Global Information Assurance Certification Paper

Connecting Your Home LAN to the Internet -- Securely

Andrew S. Baker

Introduction

Over the past few years, a number of technology advances have converged on the computing scene, resulting in a need for secure Internet connectivity from the home.

- Increased availability of Broadband connectivity
- Multiple, low cost computers in the home
- Telecommuting and Home Offices
- Online Banking
- Online Trading

Depending on a number of things, including the technical savvy of the home user in question, there are several avenues that can be used to provide secure Internet connectivity. The typical options range from simple **NAT/IP Masquerading** to full-blown firewalls with **Stateful Packet Inspection**.

Risk Assessment

As always, the level of security deployed should be based on the value of the data that is to be protected. Although you might not feel that you have anything significant on your system, you should consider what would happen if someone gained access to your financial records, or was able to infiltrate your employer via **VPN** because of access to your home system. And what about liability? Suppose your machine(s) are used as the staging grounds for a DoS attack against someone else? What happens when the attack is traced back to your system?

Finally, there's the inconvenience of rebuilding your system, even if none of the risks mentioned above is a reality.

Software Firewalls

For the Windows user, this category of product covers both the **Personal Firewall/IDS** (e.g. **ZoneAlarm**, **Tiny Personal Firewall**, **BlackICE**) and the more powerful Internet Connectivity products with integrated firewall component (e.g. **WinRoute Pro**, **SyGate**)

The former are installed on individual systems, and configured to allow the appropriate traffic in or out of the system. They possess very easy to use interfaces, and provide even novice computer users with a very good option for security of a single desktop. Best of all, many of these Personal Firewalls are free.

Even if you are using one of the other products mentioned in this document, a Personal Firewall allows you to control specific traffic into and out of your system. Many freeware products use a category of software referred to as **SpyWare**. This software, in the form of ads, tracks your web browsing habits and reports them back to a central server. Many folks dislike the invasion of privacy that **SpyWare** can represent, and using a Personal Firewall (like **ZoneAlarm**) will help you detect and eliminate utilities and applications trying to access external resources without your consent.

Figure 1.

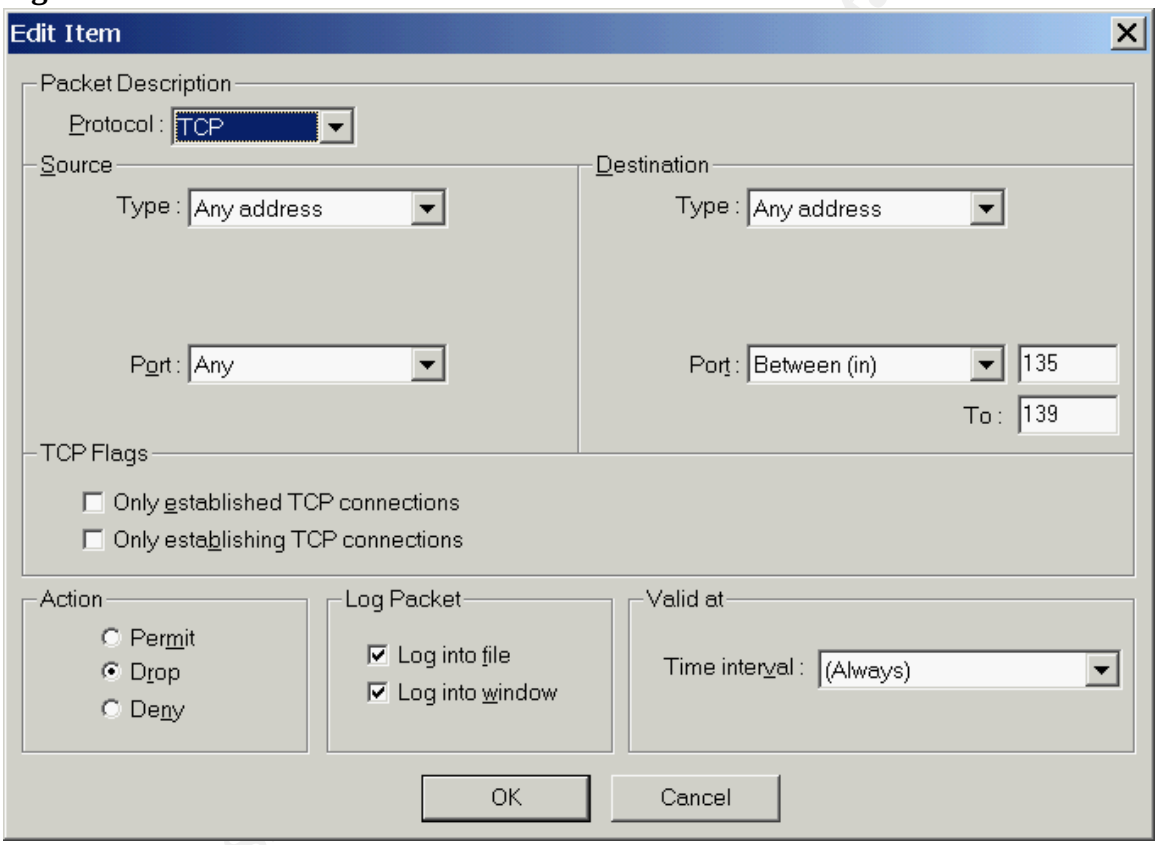
Figure 1 shows **ZoneAlarm** in action. It is blocking a Telnet attempt to a high port, and reporting this information to the user, who can then configure the product to allow or always deny this type of connection. While there are no known trojans which operate on Port 2032 by default, many of them are configurable. A list of ports that are used by malicious programs can be found here: http://www.simovits.com/nyheter9902.html

