Graphica Software
160 Queen St
5th Floor
Melbourne, 3000
Victoria, Australia.
e-mail: sales@melb.graphica.com.au

A Scalable, Secure Internet Solution

Document: secinet.doc
Issue No: Draft
Printed: 02/01/98 11:11

Table of Contents

1. Preface 3

2. Related Documents 3

3. Changes History 3

4. Introduction 3

5. Secure Connection 4

5.1 Router Hardware Options 4

5.2 BSD Application Firewall Hardware 5

6. Firewall Proxies and Services 7

6.1 Application Proxies 7

6.2 Domain Name Service 7

6.3 E-Mail 8

7. The Intranet 8

7.1 IBM Server/Windows NT Hub 8

8. The Perimeter Network 9

9. Complete Solutions 10

10. Hardware Policy and Warranties 10

11. APPENDIX A: Definitions and Acronyms 11

List of Figures

Figure 1. Basic Internet Connectivity 3
Figure 2. Perimeter network setup 6
Figure 3. Firewall DNS Service Configuration. 8

List of Tables

Table 1. 2210 Nways router costing. 4
Table 2. Basic BSD 4.4 Firewall Cost 5
Table 3. BSD Firewall 4.4 Options 5
Table 4. Firewall Application Proxy Services. 7
Table 5. Intranet Solution 9
Table 6. Complete Solution Network Hardware/Software Costs 10

1. Preface

The following document gives an overwive of the network setup, and costing for a scalable, secure internet connectivity solution for corporate networks.

2. Related Documents

[1] IBM 2210 Nways Multiprotocol Router Summary Sheet.
[2] IBM 325 Server PC Summary Sheet
[3] IBM 350 PC Summary Sheet
[2] Firewalls and Ineternet Security by Cheswick & Bellovin
[3] Building Internet Firewalls by Chapman & Zwicky
[4] TIS Firewall Toolkit "http://www.tis.com"
[5] SOCK5 "http://www.socks.nec.com"
[6] Intetnetworking with TCP/IP Vol.1 by D.Comer

3. Changes History

Version 1.0	Monday, 19 August 1996	Graphica Software Pty. Ltd.

4. Introduction

The Graphica Software Internet connectively solution relies on premium quality network hardware combined with proven, configurable software that allows your organisation to to utilizse the Internet securely. The solution allows you to choose both the TCP/IP based services required as well as the connection bandwidth required. For international or national organization the basic configuration is replicated in each addition site.

The following basic units are used to provide a secure and scalable connection.

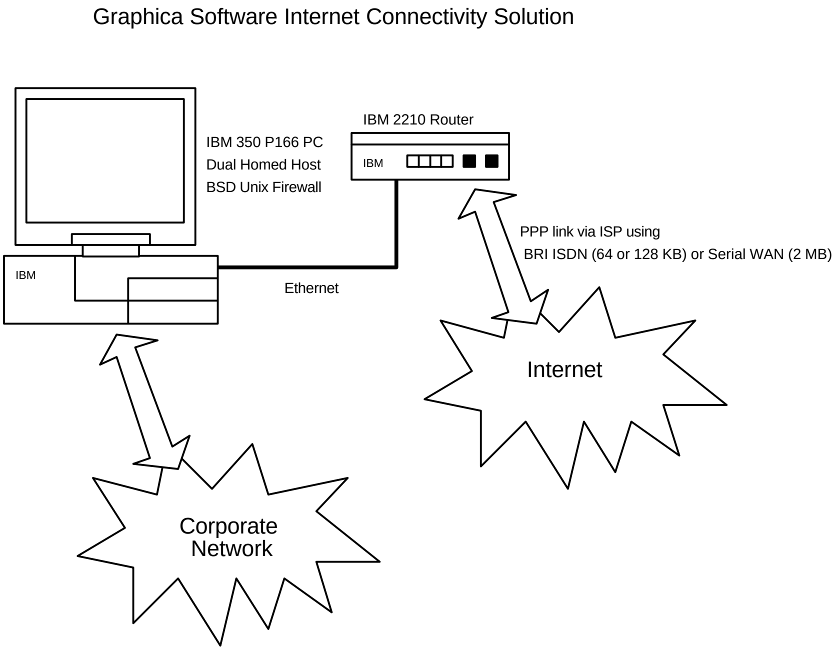

Figure 1. Basic Internet Connectivity

The basic connection solution provides the choose of either a lower bandwidth 64KB ISDN line or up to 2 MB dedicated line. Both options use Point-to-Point Protocol (PPP) via an internet service provider (ISP). The flexiblity of this solution is that the router allows you to initially choose an ISDN connection using a single or dual 64 KB channels with the option of moving to a HDLC leased line based connection, without requiring any further expenditure on network hardware. This flexiblity is provided at a cost well below that of a CISCO router based configurations.

