m0n0wall - PC Platform Quick Start Guide

Chris Buechler

m0n0wall written by Manuel Kasper. Additional Contributors listed in the m0n0wall Handbook.

m0n0wall Versions 1.2 and 1.3

THIS DOCUMENTATION IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS DOCUMENTATION OR THE ASSOCIATED SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

January 2008

Abstract

Getting started with m0n0wall, a complete embedded firewall software package.

Table of Contents

List of Tables

Next

Chapter 1. Introduction

Chapter 1. Introduction

Table of Contents

1.1. Features

m0n0wall is a project aimed at creating a complete, embedded firewall software package that, when used together with an embedded PC, provides all the important features of commercial firewall boxes (including ease of use) at a fraction of the price (free software). m0n0wall is based on a bare-bones version of FreeBSD, along with a web server, PHP and a few other utilities. The entire system configuration is stored in one single XML text file to keep things transparent.

m0n0wall is probably the first UNIX system that has its boot-time configuration done with PHP, rather than the usual shell scripts, and that has the entire system configuration stored in XML format.

m0n0wall already provides many of the features of expensive commercial firewalls, including:

- web interface (supports SSL)
- serial console interface for recovery
  set LAN IP address
  reset password
  restore factory defaults
  reboot system
- wireless support (access point with PRISM-II/2.5/3 cards, BSS/IBSS with other cards including Cisco)
- captive portal
- 802.1Q VLAN support
- stateful packet filtering
  block/pass rules
  logging
- NAT/PAT (including 1:1)
- DHCP client, PPPoE, PPTP and Telstra BigPond Cable support on the WAN interface
- IPsec VPN tunnels (IKE; with support for hardware crypto cards, mobile clients and certificates)
- PPTP VPN (with RADIUS server support)
- static routes
- DHCP server and relay
- caching DNS forwarder
- DynDNS client and RFC 2136 DNS updater
- SNMP agent
- traffic shaper
- SVG-based traffic grapher
- firmware upgrade through the web browser
- Wake on LAN client
- configuration backup/restore
- host/network aliases

Prev Next
m0n0wall - PC Platform Quick Start Guide Home 1.2. Getting Started with m0n0wall on the PC

2.3. Final Preparation

Now put your written hard disk, CF card or CDROM into your PC system and boot from it as described above. The monitor should show text output during the bootup and finally the console menu waiting for you to start the configuration.

These final steps will assign functions to the interfaces and change the LAN IP address as needed.

1. Wait for the console menu to appear, select 1. (assign network ports)
2. Assign functions (LAN/WAN/OPT) to your interfaces (hint: use auto-detection, or let the MAC addresses tell you which card is which one)
3. Change the LAN IP address, or use the default (192.168.1.1; m0n0wall acts as a DHCP server by default)
4. Access the webGUI (user: 'admin', default password: 'mono')
5. Make the necessary changes to the default configuration

2.3.1. Plugging in the Network Interfaces

Plug the LAN interface into the hub or switch that is connected to your LAN. Plug the WAN interface into your Internet connection (DSL or cable modem, router, etc.) Additional Network interfaces can optionally be connected to other routers, hubs or an Ethernet capable device.

Tip

If your Ethernet devices have built-in LEDs to show connectivity, verify that connected links are showing a green LED when the devices are physically powered on. If it is not showing green then there may be a problem with the cable (damaged or wiring) or with one of the Ethernet interfaces.

1.2. Getting Started with m0n0wall on the PC

The m0n0wall Quick Start Guide is intended to get you up and running with m0n0wall on a two interface (LAN and WAN) setup. The m0n0wall Handbook contains the information you need to further configure your m0n0wall installation after completing this guide.

This version of the Quick Start Guide is specifically tailored to the PC platform. If you are using Soekris hardware, please see the Soekris Quick Start Guide and for WRAP hardware, please see the WRAP Quick Start Guide.

Additionally, a VMware version exists for testing or even using alongside a client computer. More information on this version can be found on the m0n0wall web site.

There are a number of example configurations in Chapter 9 of the m0n0wall Handbook. These configurations describe how to configure several things such as multiple LAN interfaces, setting up DMZ interfaces, wireless interfaces, etc. The base for adding those additional features will be the basic LAN/WAN setup this guide describes.

1.2.1. Why use a PC?

Below are some reasons you might chose to use a PC instead of an embedded system.

- Free if you have extra computer equipment lying around
- Multiple PCI interfaces for high-quality networking cards
- Higher powered CPU for increased speed for VPN or network traffic processing

Prev Up Next
Chapter 1. Introduction Home 1.3. Prerequisites

Next

m0n0wall - WRAP/ALIX Platform Quick Start Guide

Chris Buechler

m0n0wall written by Manuel Kasper. Additional Contributors listed in Users Guide.

m0n0wall Versions 1.2 and 1.3

March 2008

Abstract

Getting started with m0n0wall, a complete embedded firewall software package.

Table of Contents

List of Tables

Next

Chapter 1. Introduction

1.3. Prerequisites

This chapter will go through the hardware and network information you need to gather to proceed through in this guide.

1.3.1. Required Hardware

First, you need to make sure you have the following hardware.

- Destination PC with an 486 or better based CPU
- Bootable storage medium: disk drive, usb drive, CDROM/Floppy, compact flash drive...
- 64 MB of RAM or more
- Two Ethernet network interfaces
- A client computer with network or serial console access to your new m0n0wall, a screen and keyboard to make your initial configuration

Note

Check the manual that came with your destination PC to see what sorts of bootable storage devices are usable.

A keyboard and video card is required for the initial configuration. The serial console can be enabled in the webGUI after this initial configuration, allowing the system to run without a keyboard and video.

1.3.2. Optional Hardware

VLAN tagging: The following drivers/NICs either support VLAN tagging in hardware or handle long frames properly. All other drivers/NICs use software emulation that causes a reduced MTU (which may lead to problems).

