GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Home LAN Defense: A Practical Example for the Home User

George Starcher

January 20, 2002
GSEC Practical v1.3

Abstract:

Most papers written for the System Administration, Networking and Security Global Incident Analysis Center Security Essentials Certification (SANS GSEC) are targeted to other Information Security (InfoSec) professionals. However, there is a rising trend of malicious targeting of the newer powerful home networks and computers run by home computer enthusiasts. Home computer enthusiasts are people from all walks of life. The majority of these enthusiasts deal with computers as a function of their professional or student lives without being, or having the direct support of, information technology and security specialists. Information security related articles, advertisements and product reviews deluge the enthusiast from all sides. Security warnings from the media, government agencies, InfoSec organizations and vendors espouse the mantra of patch and protect without providing practical examples. In this paper, we will specifically address the needs of home computer enthusiasts and provide a practical example for their guidance.

Any experience in workplace computing will quickly teach that if a system is too difficult or changes hamper the users' experience that it will be abandoned or circumvented. What should we expect to happen in the home if a computer user finds their online game, chat tools, etc. cease to function due to the latest hyped home protection software package or shiny new cable router? Just as in the workplace, the changes will be quickly undone as the computer is there to serve entertainment, home business or financial purposes. Our practical example of today's typical enthusiast home network will detail the issues and solutions taken to secure it without crippling its value to the household. Security and usability are on opposite ends of a balancing act. We will find that balance in the course of this paper.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Beginning Scenario:

The typical non-networked home is comprised of a couple of Microsoft Windows machines with modems for dialup to the Internet. The Internet provides for web surfing, web page building, email, online chat and online financial tasks. In this example we will start with just two PCs. The first PC belongs to the husband and is used mainly for web page building with MS FrontPage, game and web entertainment and ICQ for chatting with his friends and son online. The other belongs to the wife who uses hers for online shopping, balancing the checkbook, AOL Instant Messenger and email with family and friends. Both machines use Microsoft Office, Outlook Express for email and Internet Explorer for web browsing.

The first step: Anti-virus Protection

We all heard about that that really cool screen saver that went around via email or the ICQ chat program. It happened to be called gone.scr (1). This is was a worm and taught us quickly that everyone tends to trust their friends and family who send these cute little programs that you just have to run. It equally shows that every PC should have up to date anti-virus software. There are many anti-virus products on the market that provide solid protection and automatic updates via the Internet. Jon Willert provides a thorough list in his SANS paper, "Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters" (2). Save reading his paper till after you are done here as you will quickly relate our work together to the security concepts he presents. I disagree only with his placement of Computer Associates InnoculateIT at the bottom of his list. The home user version of their product can be found at http://www.my-etrust.com/. We will not touch on the actual configuration and installation of any particular anti-virus package as few of them these days actually interfere with our systems and functions, are easy to install and are recognized as necessary by the most common home user. A quick download from Computer Associates or a trip to the nearest tech store such as BestBuy, CompUSA, or Fry's, depending on the region you live in, will snare a suitable anti-virus product. Now we have our example home machines protected from those nasty worms and viruses we hear about on the news. We chose the anti-virus solution from http://my-etrust.com for our machines

All current anti-virus packages allow automatic updates from the Internet. My-etrust prompts us to give it permission to download an update after installation. We then open the program and click the Go so we get a clean scan of our system. You will find all anti-virus packages have a similar interface when the main program is running. Typically a panel on the left side showing all the machine's disc drives and somewhere on the menu bar will be a start or go button to force a scan. It is good form to force a scan when you first install anti-virus software then repeat or use the automated scheduling options within the software for weekly or monthly complete scans.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The second step: Patch, patch, patch!

Our family computers are doing what we require of them and are protected from malicious software (viruses, worms and Trojan horses). Our husband and wife team surf the web, email friends and chat online with relative peace of mind. After all our machines are protected from those viruses we hear about on the news. We do learn one important additional fact from all those news articles. They keep telling us to patch our computers. This is relatively easy since our duo has standard Microsoft Windows computers. It just might take a while since right now we use normal phone line modems to access the Internet.

1. We just go onto the Internet, open our chosen web browser Internet Explorer. Also known as the big blue 'E' on your computer screen desktop.
2. In the Address Box above the home web page that comes up we will enter http://www.windowsupdate.com then click the GO icon next to the box.
3. In the left hand column you will see a spot called Product Updates. Click This spot.
4. You might get a dialog popup box asking if you trust content from Microsoft. Just click Yes.
5. A new window should come up stating that it is checking your machine for the updates needed.
6. When it is completed, your web browser will come up Select Software and if you are not up to date you will see just underneath "Critical Updates and Service Packs" a selection called "Critical Updates" and it should have a checkmark in the box to its left. If it is not checked then click on the box.
7. Click the Download arrow button in the top right corner.
8. The browser window will come up to Download Checklist where you need to click Download again to confirm and start the download and installation of the latest patches for Windows and Internet Explorer.
9. A dialog box will come up and you will have to click Yes to accept the license agreement and begin the download.
10. When it is completed the window will come up to Download Results and tell you if the patches installed correctly. It will also popup a dialog box asking if you wish to reboot. Go ahead and let your system reboot with the patches in place.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

To completely address the two simple facts of life in computer protection (anti-virus and software patches) all software on the machine such as MS Office, AOL IM, ICQ etc should have the latest patches installed. We should see the vendor web site for downloadable patches or the newest versions. A little known site for MS Office 2000 and XP is http://office.microsoft.com/. We will see on the left hand side an option for product updates just as you found in the procedure for updating Windows itself. Just click and follow the directions they provide. One word of warning applies to both the Office 2000 Service Pack 2 or Outlook 2000 SR-1: Extended E-mail Security Update. If you use Outlook 2000 for your email client you will cease to be able to get certain types of attachments such as EXE files through email. This is only reversible by removing and re-installing MS Office 2000. This is good from a security point of view but rarely desired in the home environment. MS Office XP has this feature built in with no recourse for the user.

The third step: Usage analysis and special risks

Up to this point we have ensured our computer operating system (Windows) and our various applications (MS Office, ICQ etc) are patched and the latest versions. Now we look at how the systems are used and what risks are added.

Our couple sends lots of email to family and friends. The husband spends a large amount of time making web pages for people he knows and chatting via ICQ. This type of constant usage leads to lengthy online time on the phone. We have just stumbled into the first misunderstood concept in home PC security. It is often said how computers with those always on high-speed connections need protection from hackers. This is also true for normal dialup based connections. There is little difference if your machine is online for hours with a modem or a fast always-on connection such as a cable modem. Bonnie McDougall experienced over 400 hits from the Internet when writing the SANS Paper, "Personal Firewalls – Protecting the Home Internet User" over the course of 5-6 hours (3).

The question most home users have is, "How can hackers hurt my computer and how do I stop it?" The problem is that if you have software such as Microsoft FrontPage, AOL Instant Messenger, ICQ, etc you are running software that acts as a "server." It is hosting software that is listening on the network so it can provide the services you want such as people sending you live messages or creating web pages locally before posting it to your ISP. FrontPage and Windows2000 run a "small" version of Microsoft's web server IIS. You might recall all the news articles on the Nimda worm. It would invade PCs and Web Servers running Microsoft's IIS web services (4). Nimda, other such worms and hacker attacks tend to use what is the most common and powerful software vulnerability know as the buffer overflow attack. An editorial in ComputerWorld by Frank Hayes called "Swat the Buffer Bugs" tells us all about this form of attack (5). Most InfoSec professionals would hardly argue with the statement "…2002 looks like the year of the buffer overflow." (5) All software can have such vulnerabilities. BlackICE personal firewall just required a patch update to correct a buffer overflow issue (6).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The fourth step: A Software Firewall

Now that we have a little education on why patches need to always be applied we are still left with how we are supposed to protect our machine until those patches are released. The software we need is referred to as a personal firewall. There are many popular choices such as the ZoneAlarm (free for home users), Norton, McAfee and BlackICE. Again Jon Willert provides a thorough list in his SANS paper (2). ZoneAlarm allows the user to shutdown all Internet access with a click, allow only certain programs outbound access while protecting from unauthorized inbound connections across the network. My personal favorite is BlackICE, which does not do anything for outbound protection as ZoneAlarm does but I find it less bothersome for that same reason. A more technical reason I like the BlackICE product has to do with how it looks for "malicious" network traffic as opposed to just blocking types of connections. BlackICE is an intrusion detection system (IDS) as well as a firewall. This allows it to identify and block attacks such as the dreaded Buffer Overflow coming from the network giving us more time to obtain and install software patches. The technical explanation of how BlackICE performs "full protocol analysis" is beyond the scope of this paper (7). You may read "The Evolution of Intrusion Detection Systems" by Internet Security Systems for further information (7). It is also the personal firewall of choice for the home Internet gamer as it is faster in handling network traffic for games such as DiabloII while still protecting the system. We will address both ZoneAlarm and BlackICE in this paper as our user, the Husband, likes to actually run both on his machine to the chagrin of his son, but we will address this later in the paper under troubleshooting applications.

