Global Information Assurance Certification Paper

COST EFFECTIVE FIREWALLING USING LINUX TECHNOLOGY IN SMALL BUSINESSES.

Steve Lang
April 14, 2003

Introduction

In New Zealand, most businesses employ only few staff**.** One of the constraints of small businesses is the cost of adequate network protection. With the relatively recent introduction of broadband Internet access (ADSL), the lack of experience with dedicated Internet connections and the high cost of enterprise level firewalls, network security in many small businesses is less than adequate.

Whilst in recent years there has been significant reduction in the size and cost of commercial firewalls, there has also been an increase in the usability and functionality of Linux based firewalls. The differences between the two is narrowing. In this paper, I will consider some modern Linux based firewalls that are available and the main differences between them then take a recent release of one Linux based firewall, detail the design, implementation that could be used to increase a typical small business' security with minimal cost.

Background

There are many reasons that influence small business spending on security. In my experience, four of the main ones in New Zealand are:

1. Business size - the average business size is very small by international standards. A report [i] from the Ministry of Economic Development highlights the fact that New Zealand is predominantly a nation of small firms. 86.9% of enterprises employ 5 or less full time staff, 97.3% of enterprises employ 19 of fewer staff and 99% employ 49 or fewer staff. The average size of a New Zealand firm is 5.9 Full Time Equivalent employees.[ii] By international standards, this could be considered very low.

2. Cost of technology - the local currency (NZ$) is relatively weak (NZ $1.00 = US$0.55) compared with the US$ with which many technology based products are priced. Many firewalls are aimed at the enterprise level market of US companies. This is significantly larger than than a typical New Zealand company, and will provide more functionality and greater performance than what would be required. A firewall appliance for the US market that might cost US$3,000 becomes considerably less affordable to the majority of small businesses in New Zealand at over NZ$5,400 before additional installation costs. This is more than many businesses can easily justify. Only in recent years have firewall manufacturers released products that fill smaller areas (SOHO – Small Office Home Office) in the market.

3. Cost of infrastructure – the size of population (3.9 million), the low density of population (spread over 268,000 square kilometers), the distance from other similar countries and cultures (Australia, United Kingdom, America) contributes to the high cost of telecommunications and Internet services.

   The relative low density of population adds another layer of difficulty in delivering

network service to businesses. While larger cities have much greater densities of population, even these aren't especially high when compared with large cities in the United States and the European Union. This has had a direct influence on the cost of data circuits.

In addition to this, the preferred peering point for Internet connections is the United States which is very far away, and the underlying telecommunications infrastructure (sub-oceanic fiber optic cable) is quite expensive to deploy. Simply put, a conventional terrestrial 2Mb/s metropolitan connection to the Internet is not affordable to the average business, even in the most densely populated areas of the country.

4. Education and awareness – there is a general lack of awareness about security, risk and the cost or consequences of security breaches. Many of the large overseas security incidents are not reported in the popular press, with the exception of the very large scale virus/worms/trojans (e.g. Melissa, Code Red).

   This has left in depth understanding of the issues surrounding security and the implications on a business to the IT staff (if they exist), or a general mis-belief that if you have a virus scanner installed, you have all of your bases covered.

   There have been very few publicised local security incidents of a nature that may apply to or effect the average business.

Approximately 4 years ago, Telecom New Zealand (who hold an effective monopoly on the 'last mile') started to roll out ADSL services to business and residential customers. Whilst the pricing of these services is arguably high when compared to other countries, they are often more affordable to small businesses than the historical Frame Relay or high speed Leased Line Digital Data Services services.

The uptake of ADSL services is increasing as more equipment is installed to enable these services in new areas, and more people become aware of the advantages of using the Internet in their business. More people are being exposed to the increased threat that a permanent connection to the Internet can bring.

A Common Broadband Installation

One of the requirements for an ADSL connection, is an ADSL modem/router. The model that was supplied by Telecom New Zealand was typically a Nokia M1122. This is an external ADSL modem that provides network level functionality (by connecting to your internal PC's by Ethernet) including NAT, and 'pinholing', a type of port-forwarding that allows you to make internal servers available to the Internet.

