Global Information Assurance Certification Paper

Cable/DSL Router and Personal Firewall: Belt and Suspenders?

Mike McCabe
February 14, 2001

Introduction

Well, I finally broke down and got a Cable Modem for my house. Man, is it fast compared to the old 56K modem. But it does present a problem. The problem is that it's always on and connected to the Internet! And that means that any script kiddie can attack my machine anytime it is powered up.

Of course, I also have the problem that many homes have now, and that is the problem of multiple computers. My wife has her own computer and would probably string me up if I didn't let her have the high speed Internet Access that I now enjoy. Fortunately, there is a device that solves both of these problems almost perfectly.

This paper will be about my experiences in getting Cable Modem access to the Internet, how I researched, purchased and installed a Firewall/Router Appliance for external security and a Personal Firewall on my DMZ system.

Background

For external security there is nothing on the market right now that is better than a Cable/DSL Router appliance for providing external security. You can buy these at your local computer store. These devices feature options like NAT (Network Address Translation), a DHCP (Distributed Host Control Protocol) client for the Wan device, a DHCP server for the inside network, the ability to specify a DMZ (De-Militarized) host for services, the ability to filter by IP or MAC address, Dynamic or Static Routing, some even offer a Print Server, and last but not least, the ability to forward specified ports to an internal host. Best of all, they are relatively inexpensive at only $150 to $300, or so, at your local computer store.

I am a big fan of online games as well as being a security consultant; unfortunately, some of the games that I like to play require direct access to the computer, which means that at least one of my computers would have to be put into the so called DMZ. So if I put a computer into the Router's DMZ, then how is it protected? The answer is not at all.

Enter the personal firewall. I know its like wearing a belt and suspenders to have first an appliance that protects the network backed up by a software firewall, but I'm just a bit paranoid. As I found out later, it was a good thing that my paranoia about people scanning me was so prevalent in my mind.

Research

The first purchase was a Linksys Cable/DSL Router at my local Comp USA store. I looked at both the Linksys and SMC models of Cable/DSL Routers. I picked the Linksys simply because I have always had good luck with their equipment and its also what our corporate VPN people have been specifying for home to office VPN use. The SMC had the added feature of a print server that would allow me to serve one printer on the network.

I didn't need this feature because I am blessed with an HP Jetdirect 3 port print server already. If you don't have a print server on your home network, you might want to look closely at this feature on the SMC product. I'm not sure how I ever got along without a print server on my network, but I remember it wasn't pretty with all those A/B/C switches and big thick cables.

Anyways, since I purchased the Linksys Router I have done some searching and review reading on the Internet and have found that I probably made the right purchase decision for my situation. The Linksys product has all the right features for my network including a 4 port high speed 10/100 switch, DHCP server, and the ability to have a host as a DMZ server host. They also have made some timely updates to their firmware. For those of you who have not decided on a specific router, I have included URL's from two very good reviews which may help you to decide:

http://www.3dhardware.net/reviews/home_router_roundup/index.x
http://www.neoseeker.com/Articles/Games/Roundups/internet_router/index.html

Much more research was performed in the selection of a personal firewall. I have included the URL's to several reviews that I used during the decision making process:

http://grc.com/lt/scoreboard.htm
http://www.securityportal.com/articles/pf_main20001023.html
http://www.8wire.com/articles/index.asp?AID=1384