There is online documentation available for both ZoneAlarm and BlackICE. This material covers the normal installation and setup issues. We will accept that the documentation for the base installation is sufficient and does not need repeating here. We will cover configuration adjustments to these packages beyond the base installation.

- **ZoneAlarm**:
  - A paper on ZoneAlarm by Curtis Elliot, "ZoneAlarm – A Free Solution for Home Security"(8) http://rr.sans.org/homeoffice/zonealarm.php
  - ZoneLabs Online Product Documentation: (9) http://www.zonelabs.com/services/support_za_zap.htm
- **BlackICE**:
  - ISS Online Product Documentation: (10)
    Both the BlackICE Defender Users' Guide and the Advanced Administration Guide are good resources. The Administration Guide is more technical but explains the precise differences in the Protection Levels. This can be found starting on page 34.
    http://www.networkice.com/support/documentation.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

We install the personal firewall of choice, either ZoneAlarm or BlackICE. We can even run both to gain a more complete level of protection, though we have to make more adjustments to make our programs work properly. Once they are installed, a few adjustments from the default settings should be made for our purposes. When this is done we will have patched and secured the systems as tight as we can for our beginning scenario while maintaining all the functions desired by our duo.

ZoneAlarm:

The default settings for ZoneAlarm upon installation are very acceptable to our needs with a few minor adjustments.

Configuration Tab (Figure 1): We ensure ZoneAlarm loads at startup and checks for updates automatically. We remove the checks on popup during Internet activity and before exchanging information with Zone Labs as that could become tedious.

Figure 1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Lock Tab (Figure 2): We enable the automatic locking when our screen saver activates as we have one set for 15 minutes and to allow the "Pass Lock" for programs we specify to always access the Internet. We do this for our antivirus updates and other programs that have automatic updates we wish to occur without us around.

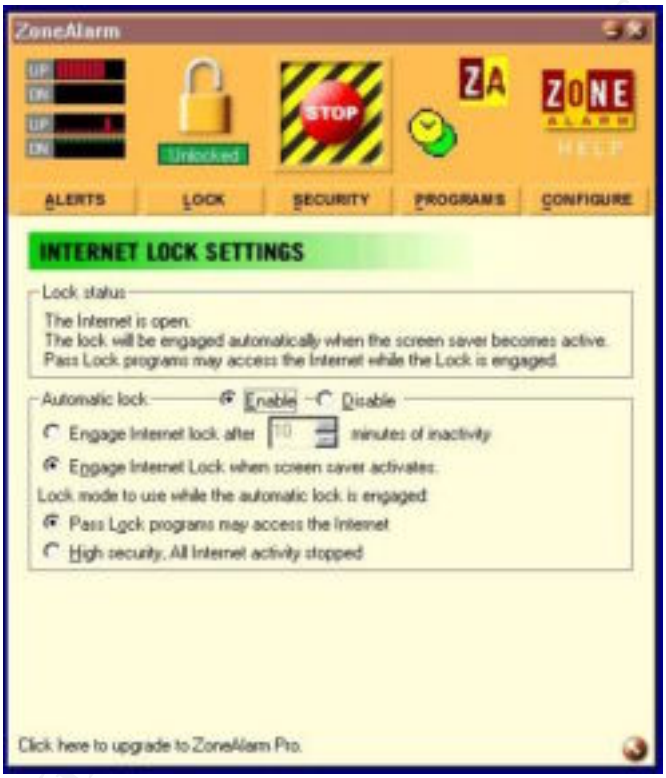


Figure 2

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Programs Tab (Figure 3): When we start programs such as ICQ, AOL IM, Internet Explorer, etc. ZoneAlarm will automatically ask us if we want to allow access and "Remember" for future use. We choose to remember and allow those programs access to the Internet as we start each one in turn. Then we come to this tab in ZoneAlarm to make a few adjustments. For every program that needs to communicate two ways such as messaging/file exchange programs, multiplayer network games like DiabloII we need to "Allow Server." To change settings just right mouse click the desired program and select the option you desire under the Internet group. The green check allows, the red X denies and the question mark means that it asks each time. You will see in the screen shot that we allowed both Internet and Allow Server for ICQ and AOL IM so that they can receive messages and file transfers from our friends and relatives. We allow our anti-virus software signature download component, AutoDownload to by-pass the lock so it may download virus signature updates at all times by checking in the box under "Pass Lock". You should force a signature download if you use a different package such as Norton or McAfee and give it the same "Pass Lock" permissions.

Figure 3

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

BlackICE:

The default install of BlackICE does not block any connection attempts to the PC, reports all activity but still blocks activity known as malicious hack attempts. We will increase the protection level and make modifications to allow the same program as we did for ZoneAlarm.

Once in BlackICE, we will go into Edit Settings under the Tools menu option. At this time we will not cover the particulars of why the settings are what are listed here. That will be covered under the troubleshooting applications section.

Settings (Figure 4): We need to alter the default BlackICE settings. The recommended level for casual Internet use is "Cautious" (10). This blocks most basic services such as incoming web connections, drive sharing etc from the network.

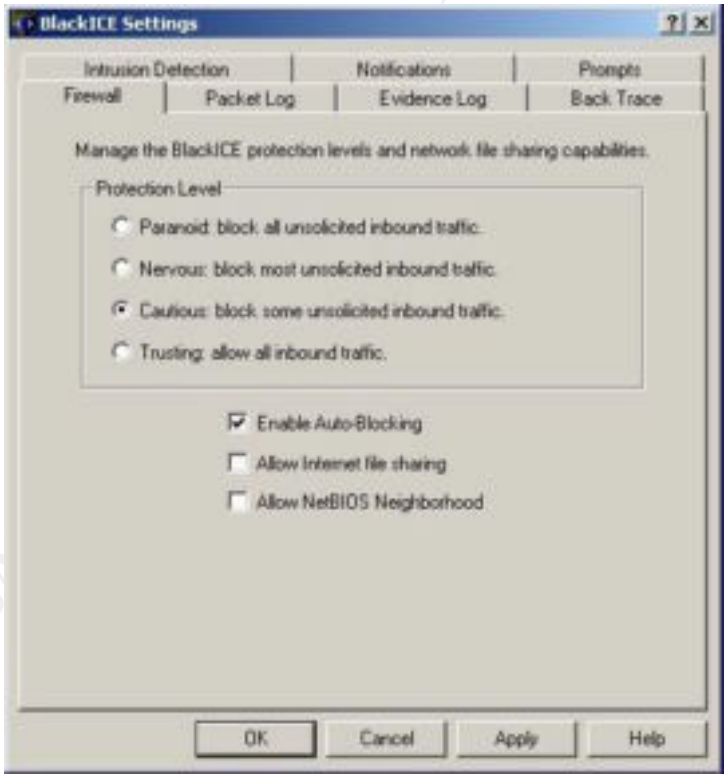


Figure 4

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Evidence Log (Figure 5): The next setting we change from default is to remove the check mark from Logging enabled on the Evidence Log tab. It is unlikely the normal home user would ever work with such logs and they would only continue to consume disk space over time.

