The matrix is set out in four columns. The details of these columns (starting from the left) are as follows:

- Column one depicts the Gauntlet™ service, the corresponding proxy that Gauntlet™ uses to process the request as well as a reference to the literature study in Chapter 3 where this service is discussed in detail.
- Column two discloses the attribute(s) to be used for each service disclosed in column one.
- Column three explains the syntax of the attributes disclosed in column two.

- Column four contains general comments on the attribute(s) and the service.

The section of the matrix dealing with general services (subsection 11) is divided into 3 columns:

- Column one discloses the name of the service (in this case, general).
- Column two contains the description of the general service as well as the text reference in Chapter three.
- Column three contains a discussion of the general service as it pertains to security in the Firewall.

Table 4.1 Gauntlet™ services, corresponding proxies, text references, attributes and syntax of attributes.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
1. SMTP *smap* and *smapd* Paragraph 3.6.1	a) *badadmin*	badadmin *user* *user* is the name of a user or an alias	This attribute specifies the username to which the *smapd* server forwards mail it cannot deliver. The system administrator should, on a regular basis, investigate the reason for undelivered mail.
	b) *baddir*	baddir *directory* *directory* is the name of a directory on the same device as the spool directory	This attribute specifies the directory in which the *smapd* server places any spooled mail it cannot deliver normally. The system administrator should, on a regular basis, investigate the reason for undelivered mail.
	c) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when either one of the proxies is running.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
2. POP3 *pop3-gw* Paragraph 3.6.2	a) *authenticate*	authenticate * (wildcard) Anybody and everybody accessing this proxy must authenticate	Users must always authenticate.
	b) *authserver*	authserver *host* *host* is IP address or host name	This attribute specifies the host running the authorisation server that the proxy uses for authenticating users.
	c) *destination*	[permit|deny]-destination *destination-list* *destination-list* specifies single hosts, entire networks or subnets specified by IP address or hostname	Only destination host(s) to which the proxies and applications are allowed to send requests, should be "permitted" by way of this attribute.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
2. POP3 (continued)	d) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.
Note that inside workstations should not be allowed to exchange mail with POP3 servers outside the perimeter. The mail server should be behind the firewall on the inside network. All POP3 clients on the inside network can collect their mail from this server.	e) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
3. TERMINAL SERVICES *rlogin-gw and tn-gw* Paragraph 3.6.3	a) *authenticate*	authenticate * (wildcard) Anybody and everybody accessing this proxy must authenticate	Users must always authenticate.
	b) *authserver*	authserver *host* *host* is IP address or host name	This attribute specifies the host running the authorisation server that the proxy uses for authenticating users.
	c) *destination*	[permit|deny]-destination *destination-list* *destination-list* specifies single hosts, entire networks or subnets specified by IP address or host name	Only destination host(s) to which the proxies and applications are allowed to send requests, should be “permitted” by way of this attribute.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
3. TERMINAL SERVICES (continued)	d) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.
	e) *password change*	[*permit* |*deny*]-password change *permit* | *deny* indicates hosts from which users can/ cannot change their passwords.	It is preferable not to use this attribute but rather have someone change his/her password by some other secure way (for example in an encrypted file).