- hardware support: bge, em, gx, nge, ti, txp
- long frame support: dc, fxp, sis, ste, tl, tx, xl (most)

Polling: The following drivers/NICs support polling mode to improve performance by reducing interrupt overhead (at the expense of a slightly increased forwarding delay). Polling can be enabled on the System: Advanced setup page in m0n0wall.

- polling support: dc, em, fxp, nge, rl, sis, ste, vr

Wireless: The m0n0wall 1.2x series only support a few 802.11b wireless adapters/chipsets (most notably Lucent Hermes and Intersil Prism II/2.5. m0n0wall 1.3b, which is based on FreeBSD 6, supports (almost) all Atheros-based 802.11a/b/g cards as well (and some Ralink cards too).

1.3.3. Required Network Information

You'll need some information about your Internet connection. You'll need to know which category of the below list your Internet connection falls into, and the appropriate details. You can usually find these details on your ISP's website, and/or in paperwork you receive when you sign up for service. You can also call your ISP's technical support to get this information.

- **Static IP.** - If you have a connection with a static IP, you will need to make note of your IP address, subnet mask, default gateway, and DNS server IP's.
- **DHCP.** - If you have an Internet connection that uses DHCP, you need not gather any more information unless your ISP requires you to pass a certain DHCP hostname value (this is uncommon). If this is the case, you will need to check with your ISP to determine this hostname.
- **PPPoE.** - Many DSL providers provide PPPoE or PPPoA service. Either of these is supported with the PPPoE WAN option. You will need to know your PPPoE username and password and possibly your service name (though this can usually be left blank).
- **PPTP.** - A few ISPs require you to connect to them via PPTP. If your ISP requires this, you will need a username, password, local IP address, and remote IP address from your ISP.
- **BigPond.** - This setting is for BigPond cable connections. You will need your username, password, and possibly authentication server and domain.

You will also need to know if you are connected directly to the Internet or if you are behind a modem or other device that is connected to the Internet. For example, maybe your Internet connection uses PPPoE but you have a PPPoE modem that receives the IP address from your Internet provider and then offers those network services to your internal network using DHCP or static IP.

Warning

The instructions for using the m0n0wall device are written with the idea that your m0n0wall has direct access to the Internet. If you have another device between your m0n0wall and the Internet that offers security or otherwise affects the network traffic (such as a proxy service, NAT device or port use limitations by your Internet provider) the configuration instructions and troubleshooting may not apply to your case.

Make note of the appropriate information for your connection type for later use.

Important

Be sure that you write down all of your existing Internet configuration BEFORE making changes to use your m0n0wall device. Once you have disconnected yourself from the Internet you will lose access to the numerous online help sources until you have re-established your connection.

Prev	Up	Next
1.2. Getting Started with m0n0wall on the PC	Home	1.4. Choosing Your Hardware

1.4. Choosing Your Hardware

The hardware you choose will depend on what features you will use, how much bandwidth you have, and some matters of personal preference (embedded device vs. standard PC). Since m0n0wall is based on FreeBSD 4, most hardware that works with FreeBSD also works with m0n0wall. See the FreeBSD/i386 Hardware Notes for a detailed listing of supported hardware.

Note

The m0n0wall 1.3 releases are based on FreeBSD 6.2-RELEASE. The Hardware Notes for this version is different than the older FreeBSD 4.x versions.

Hardware Reliability

While m0n0wall will run on very old hardware, keep in mind the reliability of older hardware is certainly questionable. If uptime isn't critically important, don't hesitate to use old hardware. If this is in a production business environment, a Soekris or WRAP board could save you some explaining down the road on why your Internet connection went down.

If you are using old hardware, make sure you have a contingency plan should it fail. Keeping a spare machine with your current m0n0wall configuration loaded, ready to be used if necessary, would be a good idea.

Processor

For most broadband connections, any 486 or faster will be sufficient. If you have less than 10 Mb of Internet bandwidth (combined upload and download speed), an embedded device like the WRAP or Soekris platforms, or an old 486 will suffice. For 10 Mb up to a full T3 or more, a Pentium II or III PC system, or embedded device like a NexCom is more appropriate. See Chapter 2 of the Users Guide for further details on compatible hardware.

For connections faster than a T3 using many VPN sessions, you will likely want to use a customized version of m0n0wall specifically built for your requirements, and high end Pentium 4, Xeon, or similar hardware. This is beyond the scope of this document.

RAM

We recommend 64 MB of RAM minimum. 32 MB RAM has been reported to work fine on a CD/ floppy setup with no VPN configurations. It has been reported to run out of RAM with a few active VPN tunnels. Hard drive or CF installs are not recommended with less than 64 MB RAM because you will probably run out of RAM during upgrades and m0n0wall has no swap, so the upgrade will fail.

Hardware Sizing

Keep in mind there is no standard "if you have X Internet connection and Y number of machines on your network, then you need Z hardware". It varies depending on what services you will use, and your Internet traffic characteristics. The one thing that will require significantly more CPU, and/or a VPN accelerator card, is if you'll require more than a couple Mbps of VPN traffic for extended periods.

Some examples of non-encrypted network throughput can be found below, when using the default configuration. Please note that some of these results were reported by users and not officially tested by a developer of the m0n0wall code. Additional information can be found on this FAQ entry.

- Soekris net4501, WAN <-> LAN TCP throughput of about 17 Mbps, including NAT
- Soekris net4801, throughput in excess of 50 Mbps
- PC Engines ALIX.1, throughput in excess of 90 Mbps
- Soekris net5501-70 500Mhz 512M RAM, 84 Mbps
- Liantec 5842 with OpenBSD 4.0, 395Mbps
- New standard PCs, > 100 Mbps (depending on Ethernet cards used)
- Sempron 2800+ (1.6GHz) using Intel Pro 1000 PT pci-e card, 760Mbps
- Sempron 2800+ (1.6GHz) using Intel Pro 1000 GT pci card, 400Mbps

Some encryption speeds are shown below. Please note that speed will change based on the number of concurrent connections and the type of encryption being used.