Slightly higher up the chain are the **NAT/Proxy** type products, and while most of them are not free, they are far less expensive than their commercial firewall cousins. Additionally, they

provide much more flexibility than their desktop brethren. Ranging from $50-$250, these products allow you to connect your entire network to the Internet using **NAT** and/or **DCHP**. What you gain is the ability to create rule sets that rival commercial firewalls. Rather than blocking everything and then waiting on you to let it through on a case-by-base basis, these apps allow the knowledgeable user to specify in advance which protocols will be allowed to enter and exit the network. A bit more upfront knowledge is needed to manage this class of product effectively, but the advantage is that less configuration is needed for all the other hosts on your network.

WinRoute Pro, for instance, allows you to block specific **ICMP** types, map ports to specific services, setup a **DMZ**, and offers complete logging (to screen and file) for whatever traffic you want to keep a record of.

Figure 2.



In **Figure 2**, **WinRoute** has been configured to drop **NetBIOS** packets, and log the results into the console window for immediate review (as well as the permanent log). For Windows networks, this is very important. Besides a potential attacker learning a lot about your network, there are a number of vulnerabilities that can be exploited if your network is exposing **NetBIOS** traffic to the Internet. Generally, there is **no** reason to allow anyone (not even yourself) to have the ability to connect directly to your Windows systems from the **WAN**. If you need to provide access to your network from the Internet, then you should setup **PPTP** or another **VPN** solution for secure connectivity.

ICMP traffic is another protocol with security implications that you should consider blocking at your router/firewall. It has often been used to probe for host information, and as a means of **DoS** attacks. The proper use of these Software Firewalls allows you to centrally protect your entire LAN at your Internet gateway.