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
3. TERMINAL SERVICES (continued)	f) *timeout*	timeout *seconds* *seconds* specifies the number of seconds the proxy is idle before disconnecting.	A value of 60 seconds should be adequate.
	g) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
4. FTP *ftp-gw* Paragraph 3.6.4	a) *authenticate*	authenticate * (wildcard) Anybody and everybody accessing this proxy must authenticate	Users must always authenticate.
	b) *authserver*	authserver *host* *host* is IP address or host name	This attribute specifies the host running the authorisation server that the proxy uses for authenticating users.
	c) *destination*	[permit|deny]-destination *destination-list* *destination-list* specifies single hosts, entire networks or subnets specified by IP address or host name	Only destination host(s) to which the proxies and applications are allowed to send requests, should be “permitted” by way of this attribute.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
4. FTP (continued)	d) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.
	e) *timeout*	timeout *seconds* *seconds* specifies the number of seconds the proxy is idle before disconnecting.	A value of 60 seconds should be adequate.
	f) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
5. RSH SERVICES *rsh-gw* Paragraph 3.6.5	a) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.
	b) *timeout*	timeout *seconds* *seconds* specifies the number of seconds the proxy is idle before disconnecting.	A value of 60 seconds should be adequate.
	c) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
5. RSH SERVICES (continued)	d) *destination*	[permit|deny]-destination *destination-list* *destination-list* specifies single hosts, entire networks or subnets specified by IP address or host name	Only destination host(s) to which the proxies and applications are allowed to send requests, should be "permitted" by way of this attribute.
6. GOPHER AND WWW http-gw Paragraph 3.6.6	a) *destination*	[permit|deny]-destination *destination-list* *destination-list* specifies single hosts, entire networks or subnets specified by IP address or host name	Only destination host(s) to which the proxies and applications are allowed to send requests, should be "permitted" by way of this attribute.
	b) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
6. GOPHER AND WWW (continued)	c) *timeout*	timeout *seconds* *seconds* specifies the number of seconds the proxy is idle before disconnecting.	A value of 60 seconds should be adequate.
	d) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.
7. X WINDOWS x-gw Paragraph 3.6.7	a) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
7. X WINDOWS (continued)	b) *display*	display *host* : *displaynumber.screennumber* *host* specifies the name of the machine to which the display is physically connected. *displaynumber* is the number of the display on the machine *screennumber* is the number of the screen for the display	This attribute identifies the destination display on which applications display when running this proxy.
	c) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.
	d) *timeout*	timeout *seconds* *seconds* specifies the number of seconds the proxy is idle before disconnecting.	A value of 60 seconds should be adequate.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
8. LP SERVICES lp-gw Paragraph 3.6.8	a) *destination*	[permit|deny]-destination *destination-list* *destination-list* specifies single hosts, entire networks or subnets specified by IP address or host name	Only destination host(s) to which the proxies and applications are allowed to send requests, should be "permitted" by way of this attribute.
	b) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.
	c) *timeout*	timeout *seconds* *seconds* specifies the number of seconds the proxy is idle before disconnecting.	A value of 60 seconds should be adequate.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
8. LP SERVICES (continued)	d) *client*	client *clients* -printer *queue* [[-deny | -log] [{*lpcommands*} | all]] *clients* - Specifies single hosts, entire networks, or subnets. Specify by IP address or host name. The wildcard * is valid. *queue* - specifies the name of the printer queue to which this rule applies. *lpcommands* - specifies the lp commands the clients can issue when sending jobs through the proxy.	The *client* attribute must be used to identify the user when running the "lp-gw" proxy.
	e) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
9. NNTP AND TCP plug-gw Paragraph 3.6.9	a) *destination*	[permit|deny]-destination *destination-list* *destination-list* specifies single hosts, entire networks or subnets specified by IP address or hostname	Only destination host(s) to which the proxies and applications are allowed to send requests, should be "permitted" by way of this attribute.
	b) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.
	c) *timeout*	timeout *seconds* *seconds* specifies the number of seconds the proxy is idle before disconnecting.	A value of 60 seconds should be adequate.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
9. NNTP AND TCP (continued)	d) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.
10. INFORMATION SERVICES info -gw Paragraph 3.6.10	a) *userid*	userid *user* Where *user* is specified as either a name or numeric id from the */etc/passwd* file	This attribute identifies the user when the proxy is running.
	b) *timeout*	timeout *seconds* *seconds* specifies the number of seconds the proxy is idle before disconnecting.	A value of 60 seconds should be adequate.

GAUNTLET™ SERVICE, NAME OF PROXY AND TEXT REFERENCE	ATTRIBUTE(S) TO BE USED	SYNTAX	COMMENT(S)
10. INFORMATION SERVICES (continued)	c) *hosts*	permit-hosts *hosts* -policy *policy* **or** deny-hosts *hosts* *hosts* specifies the hosts for which the proxy uses the particular policy. *policy* specifies the name of the policy.	This attribute specifies the hosts for which the proxy uses a particular policy or the hosts that can use the proxy.
	d) *destination*	[permit|deny]-destination *destination-list* *destination-list* specifies single hosts, entire networks or subnets specified by IP address or host name	Only destination host(s) to which the proxies and applications are allowed to send requests, should be "permitted" by way of this attribute.