- Soekris net4801, 3DES-MD5 IPSec encryption, 3.5Mb/s

Network Cards

You will need at least two network cards in the hardware you are using. Most any PCI based cards are compatible, check the Users Guide for further details. ISA cards are much more problematic than PCI cards, and PCI cards are readily available and cheap if you need to buy some.

For this document, we will assume there are two Ethernet interfaces. You can have additional interfaces installed in the system, but do not configure them during these quick installation procedures. Documentation in the Users Guide will soon be available to assist you in setting up additional LAN interfaces, DMZ interfaces, wireless setups, etc.

> ### Tip
>
> You should write down the MAC hardware addresses of each Ethernet interface card if possible. During the configuration of m0n0wall, the Ethernet interfaces will be identified by these addresses. If you do not know them in advance you may need to do some tests to find out which network card has been selected for the LAN and which network has been selected for the WAN. These addresses look like 00:1c:b3:bb:80:42.

1.4.1. Storage Medium

m0n0wall will run off of a hard drive, CD-ROM and floppy, or CompactFlash card. The pros and cons of each follow. Choose the one most appropriate for your situation, taking available hardware and other factors into account.

Hard Drive

Hard drives are readily available, and if you are using a standard PC, you'll likely have one in it. The hard drive installation is remotely upgradeable via the webGUI, so it's a better choice over a CD/floppy setup in many instances. The likelihood of a hard drive failure is pretty high, given that the hardware being used is likely old. An IDE to CompactFlash adapter should be considered where hardware failure cannot be tolerated, since the likelihood of failure is much less with a CompactFlash card. Such an adapter can be purchased new for about $10 USD. PC Engines sells them, amongst other vendors.

CD/floppy Setup

The CD/floppy setup works by booting m0n0wall off of the CD and storing the configuration on a FAT formatted floppy. This is a good solution on systems that you are physically close to very frequently (remote upgrades via webGUI not possible). Floppy disks are notorious for becoming corrupted, so it's even more important to make sure you keep a backup of your configuration. Floppy disks have much more problems in environments that are dusty or dirty, so in those situations we would highly recommend choosing a different setup.

The machine you are using must support CD booting (some 486 and Pentium systems do not). You also must set the CD-ROM as the first boot device in the boot order in the system's BIOS so it doesn't attempt to boot off of the config floppy. Consult your system or motherboard manual for information on how to configure that.

CompactFlash

CompactFlash (CF) is a good choice for most any deployment. CF cards are more reliable than hard drives and the floppy drives that hold the configuration in the CD/floppy setup, and are remotely upgradeable via the webGUI. The downside is you might spend more money getting a CF setup working. If you are not using an embedded device with an onboard CF adapter, you will have to spend about $10 USD on a IDE to CF adapter. You'll need to purchase a CF card at least 16 MB in size.

I purchase used 16 MB CF cards off eBay to use for m0n0wall installations, and get them for $5-$10 USD each. You may also need a CF reader on your PC to write the m0n0wall image to the CF card. Those are approximately $30 USD. So you could be looking at a total expenditure of about $50 USD. But most any business environment should be able to justify such a small expenditure for the increase in reliability.

Prev	Up	Next
1.3. Prerequisites	Home	1.5. Understanding CIDR Subnet Mask Notation

1.5. Understanding CIDR Subnet Mask Notation

m0n0wall uses a subnet mask format that you may not be familiar with. Rather than the common 255.x.x.x, it uses CIDR (Classless InterDomain Routing) notation.

1.5.1. CIDR Table

You can refer to the following table to find the CIDR equivalent of your subnet mask.

Table 1.1. CIDR Subnet Table

Subnet Mask	CIDR Prefix	Total IP's	Usable IP's	Number of Class C networks
255.255.255.255	/32	1	1	1/256th
255.255.255.254	/31	2	0	1/128th
255.255.255.252	/30	4	2	1/64th
255.255.255.248	/29	8	6	1/32nd
255.255.255.240	/28	16	14	1/16th
255.255.255.224	/27	32	30	1/8th
255.255.255.192	/26	64	62	1/4th
255.255.255.128	/25	128	126	1 half
255.255.255.0	/24	256	254	1
255.255.254.0	/23	512	510	2
255.255.252.0	/22	1024	1022	4
255.255.248.0	/21	2048	2046	8
255.255.240.0	/20	4096	4094	16
255.255.224.0	/19	8192	8190	32
255.255.192.0	/18	16,384	16,382	64
255.255.128.0	/17	32,768	32,766	128
255.255.0.0	/16	65,536	65,534	256
255.254.0.0	/15	131,072	131,070	512

255.252.0.0	/14	262,144	262,142	1024
255.248.0.0	/13	524,288	524,286	2048
255.240.0.0	/12	1,048,576	1,048,574	4096
255.224.0.0	/11	2,097,152	2,097,150	8192
255.192.0.0	/10	4,194,304	4,194,302	16,384
255.128.0.0	/9	8,388,608	8,388,606	32,768
255.0.0.0	/8	16,777,216	16,777,214	65,536
254.0.0.0	/7	33,554,432	33,554,430	131,072
252.0.0.0	/6	67,108,864	67,108,862	262,144
248.0.0.0	/5	134,217,728	134,217,726	1,048,576
240.0.0.0	/4	268,435,456	268,435,454	2,097,152
224.0.0.0	/3	536,870,912	536,870,910	4,194,304
192.0.0.0	/2	1,073,741,824	1,073,741,822	8,388,608
128.0.0.0	/1	2,147,483,648	2,147,483,646	16,777,216
0.0.0.0	/0	4,294,967,296	4,294,967,294	33,554,432

1.5.2. So where do these CIDR numbers come from anyway?

The CIDR number comes from the number of 1's in the subnet mask when converted to binary.

