How To Build a Hardened Linux Firewall Under Your Control

A Simple Design Based Upon Off the Shelf Components, released as Open Source Hardware

Released 04 JUL 2012
Aaron Harper, CTO
Lobo Savvy Technologies, LLC
aharper@lobosavvy.com

Introduction:

Like many CTOs, I have trusted Cisco and it's subsidiaries with everything but the most sensitive data, betting the farm on the company's ethics and discretion. Due to recent events, illustrating a starling lack of ethics and value ascribed to their customer's privacy, I can no longer do so. For those of you who have not heard, consider the following article:

http://www.extremetech.com/computing/132142-ciscos-cloud-vision-mandator...

At this point all Cisco equipment must be considered suspect due to the corporate attitude and practices this event brought to our attention. It's not what was done, but rather how, and why.

Cisco, of all companies, should have known better. It really doesn't matter if someone steals a laptop, hacks in and grabs stuff from a server, monitors and decodes the packets coming into the public network, or hijacks a firewall for corporate control and data mining, the results are the same. Someone has information they do not need, nor have my permission to have. The truth is that Cisco must have known better, but has and obviously will break this trust for the right price.

In response, after a brief meeting to discuss the issue, the board of directors of Lobo Savvy Technologies, LLC decided to release a basic firewall design to the general public. This was done for three reasons:

1. If a business finds it necessary to remove Cisco equipment from their offices, a replacement is needed before the work can get underway.
2. The design is not our commercial offering, although it does share many of the same characteristics. It does us no harm to give this information away.
3. While many have known the power of Linux in a commodity PC used in infrastructure, this is about as clear of a demonstration as we can get.

The scope of the Open Source Hardware release is simple the combination of parts as well as the use of commodity PC hardware for a firewall. This is to prevent IP law from such uses in the future. The firewall design we are releasing is:

- Green. RoHS compliant, consuming 12-20 watts depending on load.
- Silent. No moving parts.
- Powerful. Is sufficient to run a medium sized company (up to 50 users).
- Tough. It is housed in a tamper resistant steel case.
- Reliable. It has demonstrated 6-sigma uptime under extreme conditions.
- Simple. It does not require learning an arcane language or a special cable.
- Accessible. All administration happens on a secure internal web page.
- Intuitive. It has an easy to read dashboard which gives you status at a glance.

The design is released as Open Source Hardware under the OSHW Draft Definition 1.0 license, of which Lobo Savvy Technologies, LLC. Is a signatory. The recommended software is Endian Firewall version 2.5.1 Community Edition, which is a hardened version of RHES, but any PC based firewall software (such as IPCop or PFSense) may be used. *It's your firewall after all.*

Design:

Nothing about this design is critical, though each of the components listed have been carefully selected based on a number of factors. The result is a firewall built from commonly available components into a well-balanced, tough system which consumes little power. Further, the vendors listed have been great to deal with and sell in individual quantities to the general public. The actual hardware cost from the vendors listed comes to a little over $350.00 including shipping.

One question I always get is “How can such a low spec processor do anything useful, much less perform on par with something from a big company which costs 10 times the price of the parts?” This is easy to answer. First, the “low spec” processor is not really a good choice for a desktop machine, particularly with a modern graphical operating system... *but that isn't what we're doing, is it?* We are not running graphics of any kind on the firewall, freeing up the processor to do the heavy lifting. This is the reason Linux makes a better server than any Windows or Mac product given the same hardware.

The biggest pain in dealing with high end Cisco products is the command line. To make it more intuitive, there are tools to administer them graphically, but they really do not have the ultimate power that the command line wields. The firewall distributions we list later all have web based configuration and reporting, allowing anything to be changed intuitively on the fly without needing to be in front of the equipment. The administrator of the firewall may even set it up to be able to administer it from a tablet or smartphone with no limitations. The sky is really the limit.

Alternatives:

If assembling your own firewall isn't something you want to do yourself, we'd be glad to help. Our price is $999.95 for an assembled and tested unit shipped anywhere in the US with a 5 year parts and labor warranty. Lead time is 2 weeks. Installation and training is available for an additional charge.

Should we need a rackmount unit, a 1u rackmount case is available at Logic Supply for $159.00 http://www.logicsupply.com/products/sl1ur_b. This increases the price by about $80.00 including shipping, has moving parts, and is anything but silent. These are the reasons it's not listed in the build.