For quite some time (prior to alternative hardware being type-approved for network connection or accepted in the market place) the architecture shown in Illustration 1 was typically being deployed into may businesses. By default, there may not have been any external services made available, but the facility to do this was there and the configuration user interface (which was via. http) made it easy for people to add this functionality, sometimes without understanding the consequences.

One drawback of this design, is the lack of security that is provided by the ADSL router. The devices often deployed were designed to perform the function of ADSL connection and routing. They were not designed as firewalls, and their ability to perform firewalling

functions is limited. They may support some multi-stream protocols (FTP for example) but they lack generic stateful packet inspection for all communications that pass through the router.

Another common configuration is that the username/password of these routers is set the same across all installations. This means that anyone that knows the password and has local access to the internal network can either telnet (or use http) to the ADSL router, and make configuration changes, including the ability to open up port forwarding, thus exposing internal machines to the Internet. In many cases, the internal server (Outlook Web Access for example) is also performing other functions like file and print sharing and exposing just one service to the Internet can compromise many other services.

With the 'always on' nature of these ADSL connections, there is a significantly increased opportunity for people on the Internet to analyse these systems and find vulnerabilities. with the tools that are available on the Internet. These vulnerabilities can easily be identified and therefore the risk to a business can increase significantly because of the use of a permanently connected broadband Internet connection.