To provide connections to your corporate network a dual homed application level firewall is used. This provides a degree of flexibility and security that is not possible using only the filtering facilities provided by the router. The firewall is build around a FreeBSD 4.4 BSD Unix operating system kernel which has been specially build to disable IP packet forwarding, remove all spurious network and driver code and run a minimal set of known and trusted services. The firwall works on the basis that any network access that is not explicitly allowed is denied and hence provides a very high degree of security and control. No non-administrative access is available on the the firewall ie one user account for login and root account for installation are the only useable accounts.

The user then has the option of adding to this basic configuration, to provide both back end facilities for use within the corporate network or Internet accessible services, within the perimeter network.

The rest of this document provides the details on options, setup and configuration for your corporate Internet connection.

5. Secure Connection

5.1 Router Hardware Options

As outlined in the introduction the basic units for connecting to the internet consists of an IBM 22210 Nway router and an IBM 350 P166 PC with specially configured BSD 4.4 Unix kernel.

Router	Memory	Protocols	Ethernet	Serial	ISDN BRI	Cost (inc Tex)
2210 Nways S4K	2 MB Flash 4 MB DRAM	IP (IPX optional)	1	1	1	$
2210 Nways S8K	4MB Flash 8 MB DRAM	IP + DLSw (IPX + DecNet + AppleTalk optional)	1	1	1	$

Table 1. 2210 Nways router costing.

The basic configuration consists of an IBM 2210 Nways S4K IP router. This gives the user the option to use either the ISDN BRI interface or a high speed serial WAN link. The selection of which interface to use is software configurable. Initial configuration is performed using the units RS-232 serial port, subsequest configuraiton is possible using any of Telnet, SNMP or provided Windows configuration application.

The choose of either the S4K or S8K model can be made, based on expected traffic patterns or the requirement to route additional protocols, asides from IP. For most installations S4K option should be more than adequate. For a central site which expects heavy traffic, is expected to be routing further subnets and is using an HDLC connection, the S8K model should be considered.

The Ethernet LAN connection is via 10BaseT, using crossover cable direct to Firewall PC network interface card. Cost includes one of either serial connection cable or ISDN S/T interface cable with RJ-45 connector. Subsequent shift from ISDN to serial WAN connection will require additional cable.

The ISDN BRI consists of two 64 kps “B” channels for data and one 16 kps “D” channel for signalling. The connection can be configured for multi-homed or aggregated ISDN connection options that gives a total of 128 kps.

5.2 BSD Application Firewall Hardware

While the router provides connection to the Internet, it does not provide the degree of security required between your corporate network and the Internet. This is done by using an application level Firewall gateway. The Firewall is considered application level because it has specially configured application level proxies (ie FTP, WWW, Telnet etc) which are responsible for managing and authenticating all access between the corporate network and the Internet.

PC	Processor	Periperals	Memory	Network	Cost (inc tax)
IBM PC 350 14” Monitor Keyboard Mouse	Pentium 166	Adaptec 2940 SCSI 2 GB Fast SCSI HD SCSI CD-ROM 2 GB SCSI QIC Tape	512 KB Cache 80 MB EDO RAM	2 3COM PCI 10/100 10BaseT	

Table 2. Basic BSD 4.4 Firewall Cost

The Firewall hardware setup uses the most stable and tested platform available. The combination of standard IBM PC hardware with Adaptec 2940 SCSI based peripherials and 3COM network cards provides the most widely tested and utilized operating platform. Large disk and high memory configurations are utilized to allow for WWW caching, and to support large number of concurrent connections. The following options are available for the Firewall BSD system, to allow for heavily loaded networks and an extra perimeter network for the purpose of running public WWW and/or FTP servers.

Options	Reason	Cost (inc tax)
Extra 64 MB	Heavy WWW usage, in combination WWW cache configuration	$
Pentium P200	Heavily loaded network	$
Initial configuration	To custom configure the Firewall software proxies and services as documented in Section 6.	$

Table 3. BSD Firewall 4.4 Options

The configuration quoted includes installation of FreeBSD 4.4 Unix OS and network proxies ready for configuration and network implementation, included is a day zero tape backup of system. To further enhance security the system compiler is delivered in an encrypted form, which renders it unusable in the event of a firewall security breach.

Should the organisation wish to run a public WWW service or FTP service the system should be configured as shown in the following diagram.