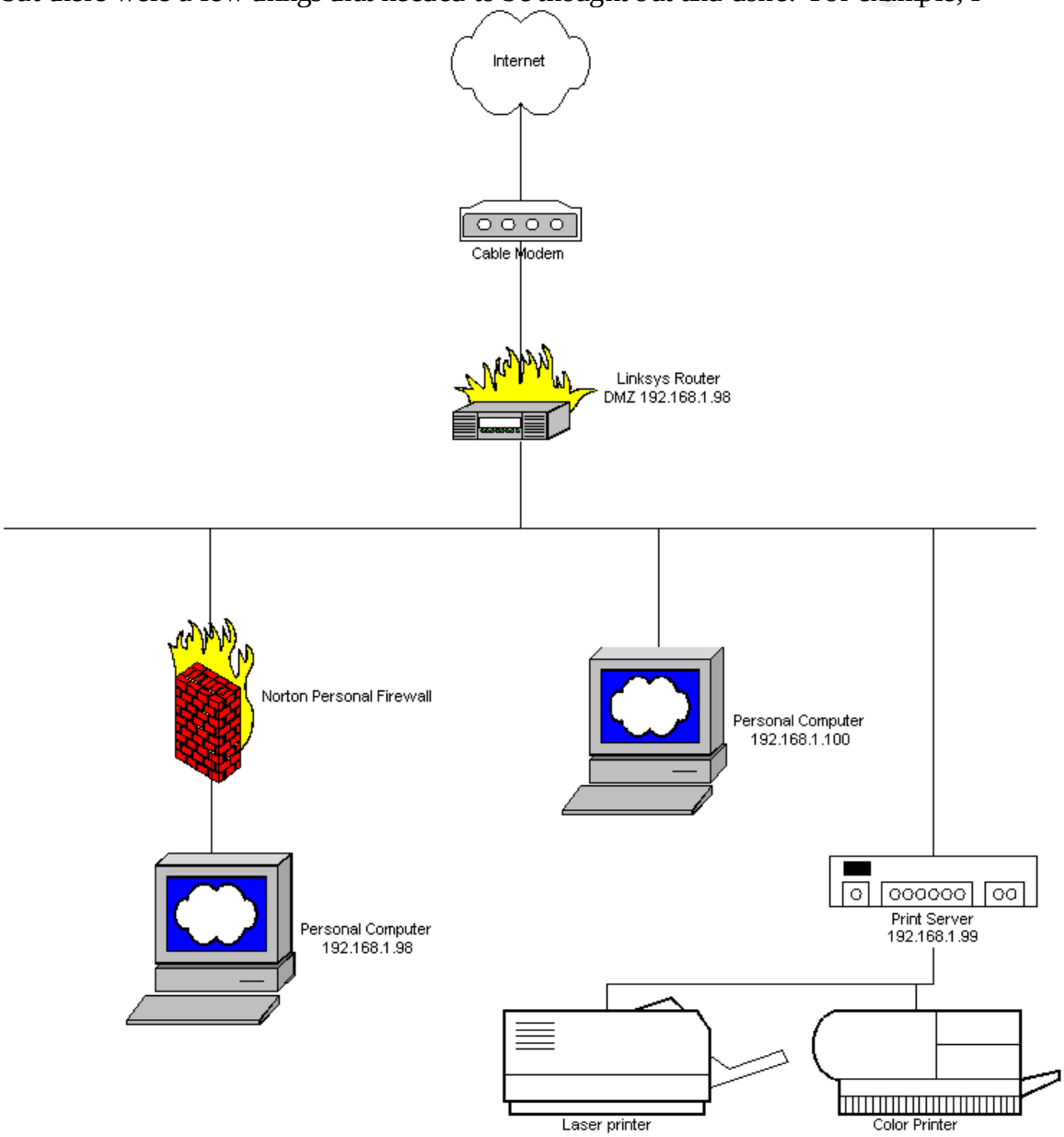
My final firewall selection was for the Norton Internet Security 2001. This package includes a firewall, Anti-Virus software and a personal protection feature to keep web pages from stealing my personal information. The things that attracted me to the Norton Personal Firewall were its ability to generate specific rules for various incidents. The Norton Personal Firewall 2001 gives you the ability to either allow for automatic generation of firewall rules (if the firewall knows of the program) or to specify your own. The information that can be specified in a rule includes the following:

1. Application Name (selected or any)
2. Source and Destination IP Addresses (single host, specified network, or any)
3. Source and Destination Port Numbers (single, selected, ranged or any)
4. Logging Preferences (including whether a security alert should be posted)

The other thing that I was interested in was the ability of this package to wrap up Anti-Virus and personal protection software along with the firewall for a reasonable price. Symantec also sells just the firewall separately and another package that includes parental control features, which I didn't need.

Installation

As can be seen in the diagram, the network configuration is pretty simple as networks go, but there were a few things that needed to be thought out and done. For example, I



needed to be sure to set the printer server to a non-dynamic address so that the computer would always find it at 192.168.1.99. Also, my computer needed to be at a fixed address to be able to use the DMZ feature of the Linksys router, so it got assigned an address of 192.168.1.98. However, the rest of the network I wanted to be dynamically assigned, so I ran the DHCP server and set it to start at 192.168.1.100.