Broadband Routers

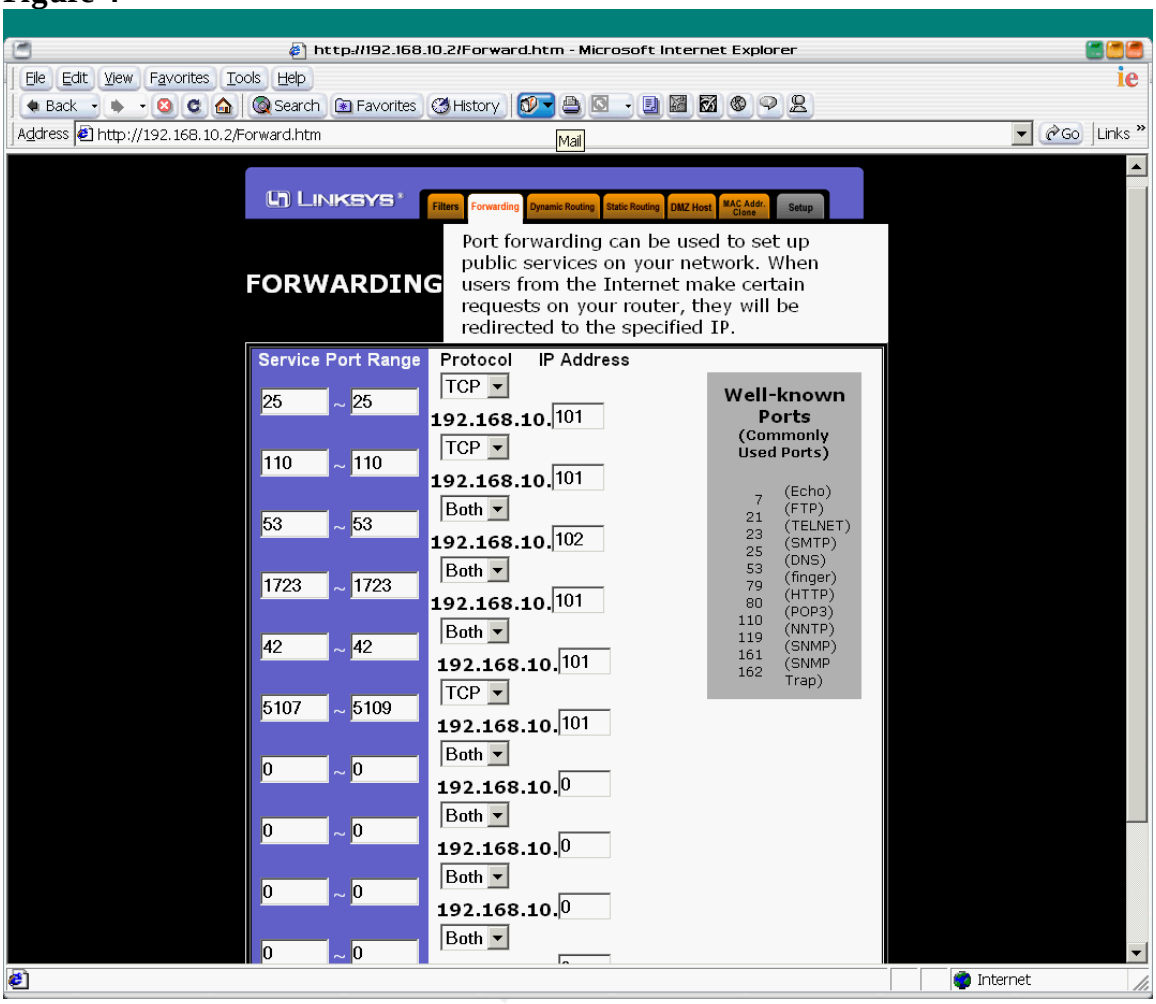
Cable/DSL routers (e.g. **LinkSys**, **SMC**, **NetGear**) sprang onto the scene in a major way in 2000. These small, compact devices provide Internet connectivity with integrated **NAT**, **DHCP** and **DNS** forwarding. For many consumers, this is a better (easier) option than a software firewall, as it does not require a machine to be left up and running, and it takes up far less space than a full-blown desktop. Additionally, many of the networking vendors are producing these routers with integrated **4-port** and **8-port** unmanaged switches, obviating the need for the purchase of a separate hub or switch.