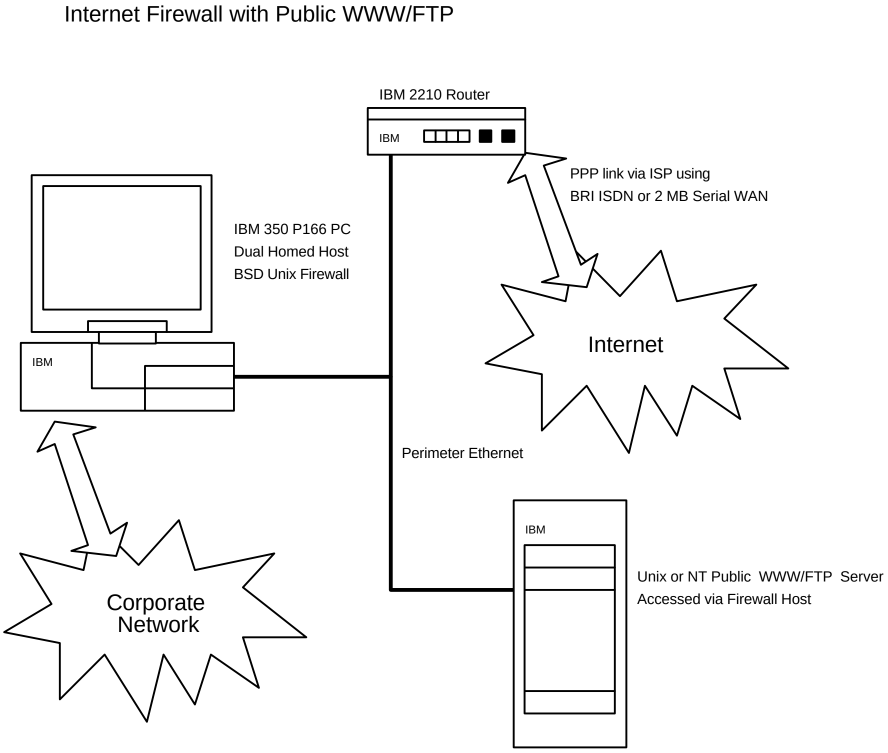

Figure 2. Perimeter network setup

By placing the public WWW/FTP services on the guarded perimeter network, it is possible to provide service access to Internet users, with jepordizing internal network security. Access to services on the perimeter network is acheived via the Firewall. This is enforced by configuration of 2210 Nways router filtering options to allow external access to the Firewall IP address only.

Setup of the perimeter network services can be provided by Graphica Software as part of a total solution, or the client can opt to configure their own solution. The standard solution provided by Graphica Software Pty. Ltd. consists of an IBM PC Server coupled with Microsoft Winodws NT version 4.0 with Microsoft Internet Information Server.

6. Firewall Proxies and Services

6.1 Application Proxies

The following application proxies are used on the firewall, to provide access to the Internet from the corporate network. It is possible to configure proxies to provide generic access or particular access based on IP addresses.

Service	Proxy	Configuration	Comments
WWW	Squid Object Cache	squid.conf	Caching WWW proxy, which provides for much more efficent use of network bandwidth, by using a centralized memory and hard disk based HTML/FTP object caching, coupled with a heirachical network of parent and child proxies.
FTP	TIS ftp-gw TIS acl	net-perm.table inetd.conf	FTP access to firewall is configured via special TCP/IP port address, to allow for software installation.
SMTP	TIS smap/smapd	net-parm.table inetd.conf	A wrapper for SMTP sendmail program. This ensures that no direct access to the sendmail is possible.
NNTP	TIS plug-gw	netparm.table inetd.conf	This is configurable to provide Network News (UseNet) access
Telnet	TIS tn-gw	net-parm.table inetd.conf	Telnet access to the Firewall will be required for administration. Root telnet access is not allowed. It is recommended to allow only internal telnet access to the firewall from particular workstations with others getting the outbound telnet access proxy.
X-Windows	TIS x-gw	net-parm.conf inetd.conf	Is is strongy recommended not to allow X-11 access as it is inherently insecure.
Generic	SOCSK5	socks5.conf	A generic proxing service which has been accepted as an IETF standard (RFC 1928). To use socks reqiures modification of the client application. For windows application a special purposes winsock modification wrapper is available which allows use of socks without client program modification. This proxy is useful for NNTP to external servers or IRC access.

Table 4. Firewall Application Proxy Services.