GAUNTLET™ SERVICE	DESCRIPTION AND TEXT REFERENCE	COMMENT(S)
11. GENERAL	a) Logging and reporting Paragraph 3.7.1	Logging and reporting is an extremely important feature of the Gauntlet™ Internet Firewall. The proxies, kernel and authentication management system automatically write information to the logs. All logs and reports are created by default. The logging feature should **not** be disabled. Gauntlet™ retains the logs for fourteen days. The system administrator should print out the logs say, every week, scan them, follow up on problems and file them for future reference and proof of action taken, if needed.
	b) Verifying integrity Paragraph 3.7.2	After the Gauntlet™ has been initially configured, the system administrator needs to create an integrity database. This program calls a shell script that runs a scan program that walks the directory tree and creates message digest checksums for each file. The scan program writes the checksums to the integrity database. If the checksum differs from that of a previous scan, it is probable that the firewall has been compromised. The system administrator should run this scan program at least once a week to determine if somebody has made changes to the system.

<u>GAUNTLET™ SERVICE</u>	<u>DESCRIPTION AND TEXT REFERENCE</u>	<u>COMMENT(S)</u>
11. GENERAL (continued)	c) User authentication Paragraph 3.7.3	Use of the authentication management system is optional. It must be used, however, at any time when the FTP, TELNET, Rlogin and POP3 proxies were configured to require authentication from untrusted networks (the default for the Gauntlet™ Firewall). **From a security point of view, authentication must be used at all times, regardless of circumstances.** The various proxies use the information in the user authentication management system any time the proxies are configured to require authentication (which they must be). Using the default policy, the proxies do not authenticate requests from trusted networks. The proxies operate under the assumption that users coming from trusted networks are who they say they are. This is a dangerous policy as a criminal may log in from a trusted network outside the organisation and he/she will not be required to authenticate. Therefore it is a good policy not to have any trusted networks (set-up in Gauntlet™) outside the organisation and thereby have everybody's requests authenticated. **DO NOT** use the reusable passwords option for authentication. **DO NOT** use the reusable password option for the firewall administrator account. Reusable passwords are vulnerable to password sniffers and are easy to crack. This feature is provided for convenience and audit capability only.

4.3 CONCLUSION

A matrix for use by the independent auditor was developed in chapter 4.2. This matrix reflects in a concise way the available Gauntlet™ Internet Firewall services, the corresponding attributes, the syntax for the attributes, as well as general comments for the guidance of the independent auditor.

This matrix should serve as an enhancement to audit procedures. Its main purpose is to guide the independent auditor in his assessment of the effectiveness (from a security point of view) of a Gauntlet™ Internet Firewall. A secondary purpose of this matrix is to inform the independent auditor on the available security functions in Gauntlet™ ver. 3.1, when a client requests advice during the implementation of a Gauntlet™ Internet Firewall.

CHAPTER 5: CONCLUSION

The objective of this short dissertation has been met; that is to help the independent auditor to assess the effectiveness (in terms of security) of a Gauntlet™ Internet Firewall.

The main problem identified was the fact that a Gauntlet™ Firewall is not by default secure. It has to be configured and managed efficiently in order to utilise its security functions optimally.

The matrix developed in Chapter 4 should serve as an enhancement to effective auditing procedures; its aim is to assist the auditor in assessing the effectiveness of a Gauntlet™ Internet Firewall in protecting an organisation's resources and, what is more important, its data. Client service (where auditors also give business advice and not only do the compliance audit for a client), which has recently become more important to auditors, can be maximised by using this matrix. An example of this is where the auditor is approached by a client to advise on data security issues when the client plans to acquire and implement a Gauntlet™ Internet Firewall.

It therefore opens new fields for academic research in the area of the impact on desired audit objectives by security features in an Internet Firewall environment, such as the design and testing of specific audit procedures for the audit of an Internet Firewall.

BIBLIOGRAPHY

ARENS, AA & LOEBBECKE, JK 1988: Auditing - an integrated approach. New Jersey: Prentice-Hall.

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

CHESWICK, WR & BELLOVIN, SM 1994: Firewalls and Internet security – repelling the wily hacker. Reading, MA: Addison-Wesley.

SIYAN, K & HARE, C 1995: Internet firewalls and network security. Indianapolis, Indiana: New Riders Publishing.

STANG, DJ 1993: Network security secrets. California: IDG Books Worldwide, Inc.

TRUSTED INFORMATION SYSTEMS INCORPORATED 1996: Gauntlet Internet firewall administrators guide – version 3.1. Rockville, MD: Trusted Information Systems Incorporated.