These devices offer generic protection, in most cases, as many of them do not add anything above **NAT** to the security checklist. If your focus is more on connectivity, and general obscurity of your network, then these devices will suffice, and the price is right ($100-$150). With only a basic knowledge of networking, you can be up and running in less than 15 minutes with one of these devices. They are nice and compact, and generally provide a straightforward web interface for configuration and fairly comprehensive manuals.

Where they lose out to Software Firewalls is in configuration options. Generally, they support a limited number of mapped ports from the outside address to an internal address, and the mapping must be direct (e.g. port 25 outside must be port 25 inside), so there is no way to map the same service to two different machines as you could with the better software products. Also, broadband routers don't typically block **any** outbound traffic beyond **NetBIOS**. This leaves them susceptible to certain Trojans (http://grc.com/lt/hardware.htm)

While you can't be as creative with which ports you allow to or from your network, broadband routers offer the best in simplicity and are largely OS-neutral. For most individuals, particularly those with only modest needs to host services from their internal network, these products will make the most sense and are likely to be deployed more than any other firewall solution. By default, they will keep you safe from both **NetBIOS** and **ICMP** attacks and probes because they block those services automatically. And, because many come with 4 or 8 switch ports, they are great for first-time users of home networks. A small investment of both time and money will get your **Windows**, **MacOS**, **Linux** and **BeOS** systems networked and on the Internet in no time.

Figure 4



As **Figures 4** indicates, you can setup **Port Forwarding**, configure a **DMZ**, and setup **Static Routing** using a **LinkSys Broadband Router**. Here, **PPTP**, **SMTP**, **POP3** and **DNS** traffic are being mapped to two different servers in the internal network.

Firewall Appliances

These robust products are essentially what the Broadband routers were derived from. They provide true Firewall features (packet filtering, stateful packet inspection, secure VPN, port mapping, and logging). These devices can range from $500 to several thousand dollars, but they are a must for anyone who has outgrown the limitations of the previous products, or has more to protect on their network. They offer all the logging and configuration options of Software Firewalls (including **Linux/OpenBSD** solutions) as well as the compactness of the broadband routers.

Ease of use has been a primary goal for many of the vendors of security products, since a firewall, which is hard to use, will be abandoned or used improperly, resulting in poor security. Nevertheless, it is important that one has at least a basic understanding of IP protocols before undertaking the installation and configuration of this class of product.

Another advantage of the firewall appliance over a software solution is that the issues of hardening the underlying OS are addressed. No more worries that your firewall might be undermined by a poor installation of Windows, upon which it is running, or that you have inadvertently left some insecure service running on your Linux box. This benefit extends to any security holes that might be found in the OS, even after a secure installation, or upgrades to the OS that might break or alter the firewall functionality.

In general, it is highly advisable that you avoid putting other services on your firewall box (e.g. **SMTP**/**POP3**, **FTP**, **HTTP**). Many services can be exploited to break in to your network, or a Denial of Service may be waged against the device hosting that service. If you are running an **SMTP** server on your firewall, and that service is compromised or the victim of a **DoS**, then your network connectivity and security will likely be compromised.

One piece of key functionality is **Stateful Inspection**. Most of the products mentioned so far simply check to see what port a service is attempting to use. For example, any product attempting to connect to TCP Port 80 is presumed to be an HTTP client. With **Stateful Inspection**, the packets are evaluated to ensure that they conform to the formatting that is consistent with the protocol they purport to be.

The final advantage is performance. Hardware is almost always faster than software, and having a discrete firewall device offers better performance than an all-purpose machine with an all-purpose OS, which is performing other tasks.

Linux/OpenBSD

For the enterprising soul, or anyone who has Unix experience, or someone who wants the ultimate in control and price, there's the **Open Source** option. If you have an older x86 system (486 or above) with 32 or 64MB of RAM, you can build your own custom firewall.

This will provide you with the greatest flexibility and control, using **IPChains** or **IPFilter** and recompiling the kernel for yourself. You can gain almost all of the advantages of the **Firewall Appliance**, in that you will be able to eliminate every service or module from your installation which is not firewall related. This solution is not for the faint of heart, and is not as useful for those with modest connectivity needs who are simply interested in basic security, but there is no denying that you can customize this solution for your specific network. And, all it will cost you is some time and the use of an older box that you probably weren't going to use for anything else, anyway.