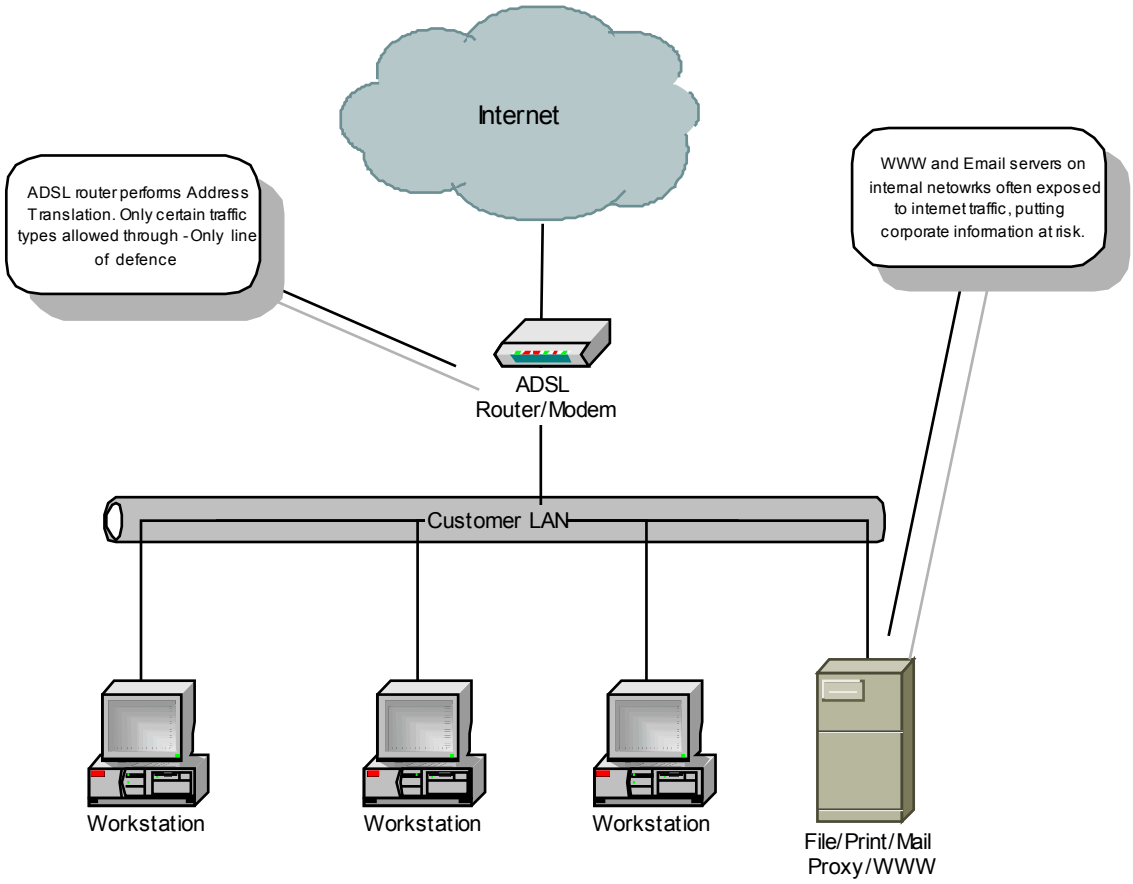

Illustration 1: A typical broadband installation

Linux Based Firewalls

Linux based firewalls have evolved a lot within the last few years. Originally, there were a few distributions that were designed to perform this type of function, but they were generally difficult to install, difficult to manage and often lacked the sophisticated functionality that is common amongst commercial firewall appliances.

This is starting to change. With the release of the 2.4 Linux Kernels, the capability to do stateful packet inspection was introduced in the core operating system across many Linux distributions. Netfilter and iptables [iii] are the framework that enables stateful packet inspection, amongst other benefits over and above previous Linux kernel versions (which only supported basic non-stateful packet filtering.)

Many standard Linux distributions can be used to create a firewall using iptables, but these can be hard to configure, take a long time to install, and be difficult to administer. They are also quite far removed from small firewall appliance that an enterprise might seek to deploy. This makes it difficult for a small business to implement such a solution.

In the last couple of years, there have been advances in some Linux distributions that are aimed at providing this type of functionality. Here, we will consider some common iptables based firewall solutions that are still under active development.

LRP/LEAF

Many years ago, the very first Linux firewall that I attempted to install was called LRP, short for Linux Router Project[iv] and based on the Eigerstein release. There were many branches of development based on LRP, but they share some common traits:

- Fits on a floppy disk
- Originally based on kernel version 2.0.36, but later on kernel 2.2.x
- Will work on very low-end hardware, typically 386's.

There are many derivatives of LRP, but they don't generally compare with the more modern firewall based distributions in terms of ease of installation and use, functionality, maintainability or documentation and have been superseded with LEAF.

LEAF [v] (Linux Embedded Appliance Firewall) was setup to create an environment for the developers of the LRP so that they can release their modifications and updates to the public. It brings together a lot of information about the various branches that have forked off from the original LRP. One primary goal of this project is to create a new LEAF version based on the 2.4 Linux kernel that will therefore have iptables (stateful) packet inspection.

Bering [vi] is a LEAF distribution that includes the 2.4 Linux kernel and stateful packet inspection. The configuration of Bering is by editing configuration files and text based configuration utilities. There is also an option for creating a bootable CD-ROM version of Bering. Additional modules available include a Web based monitoring tool, shorewall firewall scripts and there are also instructions for configuring Bering as a wireless firewall and to terminate IPSec connections.

Devil-Linux

Devil-Linux[vii] is a customised Linux distribution which is designed to be used for Routers and Firewalls. It is secure, small and customisable. It runs from a boot CD, so can contain more functionality than LRP/LEAF firewalls, and has the advantage that if there is less risk of the firewall itself being tampered with. A simple reboot should guarantee that the firewall will be reset back to a known state. It stores it's configuration on a floppy disk which can normally be left read-only, which also helps prevent unauthorised tampering of the firewall configuration.

It's CPU requirements are quite low (486 or greater) but due to the run from CD nature

(and therefore the fact that it relies on RAM disks) it requires 64MB+ of RAM. It is based on version 2.4 Linux kernel and has support for iptables and therefore stateful packet inspection. The basic network and system configuration is done by editing the Linux configuration files.

One interesting feature of Devil-Linux is that it is supported by Firewall Builder [viii]. Firewall Builder provides a GUI for creating and managing firewall rules in a similar way to some enterprise level firewall management systems. This runs on a Linux host with XWindows installed, so therefore does not run on the firewall itself. The Firewall rule policy is compiled into iptables rules, and then uploaded to the Devil-Linux firewall. This provides for very effective firewall rule generation, and ease of use, but does require an additional Linux workstation with XWindows and the Firewall Builder software installed.