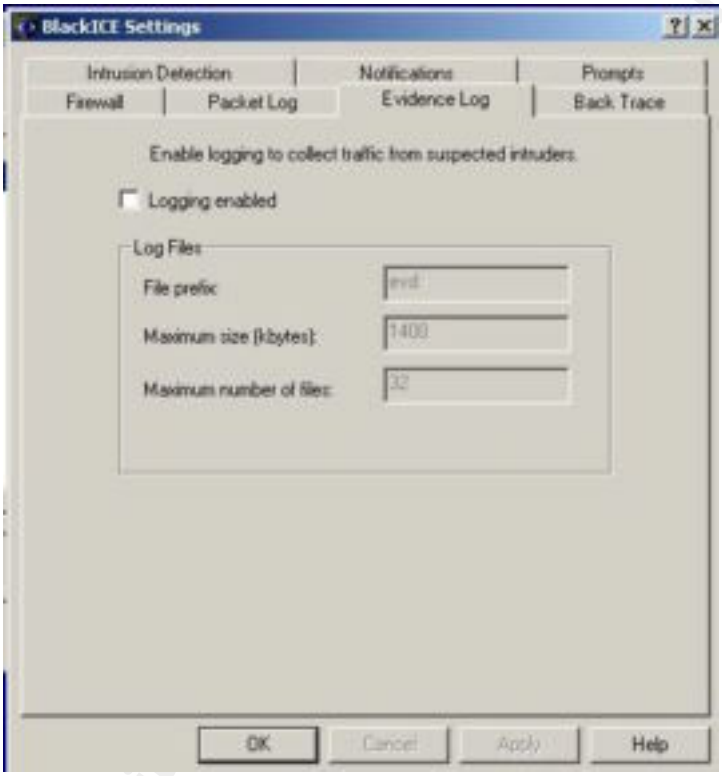


Figure 5

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Notifications (Figure 6): The last changes in the settings area occur on the Notifications Tab. We remove the Audible Indicator so we do not listen to beeps every time someone scans our system. We bump the visible indicator up to critical and serious alerts, which are red and orange coded. The final adjustment on this tab is to enable Update Notification checking so BlackICE will auto-check for software updates similar to anti-virus updates.

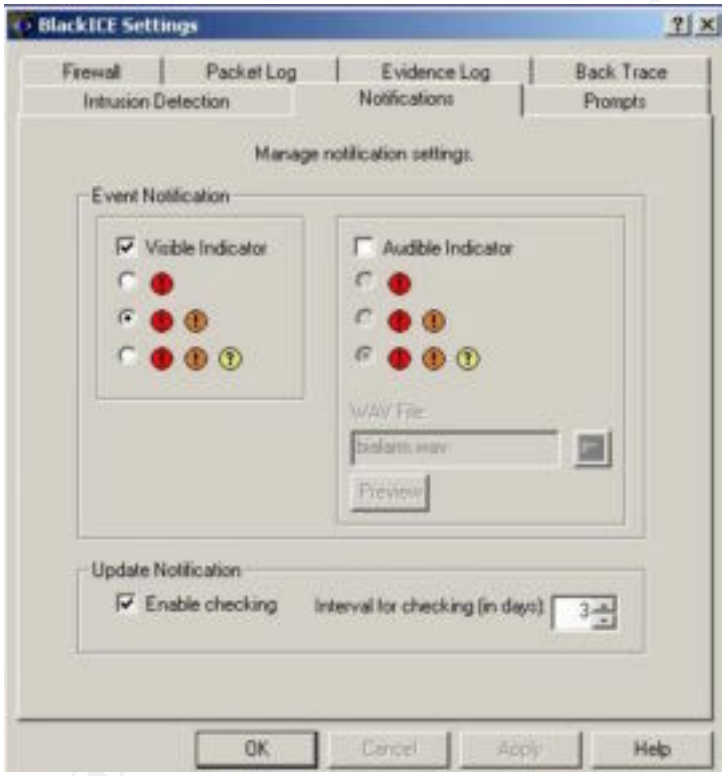


Figure 6

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Advanced Firewall Settings (Figure 7): Next we will find the AFS under the Tools option on the menu as we did to Edit Settings. This is where we will add modifications to allow AOL IM, ICQ and DiabloII connections. We want to make sure we can send files and play games with our friends. Click ADD and match **Figures 8-10**. Be careful when making these settings; match the screen shots exactly. We do NOT want to check the Add Trusted Addresses Entry. This is how we allow traffic on the desired ports but still scan it for malicious activity.

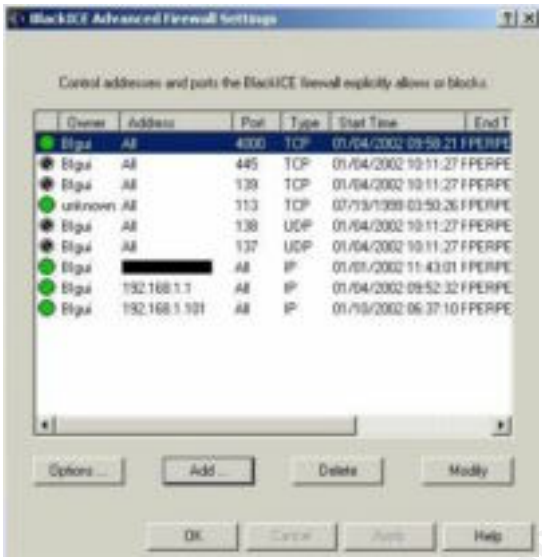
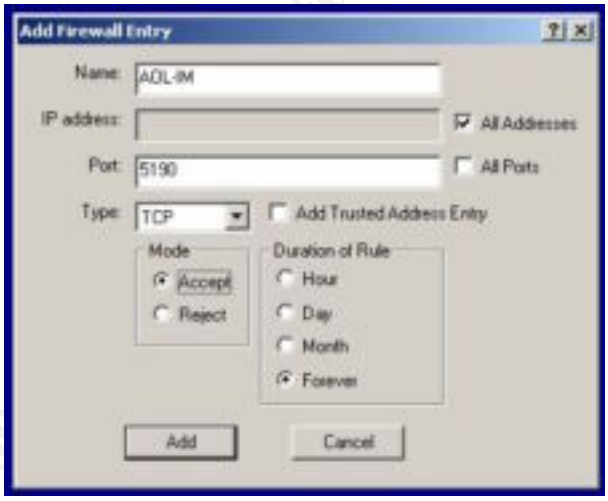
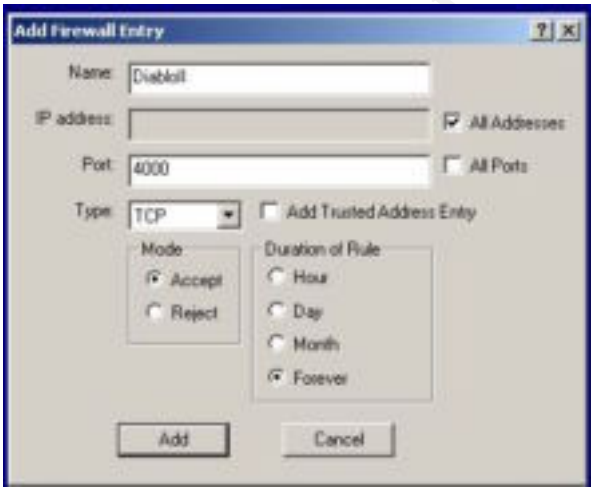


Figure 7: Advanced Firewall Settings



AOL IM (Figure 8): Click ADD and match the settings in the screen shot



DiabloII (Figure 9): Click ADD and match the settings in the screen shot.

ICQ (Figure 10): Click ADD and match the settings in the screen shot.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For ICQ we also need to modify settings within ICQ itself. We will go into the ICQ Preferences, Select Connections and adjust the Server and User Tabs to match **Figures 11 and 12**.

Figure 11

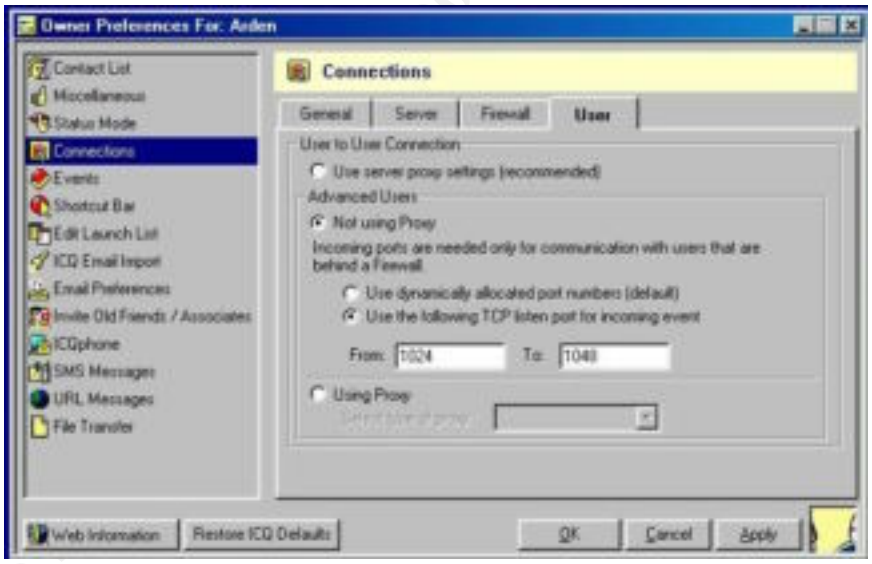


Figure 12

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Beginning Scenario Wrap-Up

We began with two home computers that dial up to the Internet often. They had no protection believing themselves safe since they did not have an always-on connection. We started with anti-virus software and ensured our machines were clean. Next we updated our software with the latest patches to close security holes known as vulnerabilities. Most hacking attempts target known vulnerabilities. However, we cannot always be sure that a new vulnerability will not be found before we can get the latest patches installed. This led us to install a personal firewall program. Modifications had to be made to the personal firewalls to allow for proper functioning of the programs we like to use. In the end, we have raised the bar malicious software and hackers have to clear without impacting how we use our systems.

We will now look at new issues that arise when the couple decides to expand to a home network and high speed Internet access.

Expansion Scenario: Going Broadband, Networking and Sharing Resources

Our couple quickly finds that sharing a phone line and the slow dialup speeds hinder their online fun. They are barraged with offers for cable and DSL high-speed access. These high speed connections can greatly enhance performance and if properly setup can be shared with a number of computers. The husband evaluates the options and chooses to go with a cable modem connection. He decides that they can share hard drives and the broadband connection by using a home network. The final twist is that he has bought a laptop for his web design hobby and wants to run it on a wireless connection to the home LAN and onto the Internet. We are fortunate that in the previous scenario we have already covered anti-virus and personal firewall issues. This leaves us to review our networking options for a broadband (i.e., cable or DSL modem) connection and adjust our existing personal firewalls to allow the added sharing of PC resources.

Expansion Step 1: Choosing/installing a router for sharing broadband

The husband of our duo embarks on the most common form of home computer research. He reads online reviews followed by a trip down to CompUSA and BestBuy for comparison impulse shopping. On the shelf we find two prominent products that offer a multi-port switch for a small local network, cable router to share the connection to the Internet and wireless support. The first is the Linksys BEFW11S40 EtherFast Wireless AP + Cable/DSL Router w/4-Port Switch (11). The other is the SMC SMC7004AWBR Barricade 4-Port 11Mbps Wireless Broadband Router (12). Both units have 128bit Wireless Equivalency Protection (WEP) encryption and offer a number of other security measures we will implement. We will again accept the documentation for default setup of all hardware in this scenario without recap in this paper.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SMC and Linksys share similar features. The installation and base configuration of these units are straightforward with their documentation. Earl Charnick provides a solid discussion on adjusting settings beyond the default in his paper, "Getting the Most Security out of the Linksys Cable/DSL Router." (13) These same changes can be adapted to the SMC unit. The unit we end up working with is the Linksys. This is due to various reviews, verbal recommendations of friends and the available documentation such as Mr. Charnick's paper. We also find that the SMC only offers three switch ports despite its name as a four-port router. They use the fourth port as the wireless interface. The built in print server is a nice option on the SMC but we have ink jet printers for our couple. The review found of the SMC7004AWBR on the website Practically Networked states the print server does not support bi-directional functions and at the time of review suffered a substantial 45% performance hit when using 128bit WEP encryption (14). We select the Cisco Aironet AIR-PCM352 Wireless PC Card for the husband's laptop PC. This is due to the integrated dipolar antenna that provides high quality reception for kicking back and web-surfing fromthe back porch hammock.

The installation of the Linksys Router is accomplished easily by following the included instructions. The scope of installing network cards and configuring a peer-to-peer network is outside this paper. We are immediately concerned with ZoneAlarm or BlackICE interfering with sharing of resources. ZoneAlarm requires only one change from the beginning scenario. In ZoneAlarm we need to enter the Security Tab, Click the advanced settings button and check the box next to our network card under Adapter Subnets. This makes any traffic for our LAN fall under the Local Security settings. BlackICE does have a checkbox for allowing what is called "Allowing Netbios Neighborhood." This is required if running TCP/IP for your home network and want the computer name to show in network neighborhood. Our diligent husband instead follows the instructions "Should I Use NetBeui?" in the Practically Networked How To section (15). This allows our couple to share resources without risk of exposing them to the Internet. We do not recommend these changes to a company laptop used for Virtual Private Networking (VPN) Internet access to work. The corporate computer support staff might take issue with the changes.

Expansion Step 2: Adding "wireless" to the laptop

The final component to our expansion scenario is the wireless portion. Robert Sprauge's paper "Cisco's Aironet 350 – An Enterprise Level Security Solution" gives us a clear definition of SSID, WEP and MAC based Access Control Lists (16). The Linksys wireless router currently supports SSID which lets us give the wireless network any name we want. It also supports WEP encryption of transmission across the wireless to secure our home wireless. Linksys has a solid reputation for releasing updates to the router firmware software every few months. We will hopefully see the addition of MAC based ACLs come later. MAC based ACL means that we would be able to tell the router to only allow specific network cards to connect via wireless.. Mr. Sprauge's paper has excellent references on wireless and its security issues for further reading. During setup and testing we found that having a 2.4GHz cordless phone base station in close proximity to the Linksys wireless router jammed the wireless network when the phone was in use. This required relocation of the phone base station.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

We first need to configure the wireless portion of our Linksys router, **Figure 13**. We select the wireless network name (ESSID) as "HomeNet." This identifier may be anything but must be consistent between the wireless router and the wireless network cards that talk to it. Mandatory WEP encryption is selected to help secure our transmissions and connection to our network. We generate a 128 bit encryption key by clicking the "WEP Key Settings" button and entering a pass phrase, **Figure 14**. This key will have to be entered into any wireless computer that will connect to our network.

Figure 13

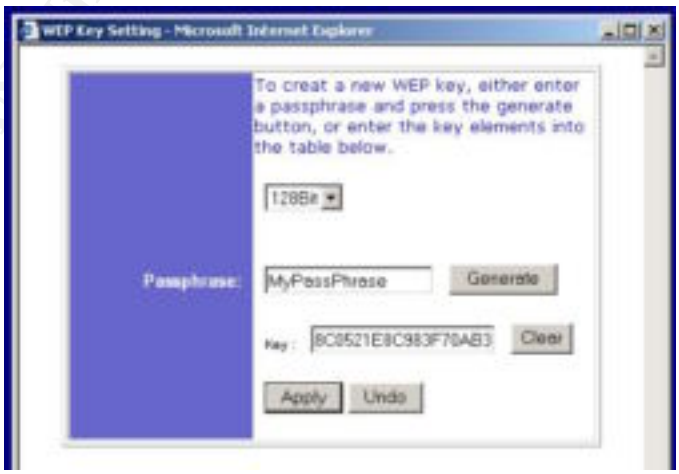


Figure 14

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The final portion of the Linksys configuration is in the Advanced-Wireless screen, Figure 15. We match these settings to be most compatible with the default settings of the Cisco Aironet 350 network card.

Figure 15

The Linksys router and wireless setup has been completed. We will accept the installation instructions for the Cisco Aironet 350 card are sufficient and will not repeat them here. The latest version of the 350 Client Configuration Utility is 5.01 at the time of this writing, **Figure 16**. This has much improved wireless profile support for moving between different wireless networks such as work and home. We click the "Profile Manager" so we may configure a "HomeNet" setting, **Figure 17**. Clicking "ADD" we configure our "HomeNet" by matching the settings to **Figures 18-20**. We use the WEP key we generated in **Figure 14** to enter the proper code for the Cisco Aironet 350 card in **Figure 20**. The laptop will join our network when we have completed these settings.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

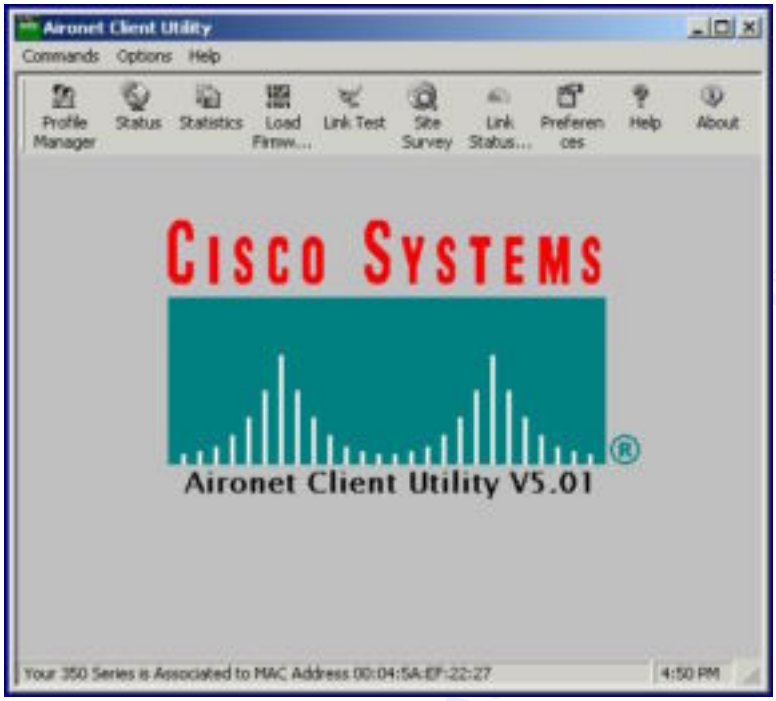


Figure 16

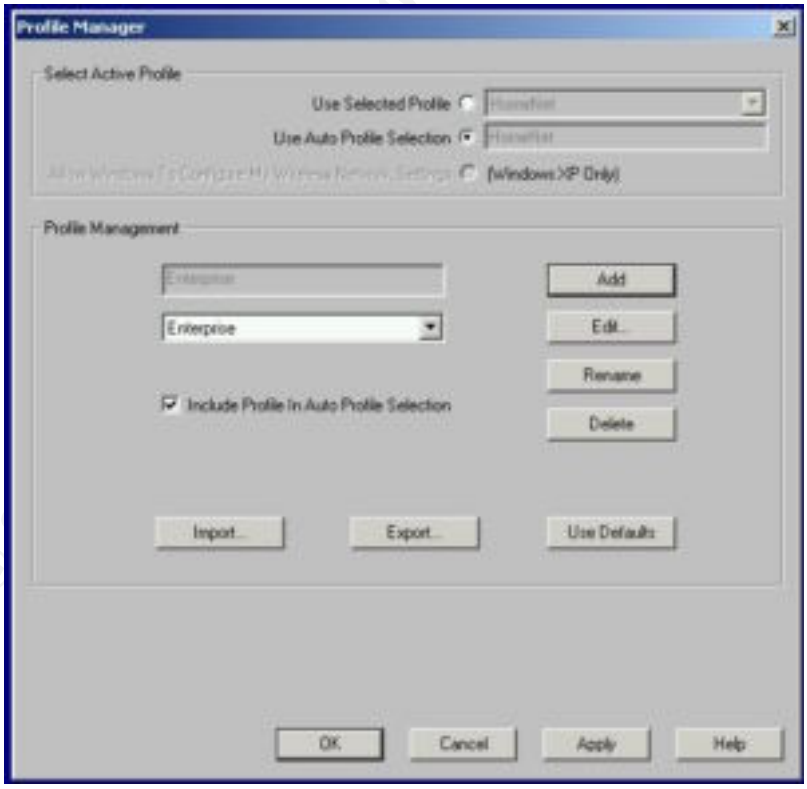


Figure 17

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

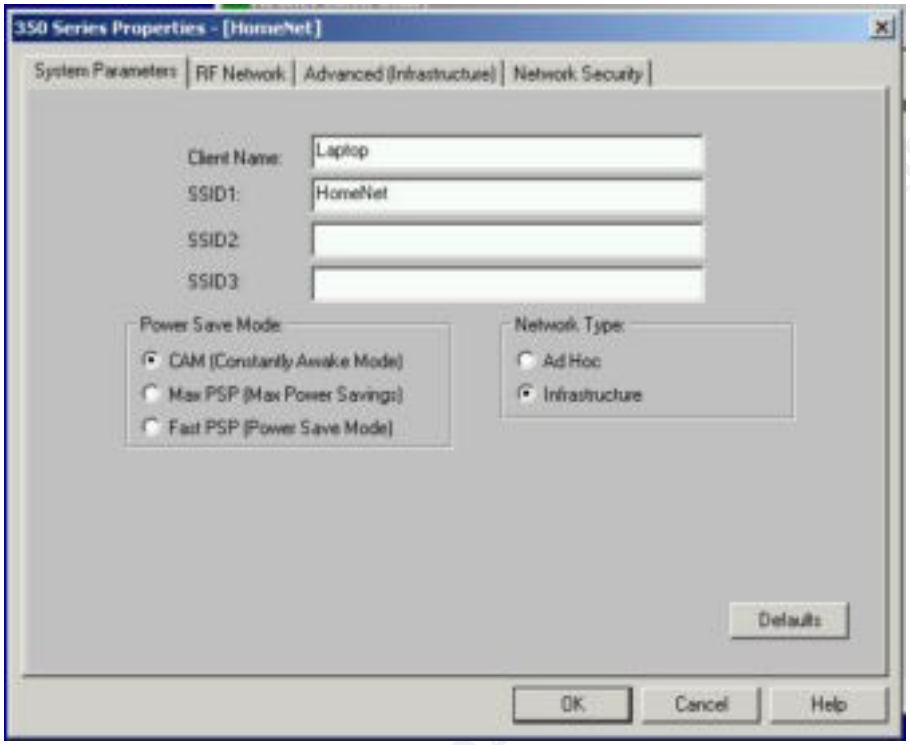


Figure 18

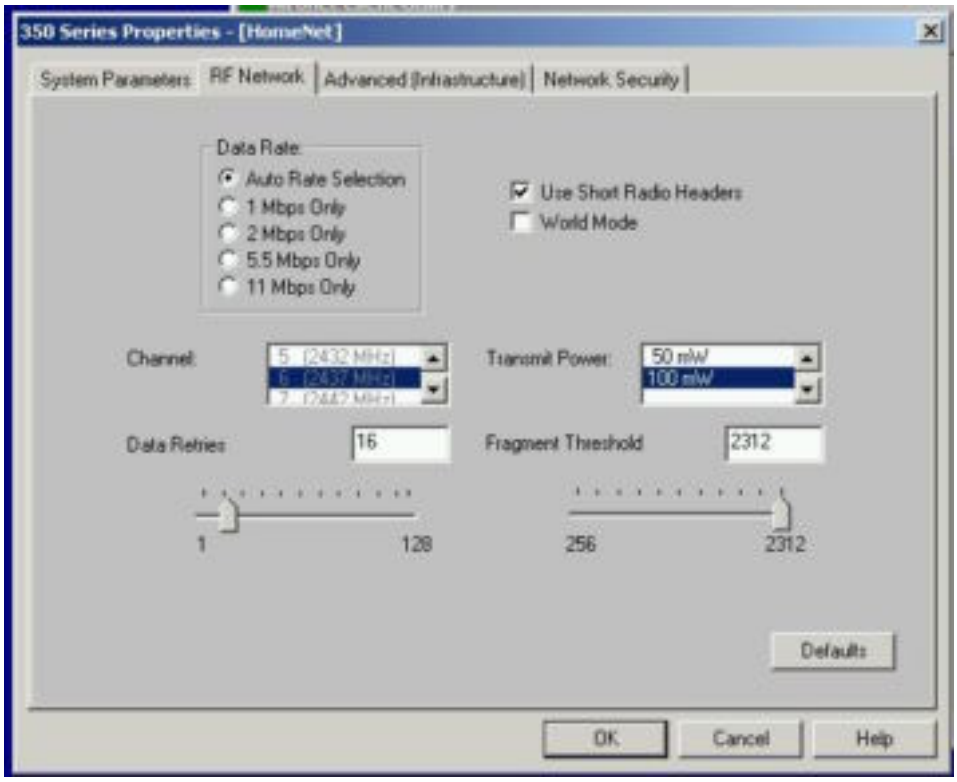


Figure 19

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

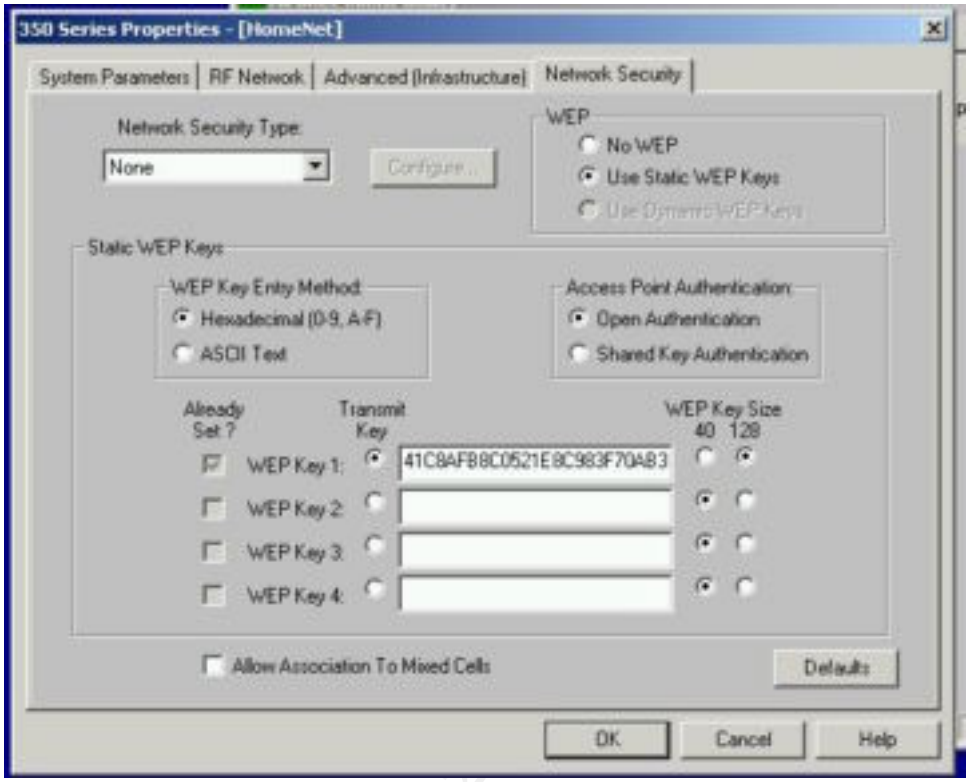


Figure 20

Expansion Scenario - Hardware Wrap-Up

We were fortunate that our couple had already established clean and secured computers in our beginning scenario. This enabled us to quickly build on the foundation when adding our cable modem with router and wireless connectivity. One might think keeping the personal firewalls would be redundant since we have added the router. The addition of the wireless with measures for security still could result in someone gaining remote access to our LAN. The personal firewalls and using NetBeui for local resource sharing further maintain our peace of mind. Our couple now also finds virus updates and patch maintenance for Windows and other applications are much easier to do the high speed downloads. In some cases staying up to date on patches may have become lax due to the slow dialup speeds. This is now an opportunity to maintain our systems with much less pain and patience. The subject of pain and patience leads us to the next topic. The now proud husband has his bubble burst when he finds ICQ file transfer and DiabloII network gaming have ceased to function.

It's time for some troubleshooting.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Troubleshooting Applications:

We find that any applications that connect directly between computers across the Internet cease to function properly. The programs have to be able to "hear" requests for connections from the Internet. The installation of the router has given us a level of security because it blocks all such traffic by hiding our listening software. DiabloII and ICQ can no longer hear our friends outside our LAN. The router has to be told to forward the things it hears to a specific PC in our LAN. This is called port forwarding. Using port forwarding causes the router to send all traffic for a given port to a specified computer. This is why we left ZoneAlarm and BlackICE on our PCs. We can open up certain ports to the outside world on the router while still maintaining layers of security inside. We have no reason to find this setup intimidating. In fact, we have done a similar sort of thing before. You can refer back to the screen shots under BlackICE where we specified the advanced firewall settings. We will collect some information then start with the simpler of the two problems.

We will need to know the network address of the computers on the network. This IP address is what we will tell the router to let ICQ file and DiabloII traffic through from the Internet to the correct PC. The quickest way to see all PCs and their IP Address on the network is to go into the router web interface, DHCP Tab then the DHCP Clients Table Button, **Figure 21**.

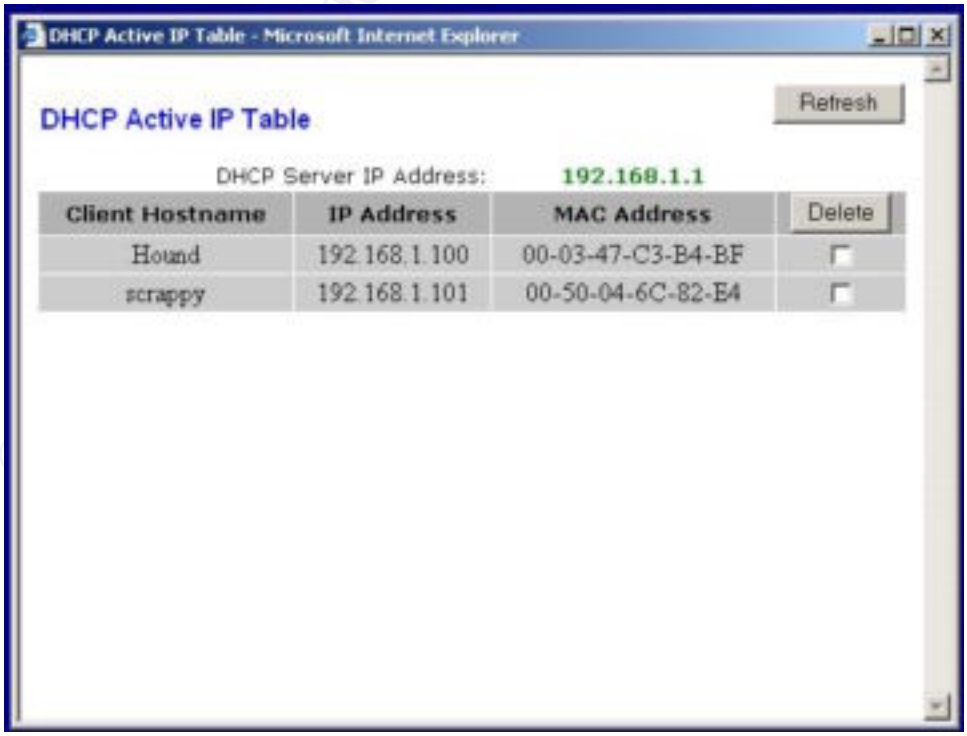


Figure 21

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

We can then look for a machine's address by the name we gave it in its network properties. We use this address when telling the router to Port Forward traffic to certain machines. The SMC router has one feature the Linksys has yet to add. This is called DHCP reservation or Fixed Mapping in the SMC documentation (17). You can tell the router to hand out the same IP address to the same machine using the MAC address every time it comes online. This prevents machines from getting a different address than we use in the port forwarding. We chose to use the Linksys router so we can either leave our machines on all the time so they do not risk changing addresses or we can switch to static. Microsoft Technet has a brief article on configuring a static IP (18). You will have to investigate this if you use the Linksys and turn off your computer or reboot your computers frequently to avoid having to change the settings we will make in this section. For this example we are accepting that both PCs remain on all the time to avoid changing IP addresses after being shutdown for periods of time. Hopefully Linksys will later release an update to the router firmware that will give us the ability to reserve IP addresses by MAC address as the SMC does.

DiabloII will require only one port to forward. This will be port 4000 TCP. TCP means it is a two-way conversation between computers. We go into our router web management page. Select Advanced then go to the Forwarding Tab, **Figure 22**. We then adjust the screen to match the below screen shot. We can make the ICQ settings now, but are currently discussing only the DiabloII issue. Note we have to forward the port to just one PC that runs our DiabloII game. Now we will Apply the settings and will find DiabloII network gaming works again with our friends. This is because we pass the information to our gaming PC and have already allowed DiabloII to work with our BlackICE and ZoneAlarm in the Beginning Scenario. How we found out DiabloII uses port 4000 will be seen when we cover the problems with ICQ file transfer.

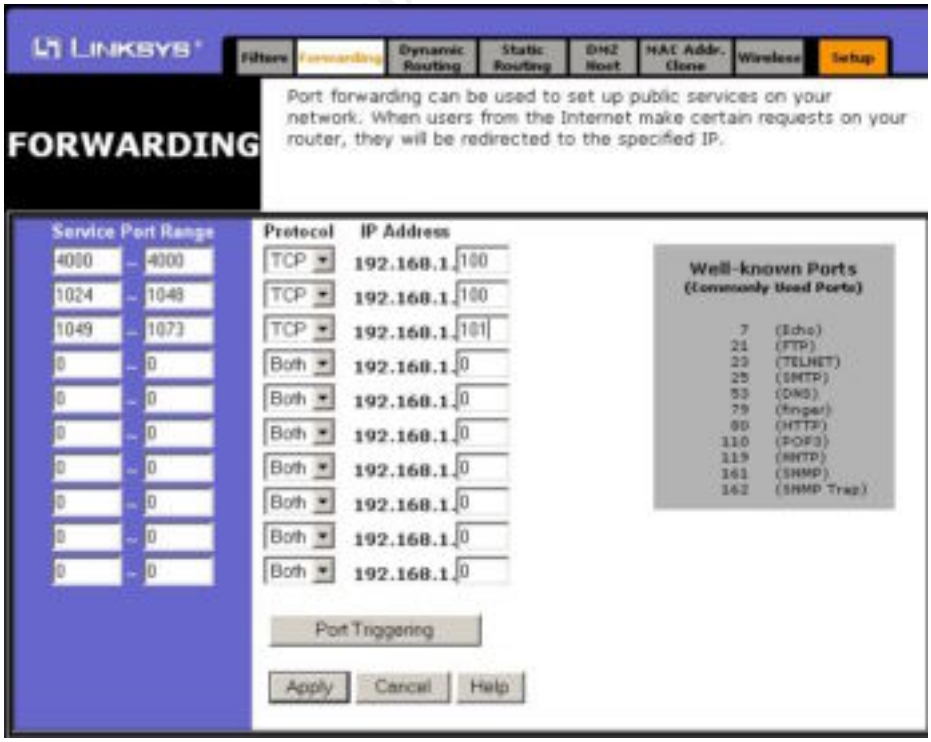


Figure 22

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ICQ turns out to be complicated issue to fix. We would have stumbled onto this back in the Beginning Scenario if we had made BlackICE run at a Firewall Protection Level higher than "Cautious." We adjusted port listening settings within the ICQ program itself. If ICQ were behaving as expected then the above port forwarding would work. Testing ICQ file transfer after this adjustment to the router turns out to still fail. We have told ICQ what ports to listen on. We have told BlackICE to pass those ports and ZoneAlarm to allow anything associated with ICQ. To find out what is going on we have to turn to the logging functions of the router. We can either go straight into the web interface for the router or use a wonderful free program called "WallWatcher" written specifically to receive logging information from a Linksys router (19). Instructions for downloading, installation and configuration of the WallWatcher program and Linksys router are on the program's web site (http://www.wallwatcher.com/). If you choose another router product such as the SMC unit just look for similar in and out log review functions in its web control interface. Note if you fail to receive information in WallWatcher it will turn out to be BlackICE and/or ZoneAlarm blocking the data from the router. ZoneAlarm will just ask if WallWatcher is authorized to connect to the network. In BlackICE, you can either trust the router's IP by right clicking it when entries appear for it in the events and choosing "Trust Only" or you can use the Advanced Firewall Settings to Allow the single UDP port 162 from the router IP with a duration of Forever.

We have installed WallWatcher and have ICQ running. The intrepid husband enlists the testing assistance of his son who is also running ICQ. The son provides his father his Internet IP and sends a file to his father. The father watches WallWatcher (the inbound logs). He sees an inbound entry for that IP with a local port (the port destination on the father's machine) outside our range of 1024-1048. This tells us ICQ is sending on any port it wants without asking the receiving machine what port range it is listening on. The result is no file transfer occurs inbound to our new network. Referring back to the screen shots where we told ICQ the ports to listen on we find no place to specify the sending range. Nothing we do can solve this problem with ICQ short of opening up all ports on the husband's PC. This totally negates the security layer we have built. The goal is to provide the computer user with security that does not take away from the usability. In this case we are painted into a corner. It is fortunate in this situation that one other option exists. The husband can still use ICQ services to talk and exchange files, but it requires changing the program from ICQ to a program called Trillian (http://www.ceruleanstudios.com/) (20). We will not go into detail on this software but you should specify the same listening port range as we did in ICQ, **Figure 23**. See the screen shot below. It turns out Trillian is able to send to receiving end's specified port range. We get to have our cake and eat it too with file transfer and maintaining our security layers. As a side note, I do feel responsible as the author of this paper to direct your attention to the ruckus in the computing community regarding "alternate IM clients". "Why AOL is right to turn away a million Trillians", by David Coursey the Executive Editor of AnchorDesk on Zdnet (21).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