The common subnet mask 255.255.255.0 is 11111111.11111111.11111111.00000000 in binary. This adds up to 24 1's, or /24 (pronounced 'slash twenty four').

A subnet mask of 255.255.255.192 is 11111111.11111111.11111111.11000000 in binary, or 26 1's, hence a /26.

And so on...

Prev Up Next
1.4. Choosing Your Hardware Home Chapter 2. Getting and Installing m0n0wall

Chapter 2. Getting and Installing m0n0wall

Table of Contents

The instructions below assume that you have a working PC computer with the proper cables and BIOS options chosen to boot from your selected media. It might save you some troubleshooting time if you first verify that your system is in working condition. One easy way to do this is to download or grab from a computer magazine a bootable Linux or BSD. These are often called Live-CD distributions and can autodetect most hardware and boot your system.

2.1. Choosing your Media

m0n0wall provides two options for PC users, either a CD and floppy setup or a hard disk setup. In either case you will need an existing computer to write to the Compact Flash or CDROM. In both cases you will download a m0n0wall file called an image that contains the bootable operating system. This image will be written to a media that your chosen m0n0wall computer can boot from.

Your customized changes to the default configuration will be stored in active memory of the m0n0wall computer. In a CD/ floppy setup, the floppy will store this customized configuration. In a Hard Drive or CF Card setup, the media itself is also writable and can store the configuration. In all cases the configuration file can be downloaded from the web interface for external storage.

> **Tip**
>
> It is recommended to always store an external backup of your configuration file in case of emergencies.

2.1.1. CD/Floppy Setup

m0n0wall can run from a CD, with a floppy disk to save the configuration. This is typically a good way to try m0n0wall without actually overwriting a hard drive. However, we do not recommend it for production use, due to the likelihood of floppy disk or drive failure. A hard drive is far more reliable, and Compact Flash is even more reliable still.

Starting in version 1.3 a flash drive can be used in place of a floppy disk for storing the configuration file.

2.1.2. Hard Drive or CF Card Setup

Many users find that a Compact Flash card offers higher reliability than an old hard drive. A Compact Flash card can be used to boot a traditional PC when using a Compact Flash to IDE Adapter.

You can also install m0n0wall to any hard drive of sufficient size (>=8 MB in version 1.2 and >10MB in version 1.3 and later), so basically any IDE hard drive ever made).

The instructions for writing the m0n0wall image are the same as writing to a hard disk unless otherwise noted.

Prev Next

1.5. Understanding CIDR Subnet Mask Notation | Home | 2.2. Getting and Installing the Software

2.2. Getting and Installing the Software

To download the generic-pc image or CD ISO, point your web browser to http://www.m0n0.ch/wall/downloads.php and select the generic-pc download link from that page. Download the file to the computer you plan to use for writing to the CompactFlash card or hard disk.

2.2.1. Installing the Standard PC by Hard Disk

Installation on a standard PC requires the following steps:

1. download the raw CF/IDE image (generic-pc)
2. write the image to a CF card (> 5 MB) or an IDE hard disk, either with dd under FreeBSD or under Windows with physdiskwrite. A more detailed description of writing the image to these media is in the following section
3. put the CF card/HD into the target PC
4. plug the PC into the network (LAN/WAN/...).

Caution

If you have an existing DHCP server, and/or wish to use a different IP subnet on your LAN, you will need to first connect via the PC's keyboard/monitor or serial console interface as described in the Initial Configuration chapter.

5. power up the PC

Now that your system has booted using the m0n0wall software continue to the section Section 2.3, “Final Preparation”.

2.2.2. Writing the Image File

If you are installing to a standard PC using an IDE or CF disk, you need to write the image to a sufficiently large CF card or hard disk (at least 10 MB for the generic-PC image in version 1.3). Extra space on the CF card or drive is ignored; there is no benefit to using one larger than 8 MB other than possibly compatibility on future releases.

The following sections will cover how to write the CF card in Windows, FreeBSD, and Linux. A summary is below with details following for each operating system.

- Windows:

  (use the -u flag if the target disk is > 800 MB - make very sure you've selected the right disk!!)

  ```
  physdiskwrite [-u] generic-pc-xxx.img
  ```

  (you must use v0.3 or later!)
- FreeBSD:

  ```
  gzcat generic-pc-xxx.img | dd of=/dev/rad[n] bs=16k
  ```

  where n = the ad device number of your CF card (check dmesg) (ignore the warning about trailing garbage - it's because of the digital signature)
- Linux:

  ```
  gunzip -c generic-pc-xxx.img | dd of=/dev/hdX bs=16k
  ```

  where X = the IDE device name of your HD/CF card (check with hdparm -i /dev/hdX) - some CF adapters, particularly USB, may show up under SCSI emulation as /dev/sdX (ignore the warning about trailing garbage - it's because of the digital signature)

2.2.2.1. Windows

For Windows you will be downloading physdiskwrite from the m0n0wall web site. This is a small Windows NT/2000/XP command line tool that makes it possible to write disk images onto raw disks, like CF cards. It currently has a few rough edges, most notably in the selection of the device to be written – you have to decide which device is the right one by looking at the C/H/S values (though if the CF card was the last device to be connected to the system, it usually shows up as the last one in the list).

Note that the C/H/S values may be incorrect for CF cards – looks like this is a bug in Windows. There is some protection against accidentally overwriting your hard disk, but then again, **I CAN'T TAKE ANY RESPONSIBILITY FOR LOST DATA – YOU USE THIS PROGRAM ON YOUR OWN RISK.**

Manuel Kasper's (author of m0n0wall) physdiskwrite should be used on Windows to write the CF card. Download it from the m0n0wall web site's physdiskwrite page.