Gibraltar

Two versions of the gibralter firewall [ix] are planned for release. A free version and a commercial version. The main difference between the two is the user interface. The free version is configured using the command line, and editing tools (e.g. vi) as you would configure the native software packages on a Linux workstation/server without any GUI. The commercial version will have a http based GUI, as well as email relaying (with virus scanning) and transparent HTTP/HTTPS (also with virus scanning). The commercial version is yet to be released.

It shares a couple of common features with devil-Linux. It boots/runs from CD-ROM and stores it's configuration on a floppy disk which can normally be left read-only, and is based on the Linux 2.4 kernel thus supporting iptables stateful packet inspection.

It too can support more functionality than the LRP/LEAF firewalls, but requires a 486DX2/ 66 with 32MB RAM (or better, depending on configured functionality). It has full support for many Ethernet interfaces as well as 802.11b Wireless LAN support, supports many routing protocols, Quality of Service VPN termination and more.

SmoothWall

SmoothWall[x] currently have several versions available.

- SmoothWall GPL 1.0 (free)
- SmoothWall GPL 2.0 beta (currently beta4 - free)
- SmoothWall Corporate Server 2.0 (commercial)

SmoothWall Corporate Server 2.0 is based on Linux kernel 2.2.22. It requires a hard disk (using the ext3 file system to minimise problems) to install on, and runs without keyboard/ monitor/mouse (ie. headless.) It requires a Pentium class processor with 32MB (preferably 64MB) or RAM. There are some additional modules that are available for SmoothWall Corporate Server 2.0, and there is commercial support for the product. These appear to be the biggest difference between the commercial and free versions.

SmoothWall 1.0 free, and also based on Linux kernel 2.2 (in this case 2.2.19) with similar hardware requirements as Corporate Server 2.0. Being based on the earlier kernel (2.2.19) and therefore ipchains, this version doesn't support stateful packet inspection.

SmoothWall 2.0 (beta4) is based on Linux kernel 2.4.19, with support for iptables, uses the ext3 file system (for greater reliability) and has greater support for USB ADSL modems. The hardware requirements are similar to SmoothWall 1.0.

IPCop

There are currently two versions of IPCop[xi] available:
- IPCop 1.2.0 (free)
- IPCop 1.3beta (currently beta4 - free)

IPCop 1.2.0 is based on the Linux kernel 2.2, and supports ipchains, hence it doesn't support stateful packet inspection. It was forked from SmoothWall GPL 0.9.9 so shares much in common with SmoothWall 1.0 GPL, including a very similar user interface and features.

It installs onto a hard disk, and uses the ext3 file system, will work on 486 level processors and above with 16+MB of RAM (depending on features selected). There is a slightly modified version of IPCop 1.2.0 that comes pre-installed on a Compact Flash card (available from LinITX.com) and Traverse Technologies (www.traverse.com.au) sell appliance type hardware systems with the option of IPCop 1.2.0 pre-installed.

IPCop 1.3beta4 has recently been released. This has largely the same feature set as 1.2.0, but is based on Linux kernel 2.4, and now supports iptables and stateful packet inspection. There is better graphing of network interface traffic, and enhanced support for Road Warrior VPN connections.

IPCop 1.3 (beta) – a closer look.
The most significant recent development with IPCop (as with the other firewalls mentioned here) has been the introduction of iptables and stateful packet inspection. This enhances the security capabilities, and provides a framework for future enhancements.

IPCop1.3beta3 provides a http user interface which makes it easy to configure and manage the firewall. The model that is used is that of a three zones, RED – untrusted (the Internet), ORANGE – dmz (partially trusted, internally and externally reachable servers) and GREEN – trusted (the internal network.)

By default, it is possible for any computer on the GREEN network to establish a connection to either of the lower security zones (ORANGE and RED.) Similarly, it is possible for any computer on ORANGE to establish a connection to any computer on RED. The return traffic is allowed through the firewall as the creation of the outbound connections places information in the state table that permits the replies.

By default, it is not possible for any computer in the RED network to establish a connection to a computer in the GREEN or ORANGE networks, nor for any computer in the ORANGE network to establish a connection to a computer in the GREEN network, unless it is specifically configured to be allowed.

