Linix Firewall Security for the Small Office and Home Office

Ralph Durkee
Independent Consultant
Sponsored by Linux Users Group of Rochester
rd@rd1.net
www.rd1.net

Road Map

- What is a firewall and why do I need it?
- Policies, auditing and monitoring.
- Firewall techniques and architecture including routers, filters, proxies and NAT.
- Recommended tools and approach for building a Linux Firewall

What Is a Firewall

- In building architecture a firewall is a division of the normal continuity.
- Divides so as to limit losses in the event of a fire.
- Very limited openings and passages.
- Openings are controlled and have special mechanisms for the sake of protection.
- These principles apply to the network firewall as well.

Is a Firewall Really Necessary?

- **Yes!** Unless your have nothing of value and no concern for liability.
- Risks of attack from the outside are increasing exponentially.
- Probes for weaknesses are a daily occurrence for most externally visible system.
- Using a high-speed internet connection without a firewall will lead to an incident.

Is a Firewall All That's Needed?

- **No!** Firewall architecture is one key piece of the bigger picture.
- Policies, auditing and monitoring are also very necessary.
- As well as virus protection, and host security.
- Simple intrusion detection is good to have but not required for the small office.

Virus (Worm) Protection

- Install Virus Scanning Software.
- Subject Line? Who cares? Can't depend on it.
- It's the attachment that bites!
- Look at the last characters after the last dot.
- For Example ILOVEYOU.TXT.vbs
- It's the vbs that indicates it's a program!
- If you see an extension you don't recognize, don't open it.

A Dangerous Strain of E-mail Virus

- Security hole in IE5 and MS Office 2000
- Allows for a virus to be spread without opening the attachment.
- Doesn't require IE5 or MS Office to be running, if installed, the system is vulnerable.
- More information and a link to the MS Patch is available at **www.sans.org**

Firewall Building Blocks and Techniques

- There's a full spectrum of possible architectures.
- We will first examine the building blocks used.
  - Routers and IP filters.
  - Network Address Translation (NAT).
  - Application proxies.
  - Single and dual homed systems.
  - Logs and monitors.
- After introducing each of these we will examine their security role.

Routers

- Bridges traffic between local area networks
- Directs traffic at the intersections of the internet.
- Generally used along with an IP Filter

IP Filters

- Provides rules for filtering out unwanted internet traffic
- Most every router includes IP filtering
- Many hosts (computer systems) include or will support IP filtering software.
- Very flexible, often a bit complex.
- Most require a good understanding of basic TCP/IP.

Network Address Translation (NAT)

- NAT server acts as a proxy at the **TCP network level** for internal clients.
- Relays request to the internet and responses to the clients.
- Provides sharing of one or more public internet address.

Application Proxy

- Application proxy server acts as a proxy at the **application level** for internal clients.
- Also relays requests to the internet and responses to the clients.
- Specific server software for each application (web sever, news, mail, FTP server).
- Provides sharing of one or more IP address.

Single and Dual Homed System

- A dual homed system is one with two network interface cards.
- The dual homed system has one interface to the internal network and a second to the external network.
- A third interface can be added for connectivity to the DMZ. (Tri-homed system).
- DMZ (demilitarized zone) may contain publicly accessible servers such as a web server or mail server.
- DMZ with public servers is not recommended for SOHO, use an ISP instead.

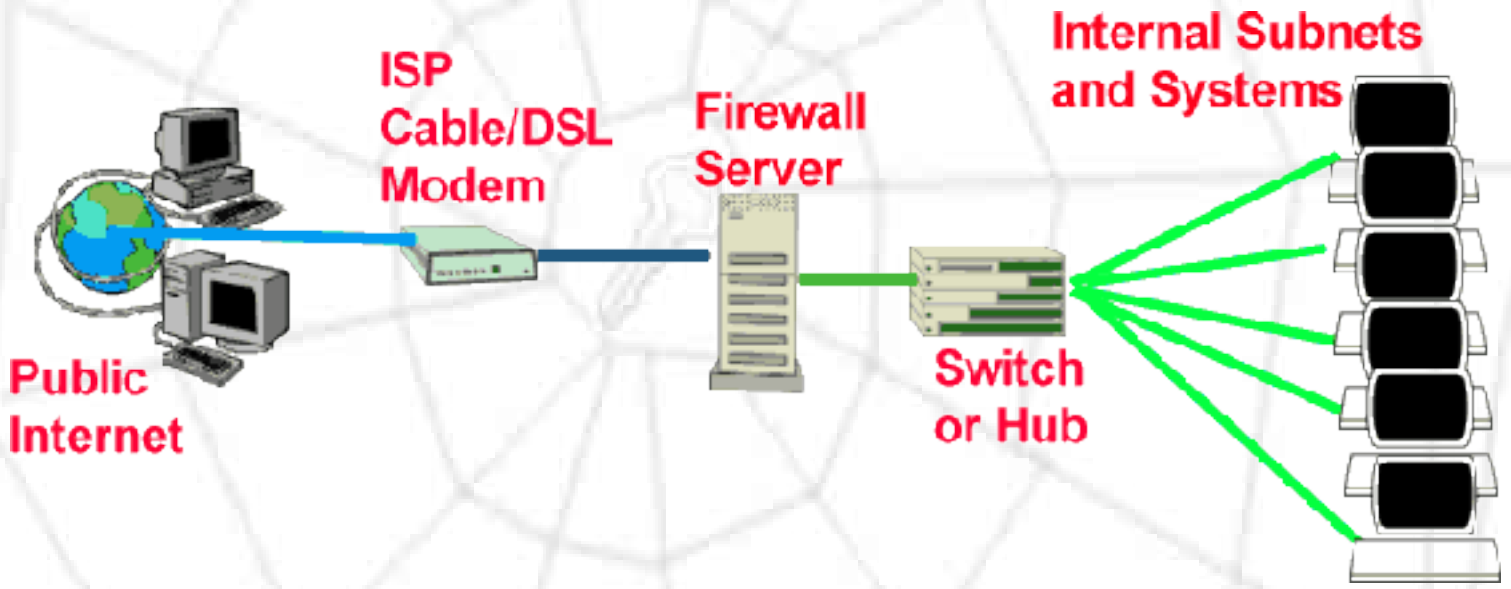
External Router and IP Filter

- Some form of an external router is already present in your cable or DSL modem which provides your access to the internet.
- It may have very limited filtering, but not enough to protect your network.
- You generally don't have control of the filtering rules on it even though you may own it.
- Most ISP's will not even tell customers what filtering features it may or may not have.

Recommended Architectures

- Must haves:
  - Configuration control of IP filtering and routing rules
  - Dual home interface
  - Network (NAT) or application level proxy
  - Usage and alert monitor capability
  - Periodic audits
  - Regular monitoring

Simple Architecture



Why Dual Home Interface

- Distinguishes between internal and external traffic by the separate physical network interfaces
- Single homed distinguishes traffic according to the source address.
- Prevents IP spoofing.
- An inside source address may be spoofed to look as if it were coming from the inside even though it's from the internet.

Application Proxy vs. NAT

- Application Proxy Firewall (APFW) chooses a few limited services as opening through the firewall, such as Web, Mail and File Transfer.
- NAT allows all TCP traffic and uses IP Filtering to limit the traffic.
- In theory the NAT can be made as secure as the Application Proxy with sufficient filter rules.
- Secure NAT filtering is a bit more complex.
- Recent TCP Stealth scanning tricks when first invented penetrated many NAT firewalls.

Application Proxy vs. NAT (continued)

- APFW allows greater authentication control, such as requiring users to authenticate with the Proxy Web Server.
- APFW more intelligent application level monitoring and logging.
- Web Proxy also allows easy hooks into content filtering services to limit liability.
- APFW and NAT can be combined for a hybrid architecture.

Simple Linux Firewall

- Network Concierge sells a Linux Software
- Very Simple to install and configure!
- Can be configured as a firewall or a internal server.
- www.NC4U.com
- 10$ shipping and Handling for 15 day eval.
- 99$ to activate

Installing NC4U Linux as a Firewall

- Setup PC with 2 Network Interface Cards
- Pentium PC with 32 Mb RAM, 1Gig HD
- Insert CD in a MS Windows system.
- Make a NC4U Linux boot floppy
- Boot Firewall PC from floppy.
- Configure via Web browser on MS Win System.

Custom Linux Firewall

- (Not simple, need to have Linux experience).
- Install 2 network interface cards.
- Install Linux.
- Rh6.2 or mandrake 6.0-1 for Bastille-Linux.
- Set the cable/DSL modem IP to be the default router.
- Turn-off IP forwarding (ifconfig private).
- Make sure routed is **not** running.

Bastille Linux

- Download Bastille-Linux hardening script.
- http://www.bastille-linux.org/
- Read the FAQ and instructions carefully.
- Run script.
- Skip the Apache hardening. (Doesn't work yet)
- Check your results carefully.
- Disclaimer: your mileage may vary.

Apache As a Proxy

- Use www.apache.org to understand the directives.
- Directives specific to a proxy firewall.

```
Listen 192.168.0.100:8080
# Port 80 (No, use the listen instead )
LoadModule proxy_module       lib…
AddModule mod_proxy.c
```

Apache Proxy Authentication

```
<IfModule mod_proxy.c>
ProxyRequests On
<Directory proxy:*>
    Order deny,allow
    Deny from all
    Allow from 192.168.0        (Substitute your Private Net ID here)
        AuthType Basic
        AuthName "RD1 Proxy"
        AuthUserFile /etc/apache/.htpasswd
        require valid_user
</Directory>
```

Resources

- Bastile Linux http://www.bastille-linux.org/
- Securing Linux (Info Security Magazine)
- http://www.infosecuritymag.com/feb2000/Linux.htm
- http://www.apache.org
- Linux Rookery / Sys Admin Mag
- http://www.sysadminmag.com/linux/masq/index.shtml
- Lugor of course! http://www.lugor.org/
- Or send me E-mail rd@rd1.net www.rd1.net

Summary

- For business, recommend professional planning, installation and monitoring.
- Such as: RD1.Net, QwicNet.Com ISS.Net and others).
- Can be affordable: 200$/month and up for small business.
- Continue to audit and monitor your firewall once it's in place.
- Security requires regular administration.
- Limit the external services.