On the other end of the spectrum and though specifics are outside the scope of this paper, it is possible to use an old PC with a couple of network cards. While we can't recommend it because of downgraded performance and the risks inherent in used equipment, it should be well within the skills of anyone who considers themselves technically inclined. This may be the way to go for a computer enthusiast who has some parts in their personal “boneyard”, since this could drop the parts cost to zero.

Parts list:

Case: Steel wall mount case with mounting plate latched with key lock with power supply.
Product: http://www.morex.com.tw/products/productdetail.php?fd_id=126
Source: http://www.logicsupply.com/products/5689
Cost: $85.00

Mainboard: Jetway NF92-270-LF Intel Atom 270 mainboard with daughtercard expansion.
Product: http://www.jetwaycomputer.com/NF92.html
Source: http://www.logicsupply.com/products/nf92_270_lf
Cost: $129.00

Daughterboard: Jetway AD3RTLAN-G provides three additional individual gigabit ethernet ports.
Product: http://www.jetwaycomputer.com/Daughter_Board.html
Source: http://www.logicsupply.com/products/ad3rtlang
Cost: $56.00

RAM: 1 x DDR2 400/533 SO-DIMM
Product: Common generic part.
Source: http://www.newegg.com/Product/Product.aspx?Item=N82E16820145593
Cost: $18.98 with shipping

Hard Disk: 1 x SATA SSD with at least 8GB capacity
Product: Common generic part.
Source: http://www.newegg.com/Product/Product.aspx?Item=N82E16820227393
Cost: $49.99

OS and Software: Embedded Linux firewall software burned to CD.
Product: Common generic part (see listing below).
Source: http://www.endian.com/index.php?id=400

Listing of Firewall Software:

Please note that this is not a listing of all firewall software usable on the system. It is a list of firewall software known to work on this platform. Since this is a PC set up for a specific use, its capable of running anything, as long as the capabilities of the hardware are taken into account.

- Endian Firewall Community Edition 2.5.1 http://www.endian.com/index.php?id=400
- Engarde Secure Linux 3.0.22 http://www.engardelinux.org/modules/download/
- IPCop version 2.0.4 http://www.ipcop.org/download.php
- IPFire 2.11 http://www.ipfire.org/downloads
- M0n0wall 1.33 generic PC cdrom http://m0n0.ch/wall/downloads.php
- PFSense 2.0.1 http://www.pfsense.org/mirror.php?section=downloads
- Smoothwall Express 3.0 SP3 http://www.smoothwall.org/get/
- Untangle 9.2.1 http://www.untangle.com/store/get-untangle/
- Zeroshell 1.0 beta 16 http://www.zeroshell.net/eng/download/

Tools and Supplies Needed:

- #1 and #2 Phillips screwdriver (a power screwdriver is recommended)
- small zip ties (10 should be more than enough)
- Small diagonal wire cutter
- 10mm wrench or ratchet and socket
- needle nose pliers
- 1 paper clip
- PS2 keyboard
- SVGA monitor
- An external USB CD ROM for setup
- Hardware and appropriate tools to mount the router to the wall.

Construction Notes:

Read the instructions completely before beginning. It should be intuitive, but it will make more sense having read the instructions, seeing the parts, and performing the work. This leverages all three learning styles; auditory, visual, and kinesthetic.

Electronic components are sensitive to static. Use a static safe workstation and wrist strap. If you do not have access to these, there is another way. By carefully following these protocols, you can keep static build up to a minimum, nearly as well as if you had the proper equipment:

- Before beginning or resuming work, touch bare steel in the case before the electronic parts.
- Stay in near constant contact with the bare steel in the case when working on the internal parts.
- Do not remove electronics from protective bags until ready, then put them directly in the case.
- Close the case as soon as the internal work is complete to prevent accidental contact.

Most of the parts fit easily. If they require a lot of force to get into position, something is wrong. Stop and figure it out before the learning experience becomes expensive. The exception to this is the I/O shield. The fit is extremely tight and requires a lot of pressure.

Build Procedure:

1. Open the Case
    1. Turn the key in the case and remove the back plate. Set it aside.
    2. Remove all screws from the case with a #1 phillips (don't forget the four on the bottom).
    3. Slide and remove the top cover. Set it aside.

2. Prepare the Case
    1. Remove the screws holding the hard disk bridge in place with a #1 phillips . Set it aside.
    2. Remove the screws holding the power supply in place with a #1 phillips.
    3. Remove the power jack with 10mm wrench or pliers. Discard the power supply responsibly.
    4. In the mainboard box find the I/O shield and press it fully in the case opening.