Note

Note to Windows Vista users: physdiskwrite works with Vista, but you must make sure to run it as administrator (simply having admin rights isn't enough), or it won't find any disks. One way to do this is to create a shortcut to cmd.exe, then right-click it and select "run as administrator". Then you can launch physdiskwrite from the command prompt window that appears, and it should work fine.

Save physdiskwrite.exe and the downloaded m0n0wall image in the same directory on your hard drive, then open a Windows Command Prompt (click Start, Run, type in cmd and click OK).

Plug in your CF card reader/writer and insert your CF card. If you are connecting your hard drive you can either connect it directly to your computer or through a fire wire or USB adaptor for external drives.

'cd' into the directory containing physdiskwrite and the m0n0wall image and run the following:

```
physdiskwrite generic-pc-xxx.img
```

Replacing generic-pc-xxx.img with the name of the generic-pc image you downloaded.

Tip

Windows users can just simply drag-and-drop the image file onto the physdiskwrite.exe icon.

You will see output similar to the following:

```
physdiskwrite v0.5 by Manuel Kasper <mk@neon1.net>

Searching for physical drives...

Information for \\.\PhysicalDrive0:
   Windows:       cyl: 14593
                  tpc: 255
                  spt: 63
   C/H/S:         16383/16/63
   Model:         ST3120026A
   Serial number: 3JT1V2FS
   Firmware rev.: 3.06

Information for \\.\PhysicalDrive1:
   Windows:       cyl: 1
                  tpc: 255
                  spt: 63
```

You will see all the hard drives in your system listed, as well as the compact flash card. Since we did not run *physdiskwrite -u*, physdiskwrite will refuse to write to any drive over 2 GB. This is a protection so you don't accidentally overwrite your hard drive.

Warning

If you are using physdiskwrite.exe to write to a second hard disk be very careful that you identify the correct disk before writing to it (i.e. do not write the image to your own computer's boot disk).

2.2.2.2. FreeBSD

The procedures to image a CompactFlash card depend upon the type of adapter you are using. The CF card will either appear as a SCSI or IDE hard drive.

Run the command **atacontrol list**. You will get output similar to the following:

```
su-3.00# atacontrol list
ATA channel 0:
Master: ad0 <WDC WD200EB-75CSF0/04.01B04> ATA/ATAPI revision 5
Slave: ad1 <WDC WD800AB-22CBA0/03.06A03> ATA/ATAPI revision 5
ATA channel 1:
Master: acd0 <_NEC CD-RW NR-7800A/10DA> ATA/ATAPI revision 0
Slave: no device present
```

Then run the command **camcontrol devlist**. You will see output similar to the following:

```
su-2.05b# camcontrol devlist
<ADAPTEC RAID-5 320R> at scbus2 target 0 lun 0 (pass0,da0)
<SEAGATE ST39204LC 0005> at scbus2 target 3 lun 0 (pass1,da1)
<ESG-SHV SCA HSBP M10 0.05> at scbus2 target 6 lun 0
(pass2)
```

You will find your CF card somewhere in the above output. Make note of its device name (adX or daX).

Run the following command, replacing adX with your CF device as determined above, and generic-pc-xxx.img with the name of the m0n0wall image you downloaded.

gzcat generic-pc-xxx.img | dd of=/dev/adX bs=16k

Ignore the warning about trailing garbage - it's because of the digital signature.

2.2.2.3. Linux

```
gunzip -c generic-pc-xx-xxx.img | dd of=/dev/hdX bs=16k
```

where X = the IDE device name of your CF card (check with hdparm -i /dev/hdX) - some adapters, particularly USB, may show up under SCSI emulation as /dev/sdX.

Ignore the warning about trailing garbage - it's because of the digital signature.

2.2.3. Installing the standard PC by CDROM

If you are installing to a standard PC using a CDROM and floppy disk, you will need to write the bootable CDROM and format the floppy disk.

Installation on a standard PC with the CD-ROM (+ floppy disk) version requires the following steps:

1. Download the ISO image
2. Burn the ISO image onto a CD-R (or -RW)

   FreeBSD (ATAPI recorder): burncd -s max -e data cdrom-xxx.iso fixate

   Windows: use your favorite burning program (e.g. Nero) to record the ISO image (2048 bytes/sector, Mode-1)

3. Take a standard 1.44 MB diskette or a USB flash drive (m0n0wall 1.3b only) and format it (with an MS-DOS/FAT file system!)

   - 1.44 MB floppy disk
     FreeBSD: fdformat -f 1440 /dev/fd0 && newfs_msdos -L "m0n0wallcfg" -f 1440 /

dev/fd0 Note: you can omit the fdformat step if the floppy disk is already (low-level) formatted

Windows: format A:

- USB flash drive

  Windows: use Windows Explorer to format the drive (FAT32)

4. Plug the PC into the network (LAN/WAN/...).

Caution

If you have an existing DHCP server, and/or wish to use a different IP subnet on your LAN, you will need to first connect via the PC's keyboard/ monitor or serial console interface as described in the Initial Configuration chapter.

5. Power up your PC, enter the BIOS and make sure that booting from CD-ROM is enabled and booting from floppy disk is disabled
6. Insert CD-ROM and floppy disk (do not write-protect the floppy disk!)
7. Continue the boot process

Now that your system has booted using the m0n0wall software continue to the section Section 2.3, “Final Preparation”.

Chapter 3. Initial Configuration

Table of Contents

3.1. Initial Configuration

By default, m0n0wall enables its DHCP server on its LAN interface, and configures the LAN interface with IP address 192.168.1.1. If you have an existing DHCP server, and/or wish to use a different IP subnet on your LAN, you will need to first connect via the PC's keyboard/ monitor or serial console interface.

Note

Unless you know what you're doing, we *strongly recommend* not changing the LAN IP address or pre-configured DHCP settings to avoid difficulties caused by misconfiguration.