The external interface doesn't have to be an Ethernet interface. IPCop 1.3beta supports having a dialup (modem) interface as the RED (external) interface. In the case of ADSL connections which may be treated similar to dialup, this connection may consist of:
1) Ethernet to an ADSL router that is performing NAT
2) pppoe (ppp over Ethernet) to an ADSL router that is forwarding the ppp session to the firewall
3) pptp (point to point tunneling protocol) to an ADSL router that is forwarding the ppp session to the firewall.

For option 1, the ADSL router can act as an additional line of defense, and only forward through connections that are specifically configured to the firewall, or any return traffic

from internally initiated connections. As most ADSL routers (the M1122 included) doesn't have very large support for complicated multi-stream protocols, it may have to be configured to forward almost all traffic through to the firewall. This will reduce it's effectiveness as an extra level of defence from external attack.

In options 2 and 3 above, the ppp connection from the ISP ADSL equipment is terminating on the firewall. This has the advantage that the firewall has the IP Address assigned by the ISP, and can therefore see all incoming traffic allowing it to log and analyse a greater level of detail. This does however have the disadvantage that there is only one line of defense from the Internet to the internal network.

Whether you configure IPCop to connect to the router using pptp/pppoe (options #2 and #3) or use conventional NAT (option #1) will depend on:
1) Business communication requirements – if all that an organisation requires is outbound http and Email, then the ADSL router functionality becomes less important.
2) Make/model of ADSL router – some don't support pppoe/pptp
3) Support for protocols – e.g. some don't support protocols like IPSec, or GRE

As well as standard support three network interface, there is also support for the following services that are available with IPCop1.3beta:
- DNS Proxy – enables more efficient name resolution for internal workstations
- DHCP – allows for both static and dynamic leases
- Intrusion Detection (snort)
- Web Proxy (squid)
- VPN (freeswan) – either between site, or site – mobile workstation
- Web Server (GUI management)
- ssh (command line management)
- Logging

Statistics like Disk Usage, Memory Usage, Enabled Services are readily available from the http user interface, as are the number of connections, traffic graphs (implemented using mrtg and ipac_ng - Illustration 2).

In order to increase the efficiency of some networks, IPCop 1.3beta provides the facility to cache web traffic (using squid), and proxy DNS requests. It also has the ability to terminate 3DES ipsec connections, and can be used to terminate VPN connections from remote computers, including Windows PC's over dialup.