6.2 Domain Name Service

In addition to running a selectable set of application proxies the Firewall will also run a Domain Name Service (DNS) which will act as the primary authorative host for the network. The only externally DNS visible hosts are those connected to the perimeter network. As the only directly connected hosts are on the perimeter this means that all IP addresses within the corparate network should adopt the non-connected IP addressing scheme as outlined in RFC 1597. As the router is guaranteed not to forward IP address using the RFC 1597 IP addressing, this makes IP mascerading attacks on the Firewall host by external network users impossible. The Firewall DNS is configured in combination with an internal network DNS service as shown in the following diagram.

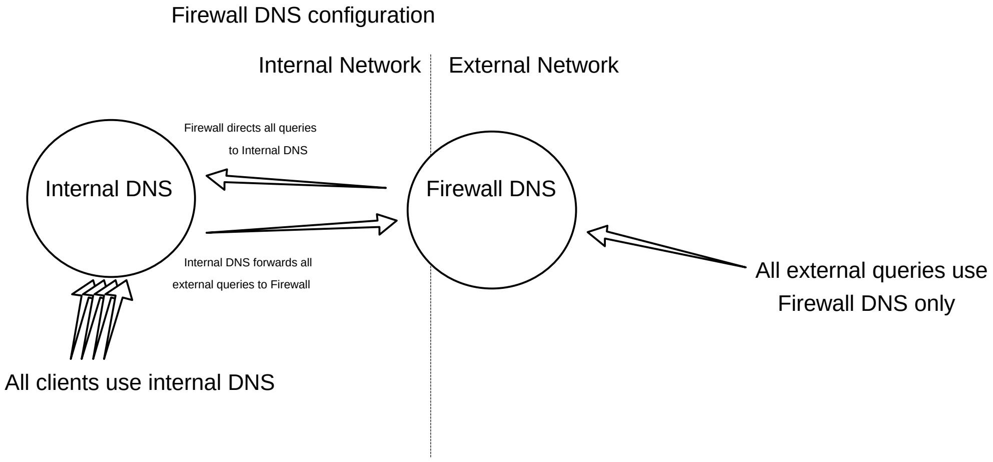
Firewall DNS configuration
Internal Network
External Network
Firewall directs all queries to Internal DNS
Internal DNS
Firewall DNS
Internal DNS forwards all external queries to Firewall
All external queries use Firewall DNS only
All clients use internal DNS

Figure 3. Firewall DNS Service Configuration.

Firewall DNS configuration includes setup for Firewall and Perimeter host DNS lookup as well as IN_ADDR reverse IP lookup, as well as Mail Exchange configuration MX records.

For clients who do not currently have allocated IP address or Domain Name there is an extra cost to cover the appliation for IP address and Domain name registration.

6.3 E-Mail

The Firewall host is configured with a Simple Mail Transport Protocol (SMTP) compatible proxy. This allows for universal SMTP mail forwarding and receipt. The Firewall mail configuration includes Sendmail configuration for forwarding of all inboound mail to internal mail hubs. Internal mail hub can be any SMTP compatable service. Once mail has arrived at the internal mail hub client delivery can by either via preferred third party mail system ie Microsoft Exchange, CCMail or via POP/POP3 (Post Office Protocol) compatible mail clients. A POP mail service is not provided on the Firewall host as this would require setup of user accounts on the Firewall host which would breach the Firewall security. Sendmail configuration includes setup of standard mail and system administration aliases such as “postmaster”, “root”, “admin” and “hostmaster”.

It should be noted that neither internal nor extenal clients have direct access to Sendmail which is a notorious for its security problems. Also by using a “standard” forwarding sendmail configuration there is not need for incomprehensible Sendmail setup on the Firewall.

The system configuration for BSD Unix includes automatic mailing of security and disk usage audit reports. By configuring of the mail alias appropriately, these can be forwarded to your internal mail hub for receipt by your system administrator.

7. The Intranet

7.1 IBM Server/Windows NT Hub

Having established a secure connection to the Internet, the client will require an Intranet to provide mail, domain name services and other internal services. The customer is free to install and configure their own internal network configuration, for which we can provide the required configuration assistance to allow intergration with the Internet Firewall.

Should the client wish to setup an easy managed and configurable Intranet then we provide a solution that utilalizes IBM PC Server’s with Windows NT Server 4.0 installed. This solution integrates extremely well into a heterogenous network consisting of Windows PCs, Unix Workstations and Apple MacIntosh workstations.

The basic supplied Internet hub consist of the following items, note the client can choose to scale this system with increased client licence or more highly configured server options.