3. Install the Mainboard and RAM
    1. Open the static bag with the main board in it and place the main board in the case.
    2. Slide the mainboard toward the I/O shield so that the connectors go out the holes.
    3. Secure the main board with the four included screws and a #2 phillips.
    4. Plug the case reset and power switches into the jacks on the mainboard.
    5. Open the static bag with the RAM in it and place the RAM module in the case.
    6. Place the RAM in the ram slot at a downward angle paying attention to the notch.
    7. Press the RAM into the connector until it engages, then push it down until it locks.

4. Install the Daughtercard
    1. Open the static bag with the daughtercard in it and place it in the case.
    2. Locate the three covers for the daughtercard ethernet ports on the I/O shield. Bend them up.
    3. Align daughtercard on the mainboard connector and press down until fully seated.
    4. Secure daughtercard to the brass post with the included screw and #2 phillips.
    5. Bend the I/O shield cover tabs back down, bringing them in contact with the ethernet jacks.

5. Install the Hard Disk
    1. Remove the hard disk from the packaging and locate the hard disk bridge.
    2. Place the hard disk on the bridge so that the connector will face away from the I/O shield.
    3. Secure the hard disk to the bridge with the the four included screws and a #2 phillips.
    4. Secure the hard disk bridge to the case with the the three included screws and a #1 phillips.

6. Wiring
    1. Plug one of the included SATA cables into the port closest to the corner of the mainboard.
    2. Plug the other side into the port on the hard disk, tucking the excess cable under the bridge.
    3. Locate power cable that came with the mainboard and plug into the mainboard power jack.
    4. Plug the other end of the power cable into the hard disk, using small zip ties to keep it neat.
    5. Trim the tails off the zip ties with the diagonal cutters, taking care not to nick the wires.

7. Close the Case
    1. Ensure the daughtercard connector is properly aligned and mated with the mainboard.
    2. Ensure the wires are not in a location which would be pinched when the case is closed.
    3. Close the case by putting the placing the top on and sliding it to the rear until it seats.
    4. Secure the case with the screws and a #1 phillips. Start with the four screws on the bottom.

Testing, Software Installation, and Mounting:

1. Power Up
    1. Plug in SVGA monitor, keyboard, CD ROM, and power brick
    2. Press the recessed power switch with the end of the paper clip.
    3. As soon as you see activity on the screen, press the <Delete> key to enter setup.
    4. You may see an error pertaining to RAM or hard disk. These are normal at this point.

2. Change BIOS Settings
    1. Hit enter to enter Standard CMOS Features.
    2. Don't worry about setting the date, as most firewalls automatically synch the clock.
    3. Make sure the hard disk appears in SATA 1 Port Master.
    4. Set Halt On setting to All but keyboard. Hit Esc to exit the Standard CMOS Features menu.
    5. Arrow down to the Advanced BIOS Features and hit Enter.
    6. Ensure the USB CD ROM shows up as a boot device ahead of the hard disk, then hit Esc.
    7. Move to Integrated Peripherals menu and set the status after power failure to Former Status.
    8. The remainder of the defaults should be fine. Hit F-10 to save the changes and exit.

3. Install Firewall software
    1. Download the firewall distribution and burn it to CD. We recommend Endian 2.5.1.
    2. Insert the CD containing your choice of firewall software in the CD ROM drive.
    3. Reboot the system.
    4. Follow directions on the screen and/or in the manual of the chosen firewall distribution.

4. Installation
    1. Find a location for the firewall close to the other network equipment it will connect to.
    2. Make sure to orient the mounting plate so the mainboard heat sink fins are vertical.
    3. Secure the plate using generic hardware dependent on the mounting surface.
    4. Slide the firewall on to the cleats of the mounting plate and lock it in place with the key.

5. Final Configuration and Testing
    1. Connect the networks and power (you should not need monitor, keyboard or CD ROM).
    2. Press the recessed power switch with the end of the paper clip and allow it to fully boot.
    3. Log in with a web browser to finish configuration as instructed by the software or manual.
    4. Test for Internet access, adjusting settings as required.

Some Final Notes:

This firewall design is capable of securing three internal networks from the outside. These networks called zones are also firewalled from each other, and will only interreact in a manner you permit with the rules you set. It is possible to make the rules so lax that there is really no point in having the firewall. It is also possible to lock yourself out by setting the rules too tight. Consider what you are doing before you change a rule. If it happens, simply reinstall the firewall software.