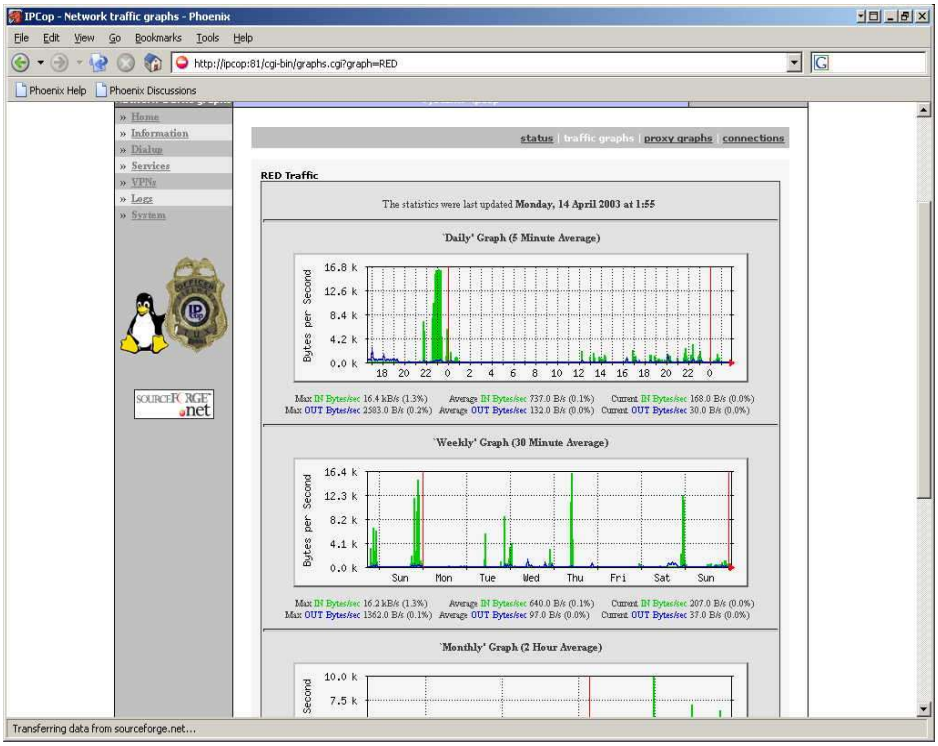

Illustration 2: MRTG graphs of RED interface traffic

Any packets that are dropped and logged, are available using the http user interface (Illustration 3), can be selected and then automatically cross-referenced against Internet whois databases to find the origin, and other useful information (Illustration 4).

Illustration 3: Log output of packets dropped by the firewall

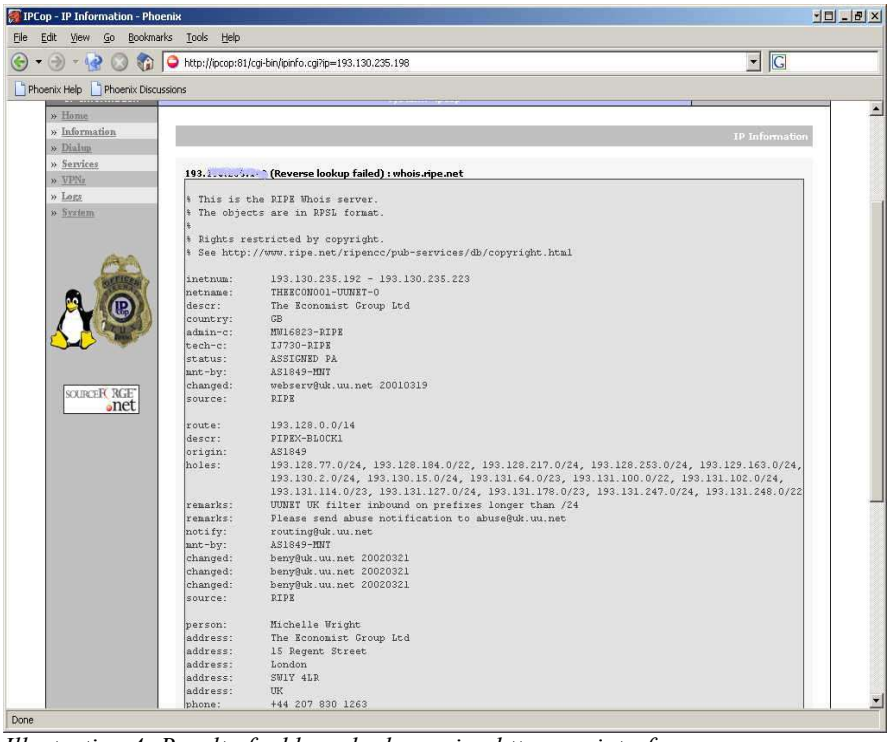

Illustration 4: Result of address lookup using http user interface

The firewall policy editor allows the specification of which firewall ports should be accessible from the outside, as well as which connections should be forwarded (Illustration 5) from RED to either the ORANGE, or GREEN networks. There is a separate configuration that allows for forwarding from ORANGE to GREEN networks called 'dmz pinholes'.

The lack of a configuration option to limit what traffic is allowed out of the GREEN or ORANGE networks is a significant drawback with IPCop (and many similar firewall

Illustration 5: firewall port forwarding configuration

packages). Code Red would not have been able to spread as fast as it did if web servers (that would normally only receive connections) were prevented from being able to initiate connections out to the Internet.

There are currently several enhancements that are being worked on to IPCop[xii]:

- Qos: One of the more significant include QoS. This would provide the facility to be able to enforce certain levels of Quality of Service on traffic as it passes through the firewall.
- Sophisticated firewall rule configuration – shorewall [xiii]. This could also be done by integrating a totally external firewall rule generation mechanism similar to how Devil-Linux can be configured using Firewall Builder. This would allow for restricting the outbound connections to the internet, something that even small businesses should have the capability to do.