When the technician came out to setup the cable modem and get us online, the only thing he was allowed to connect the cable modem to was a NIC card in a computer. So initially, the cable modem was connected to my computer. Soon after he left I used the MAC editing ability of the Linksys to change the MAC address of the outside interface of the router to match the NIC card in my computer. This is a good feature of the router and is possible because really even though MAC addresses are supposed to be globally unique, they really only need to be unique on a given Ethernet network. Once I had changed the MAC address, I watched as the Linksys was given an IP address, Name server addresses, and gateway information from the providers network.

The installation of the Personal Firewall Software I expected to be somewhat disconcerting from my prior experience with firewalls (Raptor, Checkpoint, PIX), but it was painless. The first thing I wanted to do after installing the software was to go and peruse the rule set to see what automatic actions the installation had taken. But before I could do this, I was greeted with an alert dialog box saying that my MSN Messenger service task was attempting to talk on the internet and the firewall wanted to know if this was ok or not. After working my way through a number of dialog boxes, answering questions like did I want to allow this communication and what addresses and service ports should this task be allowed to communicate on, I had a brand new rule for MSN Messenger.

Finally, I made it into the advanced setup options to look at my new firewall rules and what a sight I was greeted with. There were more than 30 rules already blocking things like Backorifice and SubSeven. In addition, there were rules for Internet Explorer, and looking closely, even my new rule for MSN Messenger.