Item	Provides	No	Cost (inc Tax)
IBM PC Server 325 + 15” Monitor	IBM PC Server 325 266MHZ Pentium II 4.5 GB Ultra SCSI HD SCSI CD-ROM 32 MB ECC RAM 10/100BaseT Ethernet	1	
MS Windows NT Server 4.0	DHCP WINS DNS IIS	10 Client	
MS Exchange Server	MS-Mail SMTP Gateway POP3 Client Pickup NNTP Service	100 Client	

Table 5. Intranet Solution

The Windows NT 4.0 Server platform runs the Dynamic Host Configuration Protocol (DHCP), Windows Internet Name Service (WINS) and the Domain Name Service (DNS) these service work in collution to releave the system administration staff of one of the most tedious tasks of TCP/IP network administration, that of IP number allocation and DNS configuration. The NT DNS service is configured to forward all external domain requests to the Firewall DNS.

The client can choose to run the Microsoft Internet Information Service (IIS) to provide internal WWW pages as well as provide an envionment for the development of HTML pages for publication on an external network host (either on the perimeter network or hosted by an ISP).

The Microsoft Exchange Server is used to provide group-ware, mail and news services. This gives a number of options for user mail agent chooses, including using MS Mail Client, MS Exchange Client and POP/POP3 based clients. The Firewall is configured to forward mail to the MS Exchange Server. The exchange server is also able to support the Network News Transport Protocol (NNTP) which provides access to the store/forward UseNet news service. Like mail NNTP works on a store and forward basis and so does not impose a high security risk. The Firewall is configured to forward NNTP to the internal MS Exchange Server.

8. The Perimeter Network

The final part of a comprehensive totally in house Internet solution is to support your own WWW/FTP publishing service. This is only a worthwhile exercise for ISDN connected networks. The throughput of 33.6 /56 kps modems is not sufficent to make this a usable options. If you have choosen to use a low speed modem connection, then we strongly recommend that you uses an ISP to host your WWW service.

If you choose to run a WWW service then it is simply a matter of installing a further IBM Server PC running Windows NT Server 4.0 and Microsoft IIS. The server contents can be developed using the Intranet server and then shifted to the perimeter network via the Firewall using Microsoft FrontPages site copy facility.

Alternatively the client can choose to run a Unix WWW server. In both case’s the Firewall and Router must be configured appropriately to include filter options, DNS entrys for the host and the appropriate proxy services setup.

9. Complete Solutions

The following table shows the total cost of providing a hardware and software secure internet connection solution. The client can choose to start with an entry level mail system which can then be scaled to provide an Acess solution at no extra cost in network hardware, by upgrading the connection method.

Option	Connection	Includes	Cost (inc Tax)
“Mail” SMTP NNTP FTP (get slow) WWW (get slow)	ISDN	2210 Router S4K 350 PC BSD Firewall Configuration	$ 0000.00 $ 0000.00 $ 000.00 $ 000.00 $ 0000.00
“Mail/Intranet” Mail + Intranet	ISDN	Mail + 325 Server Windows NT Server 4.0 MS-Exchange	$ 0000.00 $ 0000.00 $ 0000.00 $ 0000.00 $ 000.00 $ 00000.00
“Access” Mail + FTP (get fast) WWW (get fast)	ISDN 64/128 or WAN	As per Mail	$ 0000.00
“Access/Intranet” Mail/Intranet + FTP (get fast) WWW (get fast)	ISDN 64/128 or WAN	As per Mail/Intranet	$ 00000.00
“Publish/Intranet” Access/Intranet + FTP (put fast) WWW (put fast)	ISDN 64/128 or WAN	2210 Router S8K 350 PC BSD Firewall 64 MB RAM P200 Configuration 2 * 325 Server 2 * Windows NT Server 4.0 MS-Exchange	$ 0000.00 $ 0000.00 $ 000.00 $ 000.00 $000.00 $ 00000.00 $ 0000.00 $ 0000.00 $ 00000.00

Table 6. Complete Solution Network Hardware/Software Costs

10. Hardware Policy and Warranties

All the internet connection solutions documented here relie on highest quality components. All critical computer and router hardware are from IBM. Graphica Software chooses to supply IBM based solutions because they provide highest quality equipment coupled with efficent onsite service support, which is particularly important for critical network components.

All IBM equipment is covered by at least 3 year parts/labour warranty with 1 year onsite. All IBM PC Server models are covered by 3 year parts/labour on site warranty.

IBM PC 350 PC Firewall is equiped with Adaptec PCI SCSI controller, IBM HD, NEC CD-ROM, Tandberg Data QIC Tape Drive and 3COM Network cards. All the peripherical equipment is covered by a 3 year warrenty.

11. APPENDIX A: Definitions and Acronyms

TCP/IP - Transmission Control Protocol / Internetworking Protocol - The protocol of the Internet
NNTP
SMTP
POP

End of Document