What you lose in complexity, you can in speed, customization and price. Some folks prefer the use of an **Open Source** firewall to that of a "mystery box" such as a **Broadband Router** or **Firewall Appliance**, because of your ability to control everything that is installed, rather than relying on the features that the vendor chose to provide. Also, the Open Source Community is generally on top of all security related issues, and patches are often available to the Linux or BSD kernel in a matter of hours or days, rather than weeks or longer with closed, commercial products.

Again, the only real tradeoff is in time and having to learn another OS – something that many home users are not going to find acceptable for the perceived benefits.

Conclusion

Once your firewall is in place, you should verify that it is allowing only the traffic you need it to allow for proper functionality. There are several sites (e.g. **GRC**) where you can test the effectiveness of your firewalls. This should be done routinely, as there are new exploits being discovered almost daily.

As the number of network attacks increase, and as Internet connectivity becomes more and more commonplace, we can no longer afford to take security from our homes for granted. Windows users will be drawn to the simplicity, convenience and cost of the broadband routers, while more adept users will seek out options with more flexibility, such as the appliances, or building their own Linux/BSD firewall. There's no particular reason, by the way, not to employ multiple levels of security. A broadband router, supplemented by a personal desktop firewall, for instance, will provide much more security than either of the two products alone.

Regardless of which solution is chosen, one thing must be remembered: An improperly configured device is much, much worse than having no device at all, because of the false sense of security that will exist. If your device supports logging, be sure to check the logs regularly in order to ensure that no changes need to be made in what is being filtered and what you need to protect. And be sure to check the vendor's site to keep up to date with the patches and increased functionality that is offered.

References

The following resources were used in this document:

Da LAN Tech - Firewalls (Classification & Reviews)
http://www.dalantech.com/firewall.shtml
http://www.dalantech.com/zone-alarm.shtml
http://www.dalantech.com/linksys-dsl.shtml

Application Gateways and Stateful Inspection: A Brief Note Comparing and Contrasting
http://www.avolio.com/apgw+spf.html

Stateful Inspection in Action
http://www.checkpoint.com/products/technology/page2.html

Securing Your Home Network
http://securityportal.com/topnews/secure20000718.html
http://www.securityportal.com/articles/pf_main20001023.html

Personal Firewalls
http://www.zdnet.com/downloads/deathmatch/firewalls/

Hardware Router Comparison
http://www.practicallynetworked.com/sharing/hwrouter_chart.htm

Shields Up (Testing Your Personal Firewall)
http://grc.com/su-firewalls.htm

Software NAT/Proxy Products
http://huizen.dds.nl/~jacco2/isdn/ipr_ispa.html

Building Linux or OpenBSD Firewalls
http://www.wiley.com/compbooks/catalog/35366-3.htm
http://www.openbsd.org/
http://www.linux.org/
http://www.freesco.org/

Using/Configuring IPChains for Linux
http://www.pointman.org/PMFirewall/
http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html

Using/Configuring IPFilter for OpenBSD
http://www.openlysecure.org/content/html/ch9-27.html
http://coombs.anu.edu.au/~avalon/
http://www.tfsb.org/ipf-openbsd/

Firewalls FAQ
http://www.faqs.org/faqs/firewalls-faq/

Software Vendor Sites

ZoneAlarm	http://www.zonelabs.com/
Tiny Software	http://www.tinysoftware.com/
SyGate	http://www.sygate.com/products/
NetworkICE	http://www.networkice.com/

Hardware Vendor Sites

NetScreen	http://www.netscreen.com/
WatchGuard	http://www.watchguard.com/products/soho.html
ConSeal PC Firewall	http://www.candc1.com/conseal/cfindex.htm
LinkSys	http://www.linksys.com/
NetGear	http://www.netgear.com/
SMC	http://www.smc.com/