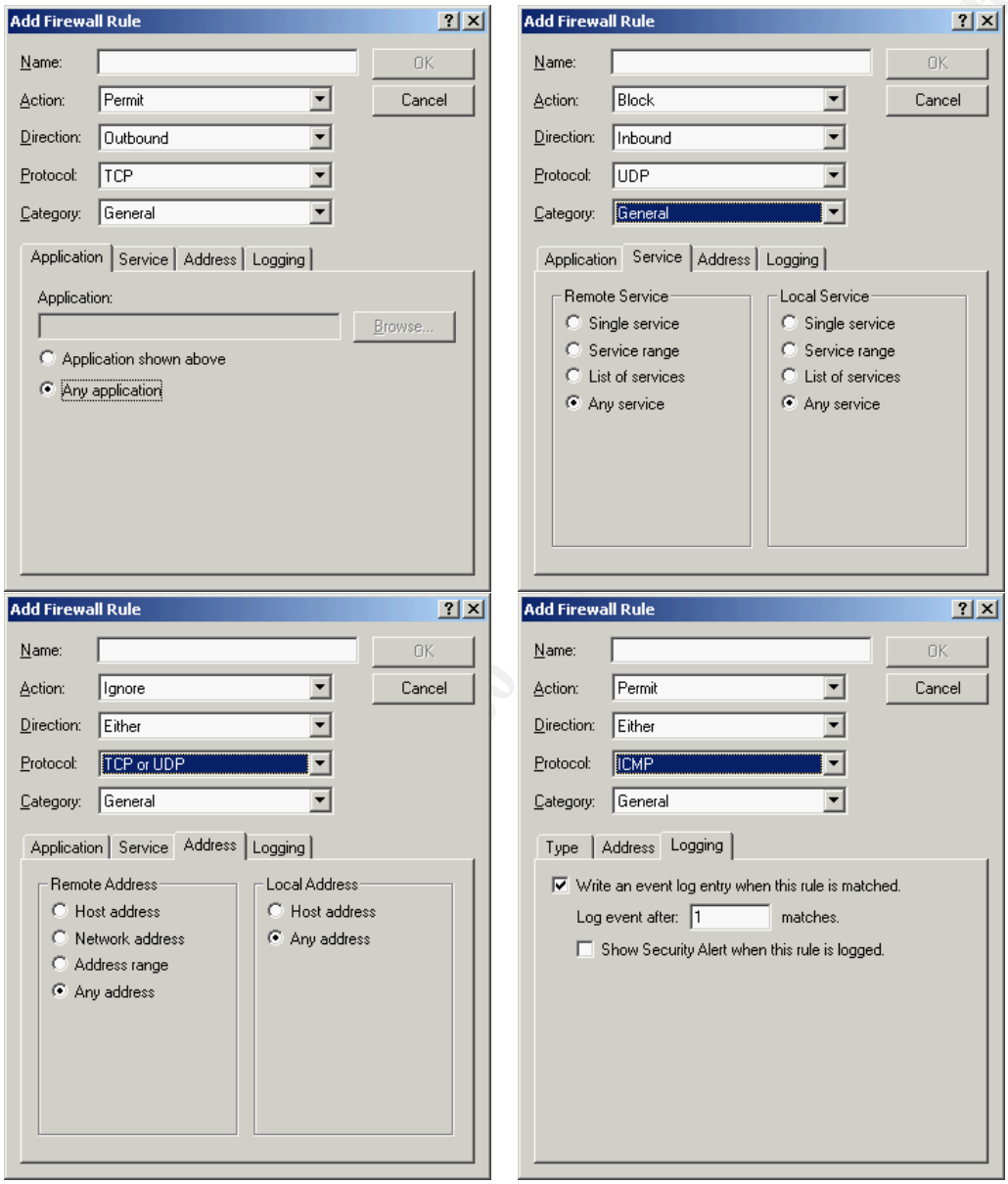
Configuration

The configuration of the Linksys router was pretty self-explanatory to anybody who knows something about IP. It's all done via a web browser based interface. You basically surf your web browser to http://192.168.1.1 and enter the default password (The password you get out of the instructions). Being security minded, the first thing I did was change the password to something other than the default.

Setting up the DHCP server was easy; all it wanted was a starting address. Setting up my computer to be the DMZ host was just as easy. I only had to type in the last digits of the IP number.

For configuration of more rules, the Norton Personal Firewall allows you to either wait until a program tries to communicate with the Internet, or you can go through the following dialog boxes which show a representative sample of the configuration possibilities of the firewall (See next page). Notice that you can specify things like the application, addresses, whether to permit, block or ignore the traffic, service information, protocol, and whether to allow the traffic as Inbound, Outbound, or both. In the following dialog box images, I have tried to show the various options available when setting up a rule.

Setting up the Anti-Virus and Personal Protection software was very routine. The package was installed and then immediately updated via Norton's liveupdate software. It then did a scan of my hard disk and found no viruses. Later on, I received some email with a virus attached and it detected and quarantined the attachment just as it should.



Conclusion

In conclusion, the combination of Linksys Router and Personal Firewall may seem like overkill, but when I was checking the logs shortly after first installing the Firewall, I noticed that within the first 10 minutes of installation I was scanned by somebody looking for the Backdoor/SubSeven Trojan on my system.

Of course, this is only one hole that I now know is closed. In order to verify what my machine looks like to the rest of the world, I decided to do a port scan from a remote box. After some research and reading, I decided to use the nmap port scanner on a linux box I have access to on the Internet. When I ran the port scanner against my box, first off Norton Firewall predictably started flashing a system alert, and looking at the log showed massive amounts of rejected attempts. What was most interesting was that nmap found absolutely no open ports on my system and could not even determine the operating system type. Now that makes me feel pretty secure. The only time ports would show as being open is when I'm running software that opens them on purpose.

References

Gillitzer, Travis, "Home Networking Router Roundup", 12 November 2000, URL: http://www.3dhardware.net/reviews/home_router_roundup/index.x (14 February 2001)

Roberts, Anthony, "4-Port Internet Router Roundup", 21 September 2000, URL: http://www.neoseeker.com/Articles/Games/Roundups/internet_router/index.html (14 February 2001)

Gibson, Steve, "Personal Firewall Scoreboard", URL:http://grc.com/lt/scoreboard.htm (10 February 2001)

Boran, Sean, "Personal Firewalls/Intrusion Detection Systems", 26 January 2001, URL: http://www.securityportal.com/articles/pf_main20001023.html (9 February 2001)

Bensimon, Michael, "Review: Software Firewalls for Personal Protection", 17 November 2000, URL:http://www.8wire.com/articles/index.asp?AID=1384 (8 February 2001)

Linksys, "BEFSR41 – EtherFast 4-Port Cable/DSL Router", URL: http://www.linksys.com/products/product.asp?prid=20&grid=5 (28 January 2001)

Linksys, "BEFSR41 – User's Guide", URL:ftp://ftp.linksys.com/pdf/befsr41ug.pdf (28 January 2001)

Symantec, "How to configure Norton Internet Security or Personal Firewall to allow an Internet application to work", URL: http://service1.symantec.com/SUPPORT/nip.nsf/docid/2000120606411136&src=hot (4 February 2001)

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS