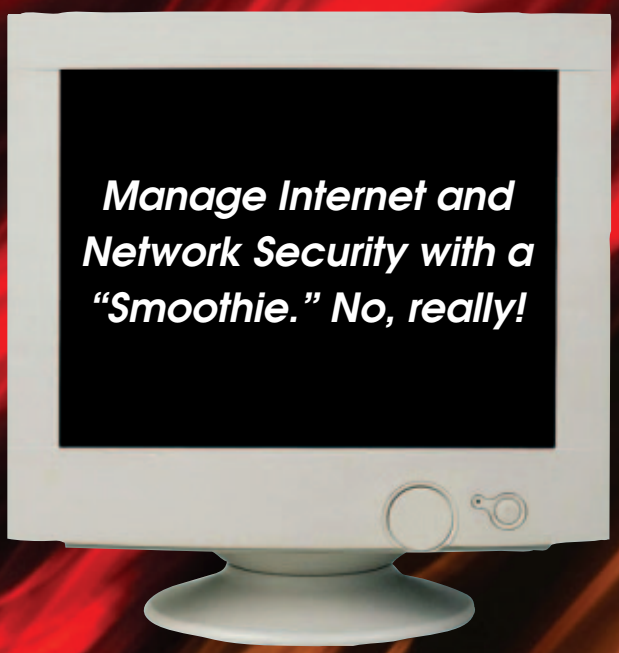
Freeware Linux Hardware Firewall HOW-TO: HAVE A "SMOOTHIE"



by David Geer

We're about to cover parts and instructions for creating your own Linux hardware firewall using an old box (computer) and the SmoothWall Express 2.0 firewalling software package.

The SmoothWall firewall is an ongoing, Linux-based firewall project that we can expect to be updated and improved on over time. A Linux platform for a firewall is important for several reasons. When coded and tested with expertise and great care, Linux is an extremely stable platform with true multitasking capabilities — more than robust enough to handle firewalling duties. Linux is also still far enough out of the mainstream that few crackers are writing viruses or thinking up attacks against it. Windows-based attacks should not get through nor can they harm the Linux code that makes up the firewall. It is also free because it is open source. And, in this economy, you know everyone loves free!

THE MOST IMPORTANT PART

In the larger picture, what you need most for this build is a healthy concern for computer security. I thought I had security holes beat with software: a software firewall on my laptop itself, anti-virus software for viruses and worms, and anti-spyware for Trojans and a long list of malware. I was wrong. My computer is more invisible to the Web than ever (as tests determined) thanks to what SmoothWall lovers call "the Smoothie."

If you have these other protections and have still gotten malware, or if you felt someone was playing on your box or stealing information, you will appreciate this useful yet inexpensive project. If you want to start out with better than average firewall protection, or want to add a layer to your current security for added peace of mind, this package is for you, too.

As with any good set of instructions, read them entirely before preparing to start your project.

You ready? Okay, then. Let's get 'er done!

PARTS — HARDWARE, SOFTWARE, DOCUMENTATION

You will need an old computer that meets the following minimum system requirements.

- A Pentium compatible processor, 150 MHz or faster
- 32 to (ideally) 64 MB RAM or more
- 2 GB or higher IDE hard drive
- A CD burner (mine was a rebated $20 Polaroid BurnMAX40 CD-R/CD-RW that I installed myself)
- I recommend CDBurner XPPro software, which is free, but you can use whatever you like.
- Video card (during install only)

- Monitor (ditto)
- Keyboard (ditto)

You will need two supported Network Interface Cards (NICs). (See documentation, coming; this is for setup with broadband, which I set up and tested successfully. Setup instructions for use with dial-up are in the documentation, but you'll still need much of what you'll read here to get through it smoothly.)

You will also need two Ethernet cables (Cat5 or better, Cat6, etc., are out now) — no mouse required.

Tools are required — to install a second NIC, you'll need the most basic computer tool kit or a good Phillips screwdriver the right size to take the cover off, etc.

Software is also required, which will need to be burned to a CD and a couple of floppies (Did I mention you need a floppy drive? Well, only if your old computer won't boot from the CD properly), and three PDF documents that can be downloaded from www.smoothwall.org The site also offers free support in the form of forums with very helpful folks posting and responding all over the place.

Here's my topology for this project, which in addition to my Internet service type, will affect how closely my steps and experiences will mirror what you need to do.

Don't get discouraged; between this article, the thorough documentation available from the SmoothWall site (we'll get to that, too), and perhaps some trial and error, you will get through it and come out the other side glad you took the time. You also will be preventing crackers (correct term for bad hackers) from coming in from the other, other side — of your Internet connection.

I connected the firewall to my internal network with the following topology: An ADSL router (some say modem, which isn't technically accurate) — a SpeedStream 5200 to be exact, set in router mode — connected to Alltel DSL service, was then connected via Ethernet to the SmoothWall firewall's first NIC card.

The "Smoothie" was installed on my old HP Pavilion XE736. Ethernet from the second NIC led inbound to my USR 5462 802.11g wireless router, into one of the LAN ports. This was so wireless would work but the router would function like a hub — passing data only. This made IP addressing easier (if you've not done IP addressing, fear not, we're going to guide you through it).

I could then connect via Ethernet back out of a LAN port into my Laptop NIC, or by Wireless to my USR 802.11g USB stick, model 5422. (If you're interested, the two come in a kit from USR, available at TigerDirect.com for about $20 after rebate. If you don't plan to go more than 50 feet from the wireless router, it's an easily configured bargain.)

Oh, and the laptop is an IBM ThinkPad R40 I got from the clearance section at the IBM site (when IBM still owned the division producing the product).

PROCEDURE

For faster downloading, go to www.smoothwall.org and get the SmoothWall Express 2.0 (final, not beta) and the documentation separately by clicking download, then the larger SmoothWall download link, and then where it says manuals must be downloaded separately.

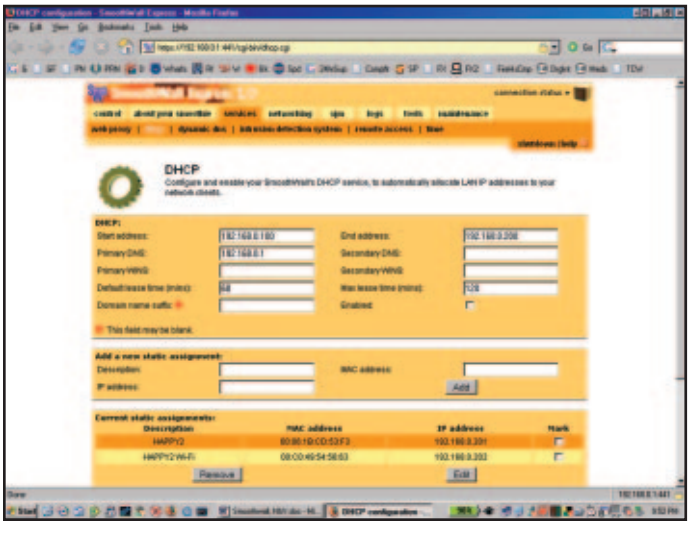
Burn the software .ISO image to a good CD-RW in such a way as to make it bootable, if possible. If not, you'll need to make and use the two boot floppies, as follows.

MAKING THE BOOT FLOPPIES

You'll need either your old computer or another one running Windows and a recent Web browser version to get what you need on floppy for the procedure. Don't run the installation on a computer other

■ HERE YOU CAN SET UP A WEB PROXY TO GET AROUND THE OFTEN ATTACKED PORT 80.

■ HERE YOU CAN SET A RANGE OF IP ADDRESSES TO SERVE TO YOUR COMPUTER OR COMPUTERS, OR DISABLE DHCP AND SET UP STATIC IPs.



■ HERE YOU CAN CHECK TO BLOCK ICMP PINGS, IGMP PACKETS AND MULTICAST, IF YOU SO DESIRE.

■ HERE YOU CAN DOWNLOAD UPDATES, UPLOAD THEM TO YOUR SMOOTHIE, AND THEN HEAD OVER TO SHUTDOWN TO REBOOT.

than your old box. To load SmoothWall, you will need to wipe and use the entire drive. This is done for you, but you don't want it to happen on a computer not entirely set aside for the SmoothWall.

Insert the first of two fully formatted floppies. Insert your new SmoothWall CD, browse, and find the RawWriteWin file in the /dosutils directory. Open it and select the Write tab. Browse to the /images directory and select bootdiskone-2.0.img using the Image file field. Click Write. Don't wash or rinse, but do repeat for the second floppy, loading it with bootdisktwo-2.0.img.

■ Smoothie How-To's Parts Where-To

YOU MAY HAVE OR SHOULD BE ABLE TO PICK UP A WORKING COMPUTER THAT MEETS THESE SPECS FOR NOTHING THESE DAYS:

- A PENTIUM COMPATIBLE PROCESSOR, 150 MHZ OR FASTER.
- 32 TO (IDEALLY) 64 MB RAM OR MORE.
- 2 GB OR HIGHER IDE HARD DRIVE.
- A CD BURNER (YOU CAN GET ONE FROM TIGERDIRECT).
- I RECOMMEND CDBURNER XPPRO SOFTWARE, WHICH IS FREELY AVAILABLE AT **WWW.SNAPFILES.COM**
- VIDEO CARD (DURING INSTALL ONLY) (ANY COMPATIBLE WITH YOUR PC FROM TIGERDIRECT OR USED).
- MONITOR (DITTO AND DOUBLE DITTO).
- KEYBOARD (DITTO ON THE ... WELL, YOU GET THE IDEA).
- TWO SUPPORTED NETWORK INTERFACE CARDS (SEE DOCUMENTATION, THEN GET 'EM FREE FROM OLD COMPUTERS, OR BUY THE CHEAPEST YOU CAN, OR TRY TIGERDIRECT).
- TWO ETHERNET CABLES (CAT5 OR BETTER, CAT6, ETC., ARE OUT NOW, TRY TIGERDIRECT, OR WALMART OR OFFICEMAX, ETC.).
- MOUSE IS NOT REQUIRED.

INSTALLING NICS QUICK TUTORIAL

Make sure you know the type of each NIC card and that it is on the compatibility list in the documentation. If it's not on the list, it may work anyway, but better to plan ahead.

Touch metal to discharge the static that could fry your computer. Take the screws out of the back. Take the cover off. Touch some external metal on the back of the computer periodically to discharge static shock. Take your nice new PCI or ISA slot NIC card(s) and pop them gently into the place they belong.

The PCI slot is smaller, and so is the card. Look closely at both. You'll figure it out easily enough. Get it in the slot firmly, but don't go crazy. Screw it into place where the screw hole obviously is at the top. Cover back on, yet? Well, hurry up, let's go!

INSTALLING SMOOTHWALL

From here, you must be on the old computer that you plan to use for

your new hardware firewall. You must have a keyboard and monitor connected to it. Boot from carefully labeled floppy one, press Enter to continue, and then feed your computer the second floppy when asked and hit Enter.

Select OK on the next screen (I already had the CD in when I did this). Alt/Tab or arrow keys to CDROM and tab to OK and Enter. It will say insert the CDROM. Do so if not done yet and hit OK. Hit OK again to partition and reformat. Select OK one more time to let the install program know that you're really, really sure (you are, right?).

You will see it making the root system and then get another screen. Now it's time to Probe (for a NIC for your green interface, that is). This is the NIC that faces in toward your local network. Select Probe, then OK or Skip to find and select the NIC you want to use for your green interface.

The name the install software gives should be close to what you know your NIC is so you should be able to figure it out. Select OK again to use that NIC. Now you need to enter the IP address and subnet mask. As the IP address, you could safely put 192.168.0.1 for a similar configuration to the one I used. The network mask number needs to be 255.255.255.0.

Unless you are familiar with IP addressing, use these exact numbers and don't forget the dots in between. Select OK and it will install the necessary files. After that, you'll be asked to remove the CD and floppy. Do so and select OK.

Select No when asked if you want to restore the configuration from a previous install backup floppy. We'll make the floppy later. For keyboard mapping, select US or your keyboard mapping. Select OK. Use the default SmoothWall hostname and select OK.

If your ISP requires you to use a Web proxy on their network to get the SmoothWall Express updates, find that hostname and port number now and enter those here. Tab to and select OK, whether you need that information or not.

Tab to disable ISDN and then to disable ADSL for this setup. (This ADSL setup on screen is for USB DSL only. If you use ISDN or ADSL with USB, tab through each field and make the most intuitive selections after going over the Quick Start, Install, and Admin PDF documents carefully.)

With our configuration, we are at Network configuration type now. Select that by hitting enter. Arrow to Green + Red and then select OK. Arrow to Drivers and card assignments and select that. Select OK. Probe again. Select OK for the other NIC on your computer. Assign it to Red and tab to and select OK. Select OK again.

Arrow to address settings. Arrow to red. Select OK. Arrow to DHCP (Dynamic Host Configuration Protocol — automates assigning dynamic Internet Protocol [IP] addresses) and hit the space bar to select it. Leave SmoothWall host name as-is. Tab to OK, leaving the IP address and network mask blank or taking out whatever is there by tabbing there and backspacing. It is best to have everything already plugged in when you do this. Select OK.

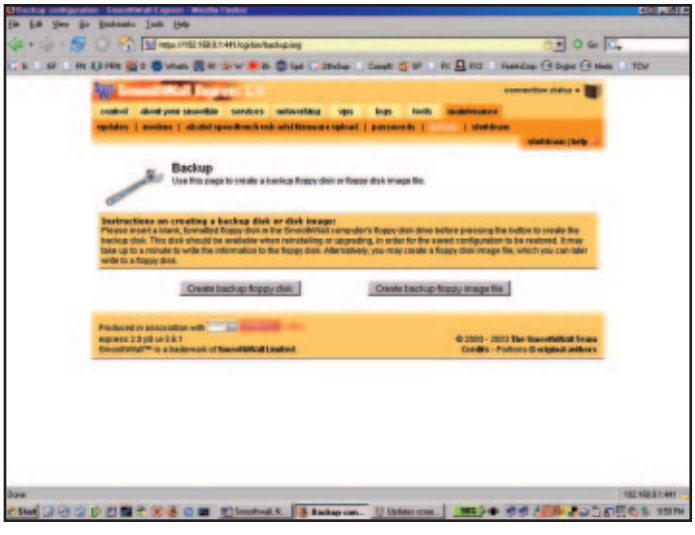
Arrow to and select DNS and Gateway settings. You can leave these blank. Select OK and Done. Make sure to be connected as in the topology described earlier. You can easily bypass the Wireless Router if you don't have one and connect straight to your laptop or desktop computer.

Select DHCP server configuration. Hit space bar to enable. For the IP address range, the first IP address should be 192.168.0.100, the same but ending in 200 for the next one, primary DNS, served from the firewall should be 192.168.0.1. No secondary DNS or domain name suffix. The default lease times should be okay. Select OK.

Select root. Select a password and OK. The UID is root and this is your password. Write it down or memorize it in case you need to use the keyboard and monitor again directly on the box to log in to make changes.

"In the larger picture, what you need most for this build is a healthy concern for computer security."

■ HERE YOU CAN CREATE A FLOPPY BACK-UP OF YOUR SETTINGS.



Do likewise with setup's UID and Admin's UID. Make all passwords different and unique. Select Quit. If you need to get into setup again, have the keyboard and monitor attached, boot the firewall, and enter setup as your login and your password as your password. No dots appear for the passwords under Linux so you'll have to watch what you type or try again.

You should now be connected through the firewall to the Internet.

FURTHER SETUP VIA WEB INTERFACE (OPTIONAL)

Open up your browser and surf to https://192.168.0.1:441 to connect to port 441 on your Smoothie. To select anything from there, you will have to put in admin and your password in the dialog box that comes up. Here are the settings I use inside. Consider them thoughtfully for your setup.

Go to Services, Web Proxy, check Enabled and click Save. This sets the HTTP port to the proxy setting of 800 instead of 80. It fools some who target port 80 because it is usually wide open.

Go to DHCP. I disabled DHCP and put in static addresses for my NIC and my Wireless USB stick. Save at bottom.

Go to intrusion detection and check Snort and Save. You'll need to check it under logs to see what is attempting to get in.

Go to Advanced under Networking and check the three boxes that start with "Block ... " to be completely invisible to the outside world.

Go to Maintenance and updates and download and install per the instructions all updates starting with one and going through seven (or how ever many there are when you read this) and reboot the firewall after each individual update.

You can also go to backup and create the floppy for restoring configurations when you're all done. Those don't include the settings made only here in the interface, though.

TESTING

Once you can connect to the Internet and get into the browser-based interface to your new Smoothie, you are ready to begin testing your firewall. ShieldsUp (www.grc.com/x/ne.dll?bh0bkyd2) is a great place to start for checking FileSharing and Port vulnerabilities.

When you arrive at the site, click the Proceed button, and the Continue dialog button if it appears. Select the File Sharing button from the menu and then wait for the results. Your results should say that port 139 is invisible and that no NetBios connection could be made.

Scroll down and select the

Common Ports button. You should soon see results that say Passed. Scroll down to see that all your common ports are invisible to the Internet. Select All Service Ports. You will eventually see that the entire grid is green, showing that all service ports are invisible.

Scroll to the bottom of this page and you can check any 64 ports beyond the service ports, one grouping at a time, by selecting User Specified Custom Port Probe and following the clear and simple instructions you'll find there.

FUTURE

Check for updates, though they are rare. Check your logs and see who is NOT getting in. If any attempts are very clearly crackers, you can report them. ■