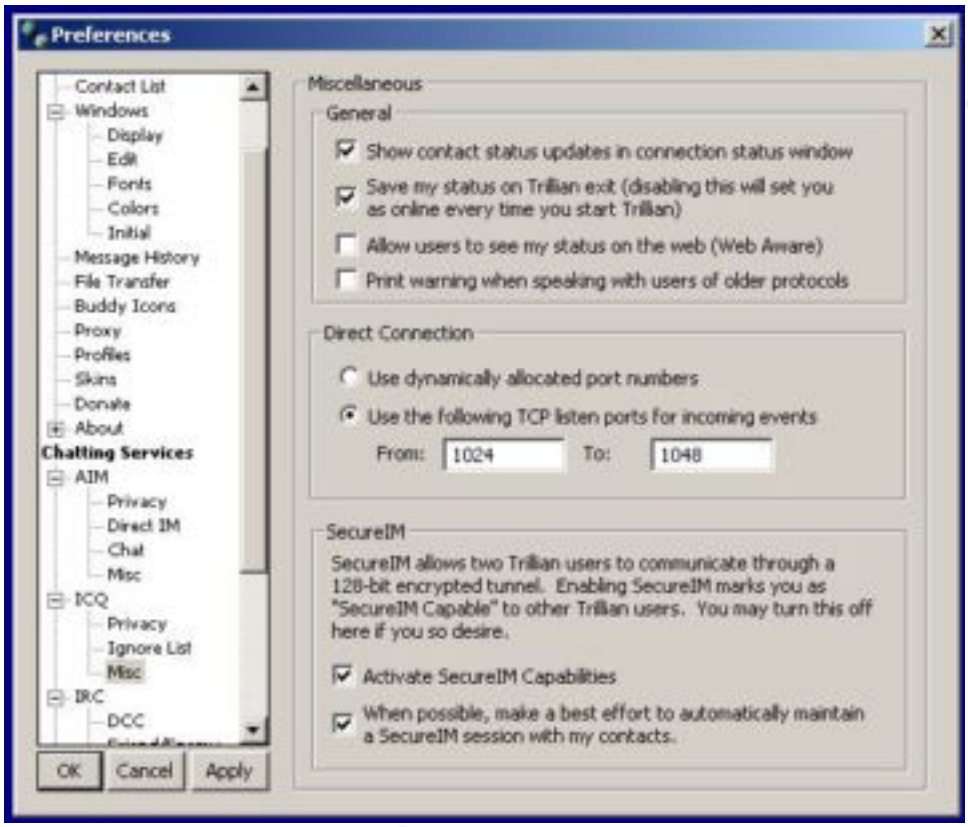


Figure 23

One last issue with ICQ is that if we wish to have this functionality on multiple machines each machine has to have a port range to listen on. Refer back to the Port Forwarding screen shot and there is an entry for ports 1049-1073 to IP 192.168.1.101. The adjustments for this additional machine would have to be made to BlackICE as we originally did for 1024-1048 in the Beginning Scenario. The reason is that to the Internet we are sharing one IP address. This address has one port range associated with it. The router is where we point different ranges to different computers. Then we adjust that particular machine's personal firewall and software such as Trillian to the port range we specify so no overlap occurs to confuse our systems. We specified port 4000 for DiabloII without explaining where that information came from. If we apply the troubleshooting technique of watching the inbound router logs we can find that when a friend tries to connect to a hosted game on our machine we see inbound attempts on port 4000 every time. Another good source of port usage information can be found at http://advice.networkice.com/advice/exploits/ports/default.htm (22). Foundstone provides an excellent free tool called FPORT under the Intrusion Detection category. It is a command line tool that reports network related programs running under windows and what ports they are listening on (23).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Summary:

A healthy dose of paranoia when dealing with security is encouraged. Any time security measures are installed or changed we should test the systems to ensure integrity. Steve Gibson's website http://www.grc.com provides a self-testing toolset to see the results of our work. The most popular tool is his Shield's Up (24). To test anti-virus software the European Institute for Computer Anti-Virus Research (EICAR) has produced a test file that contains a text string that any package written to industry standards should detect for testing purposes (25).

It is important to remember every layer of security we implement requires adjustments to allow the services we wish to use. This is why running BlackICE under ZoneAlarm on the husband's computer, which was all behind the router caused much aggravation developing the LAN behind this paper. The end result is that we raised the bar malicious hackers and software must overcome to penetrate our home LAN while providing all the services our couple desires. We installed and configured anti-virus software, updated software and OS patches, personal firewall, cable/DSL router and learned a few new tricks. Congratulations, this is the information security concept of layered defense in depth; we have now successfully applied it to our home network.

Reference Resources

1. Computer Associates Virus Information Center. "Win32.Goner.A Worm." URL: http://www3.ca.com/solutions/collateral.asp?CT=65&ID=1212
2. Willert, Jon. "Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters" SANS Reading Room. October 22, 2001. URL: http://rr.sans.org/homeoffice/best_practices.php
3. McDougall, Bonnie. "Personal Firewalls – Protecting the Home Internet User" SANS Reading Room. August 17, 2001. URL: http://rr.sans.org/firewall/home_user.php
4. Vamosi, Robert. "Nimda hits both Windows PCs and IIS systems." September 18, 2001. URL: http://www.cnet.com/software/0-5067630-8-7215675-1.html
5. Hayes, Frank. "Swat the Buffer Bugs" January 21, 2002. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO67572,00.html
6. Hopper, D. Ian. "Hole Found in Net Security Program" February 8, 2002. URL: http://dailynews.yahoo.com/h/ap/20020208/tc/computer_security_3.html
7. Internet Security Systems. "The Evolution of Intrusion Detection Technology" August 29, 2001. URL: http://www.networkice.com/docs/ids_evo.pdf
8. Elliot, Curtis. "ZoneAlarm – A Free Solution for Home Security" SANS Reading Room. October 1, 2001. URL: http://rr.sans.org/homeoffice/zonealarm.php
9. Zone Labs Zonealarm. "Support Documentation" URL: http://www.zonelabs.com/services/support_za_zap.htm
10. Internet Security Systems. "Support Documentation" URL: http://www.networkice.com/support/documentation.html
11. Linksys 4-Port Wireless Broadband Router Specifications URL: ftp://ftp.linksys.com/datasheet/befw11s4ds.pdf

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

12. SMC Barricade 4-Port Wireless Broadbrand Router Specifications URL: http://www.smc.com/drivers_downloads/library/7004AWBR_DS.pdf
13. Charnick, Earl. "Getting the Most Security out of the Linksys® Cable/DSL Router" SANS Reading Room. November 30, 2001. URL: http://rr.sans.org/homeoffice/linksys.php
14. Higgins, Earl. "Reviews: SMC Carricade Wireless Broadband Router [Version 'A']" June 13, 2001. URL: http://www.practicallynetworked.com/reviews/smc7004awbr.asp
15. Unknown Author. "Should I use NetBeui?" Practically Networked Web Site URL: http://www.practicallynetworked.com/sharing/netbeui.htm
16. Sprague, Robert. "Cisco's Aironet 350 – An Enterprise Level Wireless Security Solution" SANS Reading Room. September 28, 2001. URL: http://rr.sans.org/wireless/aironet350.php
17. SMC Corporation. "SMC Barricade Wireless Broadband Router Users Guide" 2001. page 22.
18. Microsoft Corporation. "Configuring Static IP" URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/sag_TCPIP_pro_ManualConfig.asp
19. WallWatcher for LinkSys Cable-DSL Router URL: http://www.wallwatcher.com/
20. Cerullian Studios. "Trillian IM Client" URL: http://www.ceruleanstudios.com/
21. Coursey, David. "Why AOL is right to turn away a million Trillians" February 1, 2002. URL: http://www.zdnet.com/anchordesk/stories/story/0,10738,2844439,00.html
22. NetworkIce (www.networkice.com) database of TCP/IP port assignments URL: http://advice.networkice.com/advice/exploits/ports/default.htm
23. Foundstone. "Free Tools" URL: http://www.foundstone.com/knowledge/free_tools.html
24. Gibson, Steve. "Shield's Up" URL: http://www.grc.com/
25. The European Institute for Anti-Virus Computer Research. "EICAR virus test file" URL: http://www.eicar.org/anti_virus_test_file.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to {Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS