# CUCUG

# Internet Firewalls

# Presentation

# Internet Firewalls

- **What is a ‘firewall’?**

  A firewall either permits or denies network traffic to pass based on a set of rules.

  A firewall is a software program you run on your computer or a separate piece of hardware.

- **Why firewalls are a good idea**

  A firewall can protect your networked computer and data from unauthorized access, use, or damage via the network.

  Firewalls are two-way. A firewall can also control what your networked computer can access via its Internet connection.

# Types of Firewalls: Software

A software firewall is simply a program that is loaded on your computer. It intercepts all incoming and outgoing network connections.

- **Advantages**

  Simple to install.

- **Disadvantages**

  The software program is specific to your computer, its operating system, and the version of the OS.

  If you have more than one networked computer, a software firewall must be purchased and loaded onto each one.

  The software firewall consumes disk, memory, and CPU resources on your computer.

  Relies on both the operating system and the program to not have any security holes.

# Types of Firewalls: Hardware

A hardware firewall is a dedicated piece of hardware that physically sits between your internet connection and your computer or private network.

- **Advantages**

  Can provide additional services such as routing, NAT, and many others.

  Requires no changes to your computer other than network settings. No need to worry about having problems when installing new operating systems or upgrading version, configuring new software or hardware, or viruses or other malicious software disabling or bypassing the firewall.

  Doesn't interfere with sharing resources (files, printers, etc.) on a private network.

  You computer isn't vulnerable no matter how many security bugs Bill and Steve come up with.

- **Disadvantages**

  Requires space and power aside from the networked computer.

# Hardware Firewalls

- **Commercial**

  Netgear's RT311 and RT314 are good examples of a dedicated hardware firewall for home users. They are cheap ($80 & $130) as well as easy to install.

  They come with customer support and can be configured via a web browser.

- **Making your own**

  There are several, good UNIX-based operating systems that provide a large array of networking services including firewall protection and are free. They require a cheap computer and some computer knowledge to configure and use.

# Making Your Own Firewall: Software

- **Operating System**

  For operating systems, there's FreeBSD, OpenBSD, NetBSD, Linux, and a few others.

  I recommend OpenBSD since their emphasis is security. They tightly control their software releases, closely monitor security issues, and have proactive security scans.

# Making Your Own Firewall: Hardware

- **Platform**

  I recommend a Pentium class machine (any clock rate) with 16MB or more of memory, 300MB or more of hard disk space, a floppy drive, and two PCI ethernet cards. Such a setup can be obtained for around $50 to $75.

  No CD-ROM drive or even monitor is necessary.

  Make sure you check the supported hardware list of the chosen OS before buying any hardware.

  I've had some problems with Compaq and HP due to their custom BIOSes.

  I buy all the hardware usually off Ebay and have considered Aussie Computers on North Lincoln.

# Making Your Own Firewall: Why Bother

- **Commercial vs. Home Made**

  If all that's wanted is firewall protection and maybe NAT, it's probably not worth the bother since the prices have fallen so much for entry level commercial firewalls.

  With commercial firewalls, the company must supply any updates. Services are limited to NAT and DHCP.

  With your own, you have a real computer on the Internet. Source code and binary updates are easily available. Good help available via DejaNews and web sites. Services also include remote login, file transfer, network tracing and logging, mail hub, HTTP services, virtual networks, etc. Whatever you can imagine!

# Basic Networking Services

- **DHCP (Dynamic Host Configuration Protocol)**

  Allows server (ISP) to dynamically assign the IP address and other network settings.

  @Home uses it to change assigned IP when your subnet is repartitioned.

- **NAT (Network Address Translation)**

  Allows several computers to share one internet address.

  Can cause problems with some services without additional configuration.

- **SSH (Secure Shell)**

  Provides a secure method of connecting to another machine. The connection is encrypted. Can be used to login or transfer files.

  Use NiftyTelnet on MacOS or PuTTy on Microsoft Windows.

- **Telnet / FTP**

  Unsecure and obsolete (accept for anon ftp). Use SSH instead when possible.

# Advanced Networking Services

- **Network Logging (ipfilter)**

  IP Filter is the rule set used to determine if network traffic can pass. It can also log information on any packet types, accepted or rejected.

- **Network Monitoring (tcpdump)**

  Allows active monitoring of network traffic (packets).

  Can be used on internal network to figure out why some network program isn't working right.

- **Mail (fetchmail / sendmail)**

  Fetchmail pulls mail from a mail server and stores the mail locally. It can configured to periodically and automatically retrieve mail from a mail server. Fetchmail allows you to keep mail locally on your firewall box so that you don't have to worry about your ISP mail folder size limits.

  Sendmail can be used to accept incoming mail or configured to send mail to another mail server.

# Advanced Networking Services (cont.)

- **HTTP Server (Apache)**

  The ‘standard’ UNIX web server. Needs a real IP address to be useful.

  Comes installed with OpenBSD, but needs to be configured and enabled.

  Very extensible and well supported.

- **VPN (Virtual Private Network, a.k.a IPSec)**

  Allows a secure network to be created between any two networked computers.

  Businesses can use them to connect their secure internal network to a computer on an external network (an employee at home).

- **Name Resolver (named)**

  A DNS (Domain Name Service) server converts Internet machine names (prairienet.org) to IP addresses (192.17.3.4).

  Named provides DNS service for your network and can help a DNS server do its job for your domain on the Internet.

# Local High Speed ISPs

- **@Home**

  Assigns real IPs, but wants users to use DHCP so they can be reassigned when needed.

  Doesn't like @Home users adding any servers of any kind. @Home scans for open ports. However, with a firewall, you can block the IPs that @Home scans from. Proceed at your own risk!

  50KB-150KB/s typical. 500KB/s when the students are gone. $40 / month. Additional IPs are $5 / month.

- **Prairieinet**

  Users are NATed (normally no real IP assigned, but uses private network address 10.x.x.x). If you complain enough, you can get a real IP.

  12KB/s guaranteed. 50KB/s typical. $40 / month.

# Web Sites for Further Information

www.firewall.com - General firewall information.

www.netgear.com - Netgear's RT311 and RT314 product information.

www.buy.com - Good place to buy new hardware cheap.

www.ebay.com - Good place to buy used hardware cheap.

www.deja.com - Start here when looking for answers to computer problems.

www.openbsd.org - OpenBSD's main site. Check out FAQ and Mascots.

www.openlysecure.org - Firewall information for open source systems.

www.fetchmail.org - Fetchmail's site.

www.sendmail.org - Sendmail's site.

www.apache.org - Apache's site.

www.home.com - @Home's site.

www.prairieinet.net - Prairieinet's site.

www.dyndns.org - Free dynamic and static DNS aliasing.

www.centralinfo.net - Highly rated domain registration and named provider.