Don't loose the key to the firewall case. Because both the last 4 case screws and the plate mounting bolts are inaccessible when the firewall is mounted to the plate and locked, if the key is lost, it will take a herculean amount of effort to remove and/or open the firewall. There is a way, but it isn't pretty, and may kill the firewall hardware. Simply keeping a spare key labeled and where you can find it will prevent this.

While the level flat top surface of the firewall's case may look like a convenient place to put things like power supplies, the area must be kept clear to preserve the convection flow of air that the firewall relies upon for cooling. For this reason, the firewall must be mounted on a wall, not placed horizontally or vertically on a desk. The case will get quite warm under normal operations. While it won't be hot enough to start a fire, use common sense.

Finally, set up the software to email the log files to you. Read them. These will contain hints about potential issues, problematic users, machines in the network with malware, potential hardware issues, and of course external attacks. The picture this data gives you will make a huge difference in the security and reliability of your network.

Open Source Hardware License draft 1.0:

Introduction

Open Source Hardware (OSHW) is a term for tangible artifacts -- machines, devices, or other physical things -- whose design has been released to the public in such a way that anyone can make, modify, distribute, and use those things. This definition is intended to help provide guidelines for the development and evaluation of licenses for Open Source Hardware.

Hardware is different from software in that physical resources must always be committed for the creation of physical goods. Accordingly, persons or companies producing items ("products") under an OSHW license have an obligation to make it clear that such products are not manufactured, sold, warrantied, or otherwise sanctioned by the original designer and also not to make use of any trademarks owned by the original designer.

The distribution terms of Open Source Hardware must comply with the following criteria:

1. Documentation

The hardware must be released with documentation including design files, and must allow modification and distribution of the design files. Where documentation is not furnished with the physical product, there must be a well-publicized means of obtaining this documentation for no more than a reasonable reproduction cost, preferably downloading via the Internet without charge. The documentation must include design files in the preferred format for making changes, for example the native file format of a CAD program. Deliberately obfuscated design files are not allowed. Intermediate forms analogous to compiled computer code -- such as printer-ready copper artwork from a CAD program -- are not allowed as substitutes. The license may require that the design files are provided in fully-documented, open format(s).

2. Scope

The documentation for the hardware must clearly specify what portion of the design, if not all, is being released under the license.

3. Necessary Software

If the licensed design requires software, embedded or otherwise, to operate properly and fulfill its essential functions, then the license may require that one of the following conditions are met:

a) The interfaces are sufficiently documented such that it could reasonably be considered straightforward to write open source software that allows the device to operate properly and fulfill its essential functions. For example, this may include the use of detailed signal timing diagrams or pseudocode to clearly illustrate the interface in operation.

b) The necessary software is released under an OSI-approved open source license.

4. Derived Works

The license shall allow modifications and derived works, and shall allow them to be distributed under the same terms as the license of the original work. The license shall allow for the manufacture, sale, distribution, and use of products created from the design files, the design files themselves, and derivatives thereof.

Open Source Hardware License draft 1.0 (cont'd):

5. Free redistribution

The license shall not restrict any party from selling or giving away the project documentation. The license shall not require a royalty or other fee for such sale. The license shall not require any royalty or fee related to the sale of derived works.

6. Attribution

The license may require derived documents, and copyright notices associated with devices, to provide attribution to the licensors when distributing design files, manufactured products, and/or derivatives thereof. The license may require that this information be accessible to the end-user using the device normally, but shall not specify a specific format of display. The license may require derived works to carry a different name or version number from the original design.

7. No Discrimination Against Persons or Groups

The license must not discriminate against any person or group of persons.

8. No Discrimination Against Fields of Endeavor

The license must not restrict anyone from making use of the work (including manufactured hardware) in a specific field of endeavor. For example, it must not restrict the hardware from being used in a business, or from being used in nuclear research.

9. Distribution of License

The rights granted by the license must apply to all to whom the work is redistributed without the need for execution of an additional license by those parties.

10. License Must Not Be Specific to a Product

The rights granted by the license must not depend on the licensed work being part of a particular product. If a portion is extracted from a work and used or distributed within the terms of the license, all parties to whom that work is redistributed should have the same rights as those that are granted for the original work.

11. License Must Not Restrict Other Hardware or Software

The license must not place restrictions on other items that are aggregated with the licensed work but not derivative of it. For example, the license must not insist that all other hardware sold with the licensed item be open source, nor that only open source software be used external to the device.

12. License Must Be Technology-Neutral

No provision of the license may be predicated on any individual technology, specific part or component, material, or style of interface or use thereof.