A New Broadband Installation

The facilities provided by firewalls such as IPCop are far greater than the common ADSL router. There are significant benefits from utilising this type of technology in addition to the existing infrastructure that is already deployed in many organisations. Illustration 6 shows an modified broadband installation from the first one.

Here, we still have the ADSL router that is managing the connection to the ISP. It performs NAT functions, and will only allow traffic into the network that is a reply of something that went out, or that is specifically configured to be allowed. If there are many complicated traffic types that are required to be used over these connections, then the requirement may be to have all traffic forwarded to the internal firewall. This is less than ideal, and reduces the overall security of the system.

The internal interface of the ADSL router is connected to the external (RED) interface of the IPCop firewall, which is acting as a second line of defense. At this point, we have great control of the type of traffic that we allow through, and also we have the facility to log, report (graph) that traffic. As this type of firewall also supports putting services into a DMZ, even more benefits can be gained by placing externally visible services in a DMZ, instead of making them visible while they are still on the internal network.

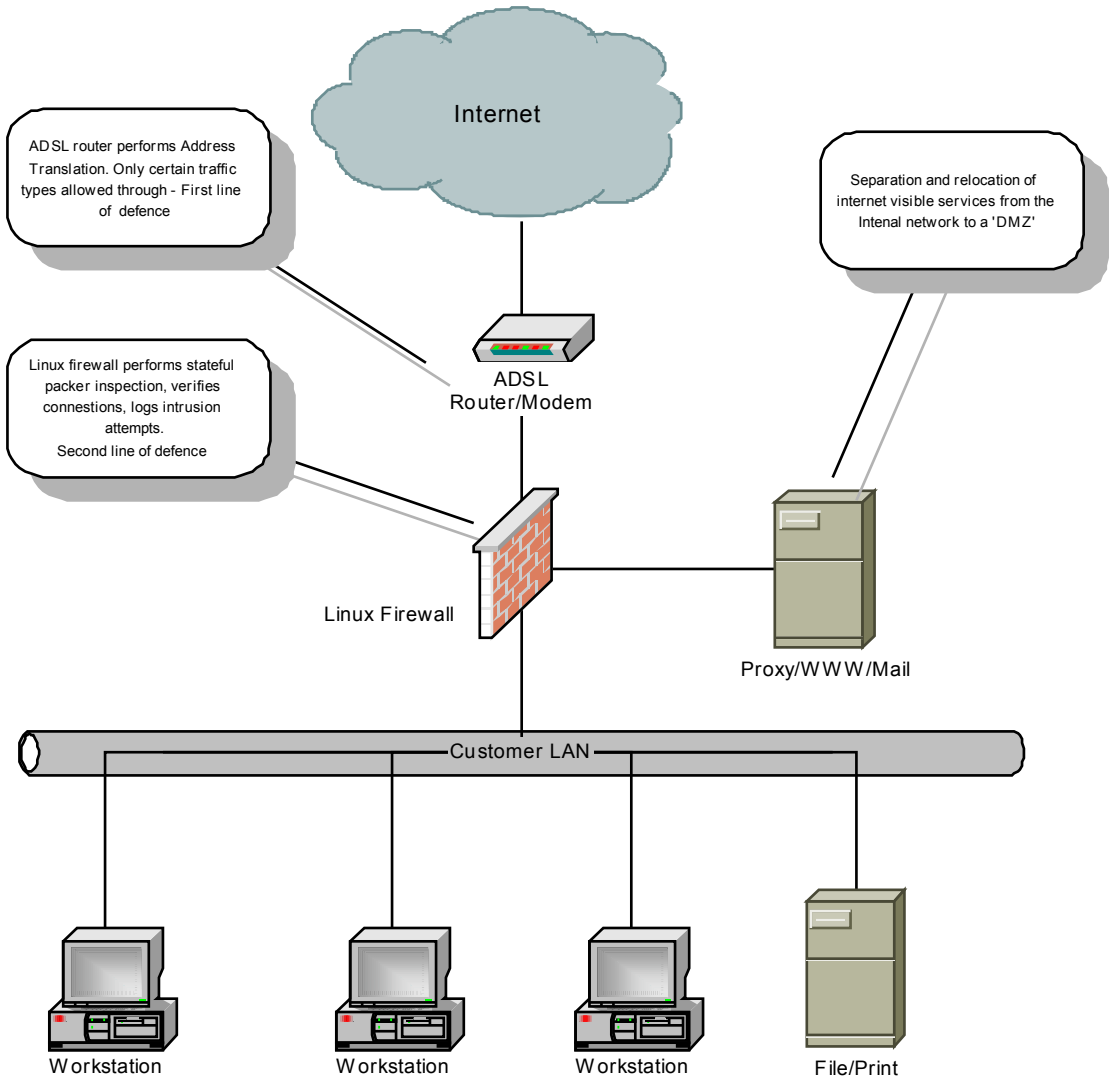

Illustration 6: An alternative broadband installation

Conclusions

The advantages gained by this type of configuration are significant. The addition of a firewall (whose software component is free) utilising existing or old hardware enhances the security of small businesses by providing an additional layer of sophisticated security policy enforcement (defense in depth) and additional functionality (e.g. Intrusion Detection, IPSec VPN termination). It also provides the capability of splitting off services from internal servers, and placing them into a DMZ where they can be accessed by both internal and external computers.

On top of this, recent Linux firewall packages are easy to install, provide for sophisticated http management and logging, and can be installed on appliance type hardware without any moving parts (where you can install the system on Compact Flash for example).

All 4 Linux based firewalls are suitable for integration into a small network. The latest versions all share the ability to implement stateful packet inspection, and although they may not perform as well as commercial enterprise firewalls and lack some functionality,

they are very cost-effective and can improve the level of security in many small businesses.

The facilities that are provided by these firewall systems approaches, and in some cases (with a DMZ interface and the ability to terminate 3DES IPSec vpn's) surpasses that of the low-end commercial firewall appliances, for less cost.

In the future, as these Linux based technologies improve to include facilities to control bandwidth (Quality of Service), Wireless Access Networks and to easily limit the outbound connections as well as the inbound, then the application of customised Linux based firewall solutions will be very compelling for many businesses, not just small enterprises.

i Ministry of Economic Development “SME's in New Zealand: Structure and Dynamics”. June 2002. URL: http://www.med.govt.nz/irdev/ind_dev/smes2002/smes2002-04.html#TopOfPage (14 Apr. 2003)
ii Ministry of Economic Development “SME's in New Zealand: Structure and Dynamics”. Figure 4: Average FTE's per Enterprise. June 2002. URL: http://www.med.govt.nz/irdev/ind_dev/smes2002/smes2002-05.html#P292_934 (14 Apr. 2003)
iii “netfilter – firewalling, NAT and packet mangling for Linux 2.4” URL: http://www.netfilter.org/ (14 Apr. 2003)
iv “Linux Router Project “ URL: http://www.linuxrouter.org/ (14 Apr. 2003)
v “LEAF: Linux Embedded Appliance Firewall” URL: http://leaf.sourceforge.net/ (14 Apr. 2003)
vi “LEAF: Bering “ URL: http://leaf.sourceforge.net/mod.php?mod=userpage&menu=904&page_id=21(14 Apr. 2003)
vii “Devil-Linux” URL: http://www.devil-linux.org/ (14 Apr. 2003)
viii “Firewall Builder” URL: http://www.fwbuilder.org/ (14 Apr. 2003)
ix “Gibralter firewall solution” URL: http://www.gibraltar.at/index.php?product_gibraltar_overview_eng (14 Apr. 2003)
x “SmoothWall” URL: http://www.smoothwall.org/ (14 Apr. 2003)
xi “IPCop Firewall” URL: http://www.ipcop.org/ (14 Apr. 2003)
xii “IPCop developers mail list “ (14 Apr. 2003)
xiii “Shorewall 1.4 'iptables made easy'” URL: http://www.shorewall.net/ (14 Apr. 2003)