If you do not need to change the interface assignments, LAN IP address, or DHCP server settings, you can skip ahead to the next chapter. Otherwise, below are steps to make changes to the default configuration using either your m0n0wall PC's keyboard/monitor or serial console interface.

In general, connecting to a m0n0wall PC with a keyboard/ monitor will prove easier for the first time users than connecting to the serial console interface. This is because there are many different console configurations possible for any given PC, sometimes with jumpers, sometimes in the system BIOS.

Note

The default configuration for m0n0wall does not activate a wireless interface, even if one is installed. That means that you can not change the default configuration using only a wireless connection. You must be connected by Ethernet or Serial console cable to make the first configuration change.

Prev Next

2.3. Final Preparation Home 3.2. Connecting to the keyboard/ monitor

3.2. Connecting to the keyboard/ monitor

If the m0n0wall PC already has a keyboard and monitor it will be easy to verify that the boot up has gone well and to make any necessary changes to the default configuration. During the start up of the m0n0wall computer the status will be output to the screen. When the boot process is finished a cursor prompt will be blinking and awaiting your command.

Assuming all has gone as explained above, you can now proceed to Section 3.4, “m0n0wall Console Setup”.

Prev Up Next
Chapter 3. Initial Configuration Home 3.3. Connecting to the serial console

3.3. Connecting to the serial console

Accessing a PC computer by its serial interface is useful for m0n0wall PC's without a keyboard or mouse connected to them or for troubleshooting. The simplest configuration however is to simply connect a client PC temporarily to the m0n0wall PC as a DHCP client and make your initial configuration using the web interface.

However, instructions are below for those that still wish to connect using a serial console interface.

3.3.1. Getting the appropriate cable

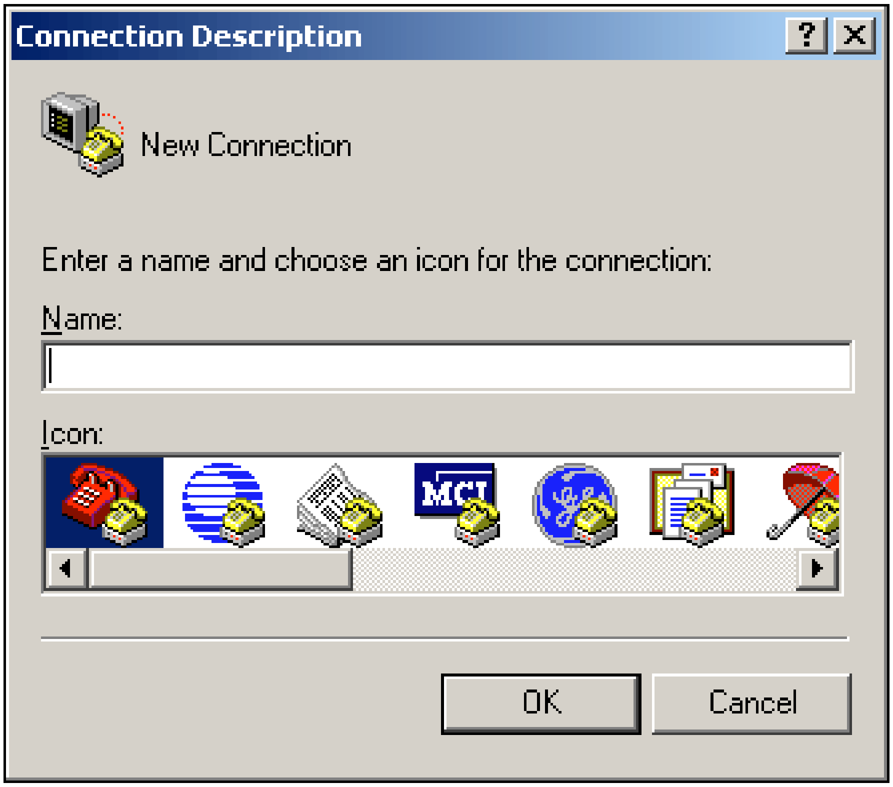
First you need a null modem cable, *not* a straight through serial cable. For the appropriate pin-out, see this page. You can purchase a null modem cable at most any store that carries computer cables, or from a variety of online sources. (Froogle link for null modem cables)

Connect the null modem cable to your embedded device and PC.

3.3.2. Connecting to the serial console

For Windows users, HyperTerminal isn't great, but it gets the job done. You can find it under Start, Programs, Communications, HyperTerminal. If you cannot find it on your system, you can download it for free here.

After opening HyperTerminal, you will see the New Connection screen.



Connection Description

New Connection

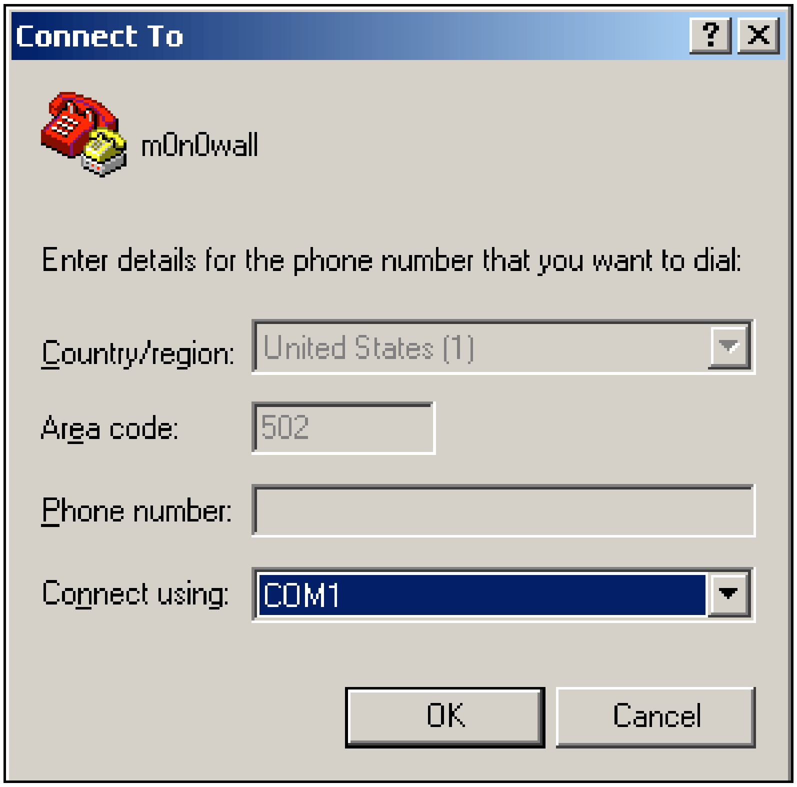
Enter a name and choose an icon for the connection:

Name:

Icon:

Type in something for the connection name and click OK.

Next, you'll see the "Connect to" screen. Select the COM port number of the serial port in your PC. If you do not know which it is, trial and error might be the easiest way to determine this. Start with COM1, and try other ports if necessary. In this case, I know my serial port is COM1.



Connect To

m0n0wall

Enter details for the phone number that you want to dial:

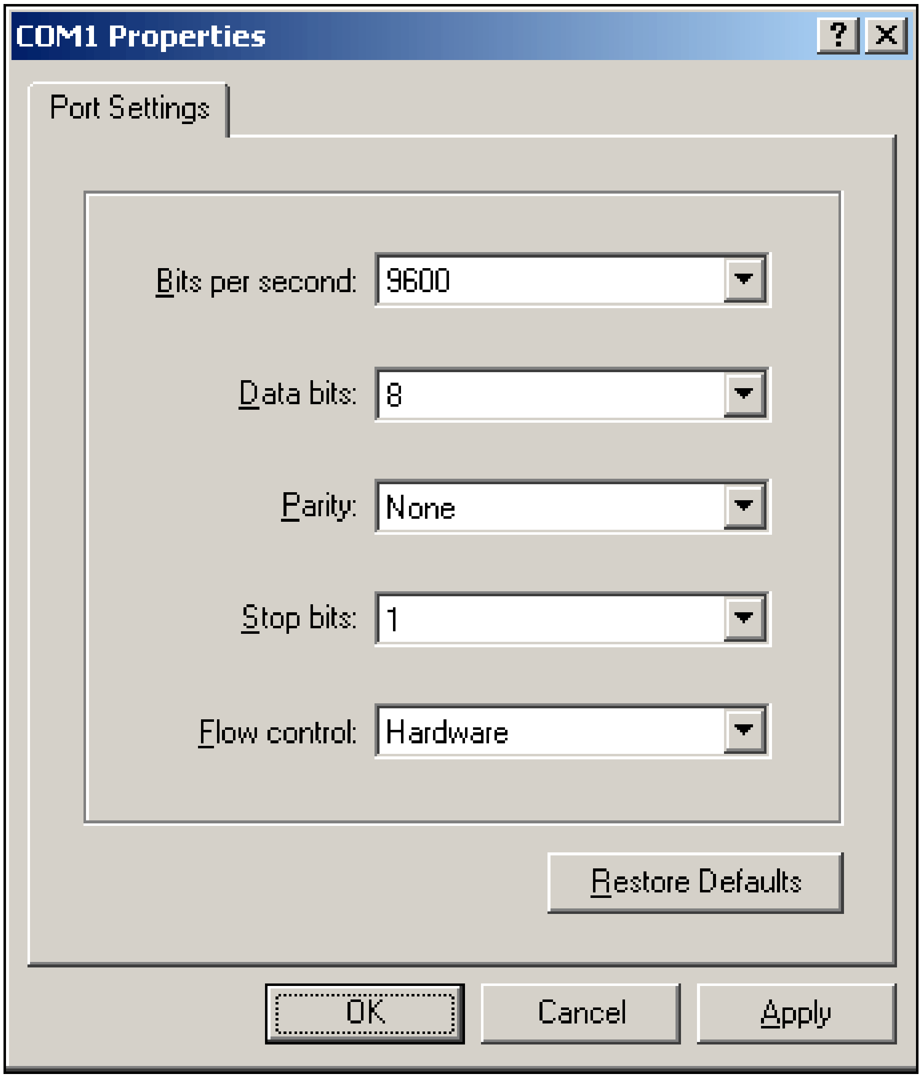
Country/region: United States (1)

Area code: 502

Phone number:

Connect using: COM1

Now you'll see the Connection Properties screen. If you have changed the console speed on your PC, you will need to change the "Bits per second" field accordingly.



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: Hardware

Click OK after filling in the Connection Properties appropriately, and you will have a blank HyperTerminal screen. Now power on your device.

3.4. m0n0wall Console Setup

To recap from earlier, your system is now ready to be configured. You are able to view the keyboard/video output or a serial console at 38400 bps (or via a video card and monitor) and have the media you loaded with m0n0wall earlier installed in the target machine.

When your system finishes booting, you will see the m0n0wall console.

```
*** This is m0n0wall, version 1.2
    built on Sun Aug 22 11:41:15 CEST 2004 for WRAP
    Copyright (C) 2002-2005 by Manuel Kasper. All rights reserved.
    Visit http://m0n0.ch/wall for updates.


    LAN IP address: 192.168.1.1

    Port configuration:

    LAN  -> sis0
    WAN  -> sis1


m0n0wall console setup
**********************
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
```

Although this example shows sis0 and sis1 as the two Ethernet interfaces these names depend on the Ethernet cards that are installed. These 4 characters simply identify the driver used to access the Ethernet card and the number of cards that are using the same driver. Other possible Ethernet interface names include, but are not limited to: bge, em, gx, nge, ti, txp, dc, fxp, sis, ste, tl, tx, xl.

3.4.1. Console Setup Menu Options

First I will explain the purpose of each menu option.

Option 1 allows you to assign network interfaces to be used for LAN, WAN, and OPT networks, as well as allowing you to configure VLAN's.

Option 2 allows you to set the LAN IP address to something other than the default 192.168.1.1.

Option 3 allows you to reset the webGUI password if you have forgotten it.

Option 4 lets you reset the system to factory default configuration. If you get stuck at some point during configuration, sometimes it is easier to start over from scratch.

Option 5 lets you reboot the system.

Prev Up Next
3.3. Connecting to the serial console Home 3.5. Assigning Interfaces

3.5. Assigning Interfaces

Press 1 at the console setup screen if you wish to reassign your network interfaces.

Below are the steps to change the assignment of which Ethernet card is used for which network connection. For example if you had both a 10Mbps and 100Mbps Ethernet card you would typically want the higher speed card (or cards) on the LAN and the slower cards on the WAN (assuming that your WAN Internet connection is less than 10Mbps).

```
Enter a number: 1

Valid interfaces are:

sis0    00:0c:29:96:5e:de
sis1    00:0c:29:96:53:e8

Do you want to set up VLANs first?
If you're not going to use VLANs, or only for optional interfaes, you
should say no here and use the webGUI to configure VLANs later, if
required.

Do you want to set up VLANs now? (y/n)
```

As this guide only leads you through a simple two interface configuration, we will press n and hit enter here to skip VLAN configuration. If you need VLAN support, configure it in the webGUI after this initial configuration is complete. You can use the Valid interfaces list to see how your installed Ethernet cards are identified by the m0n0wall operating system.

```
If you don't know the names of your interfaces, you may choose to use
auto-detection.  In that case, disconnect all interfaces before you
begin,
and reconnect each one when prompted to do so.

Enter the LAN interface name or 'a' for auto-detection:
```

Enter the name of the desired LAN interface by selecting one of the Ethernet card names such as "sis0" and press Enter.

```
Enter the WAN interface name or 'a' for auto-detection
(or nothing if finished):
```

Enter one of the remaining available interfaces and press Enter.

Next you will be prompted for assigning optional interfaces. You can do this later through the webGUI if need be. Without entering anything, hit ENTER at this prompt.

```
Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):
```

You will now see how your interfaces have been configured.

```
The interfaces will be assigned as follows:

LAN  -> sis1
WAN  -> sis0

The firewall will reboot after saving the changes.

Do you want to proceed? (y/n)
```

This confirms how the interfaces will be assigned. Press y and hit enter here to restart the firewall for the changes to take effect. To discard your changes, enter n and press Enter. If all of your hardware and cables are correctly installed you should be able to reach the m0n0wall at the 192.168.1.1 IP address from a client computer.

Prev	Up	Next
3.4. m0n0wall Console Setup	Home	3.6. Changing the LAN IP and/or DHCP server settings.

3.6. Changing the LAN IP and/or DHCP server settings.

View this online tutorial for a how to on changing your LAN IP address and/or DHCP server settings.

Warning

If you already have a DHCP server on your LAN network DO NOT connect the m0n0wall to your LAN network until you have first disabled the DHCP server on the m0n0wall. Otherwise your m0n0wall might respond to a DHCP client computer on your LAN before your normal server and thereby give incorrect information to the requesting computer.

Prev Up Next
3.5. Assigning Interfaces Home Chapter 4. Client Machine Configuration

Chapter 4. Client Machine Configuration

Table of Contents

Now you need to get one of your client machines configured so you can access the webGUI to finish the configuration. A client machine is any Ethernet device (such as a computer, network printer or scanner, network camera...) that is connected to the LAN network of the m0n0wall PC. These devices will use the m0n0wall PC to reach the Internet and they will be protected by your m0n0wall configuration.

If you are using the DHCP server built-into the m0n0wall system, these client machines will be receiving all of their IP configuration from the m0n0wall PC, even if they are not expected to connect to the Internet.

Tip

If you have any servers in your LAN network such as a file or print server, you will want them to have fixed, non-changing IP addresses. Either assign them a fixed DHCP address or a static IP address.

4.1. Using DHCP for client machines

If you aren't familiar with networking, the easiest thing to do is set all your client machines to obtain their IP address from DHCP. m0n0wall enables its DHCP server on the LAN interface by default.

4.1.1. LAN with m0n0wall as DHCP Server

If you are going to use your m0n0wall as a DHCP server, set the client computer you will be using to access the webGUI to obtain its IP address using DHCP. Then release and renew your DHCP lease and you will get a lease from m0n0wall. The procedures to release and renew vary by the client machine's operating system, but if you don't know how to do this, a reboot of the client computer will achieve the same result.

4.1.2. LAN with Existing DHCP Server

If you have an existing DHCP server on your LAN, you just need to set your m0n0wall's LAN IP address as the default gateway address assigned by your DHCP server. This is because your LAN traffic is expected to be going through the LAN interface of your m0n0wall PC so that m0n0wall can protect your network traffic.

When you get into the webGUI, you'll need to disable m0n0wall's DHCP server. You can also disable it from the console as described in the last chapter.

Prev Next
3.6. Changing the LAN IP and/or DHCP server settings. Home 4.2. Static IP addresses for client machines

4.2. Static IP addresses for client machines

If you want to use a static IP address on your client machines, be sure to configure them in the same subnet as your m0n0wall LAN interface, using the appropriate DNS servers and the m0n0wall LAN IP address as the default gateway.

We recommend you stick with DHCP at least initially to reduce the likelihood of problems.

Prev Up Next
Chapter 4. Client Machine Configuration Home Chapter 5. Initial webGUI Configuration

Chapter 5. Initial webGUI Configuration

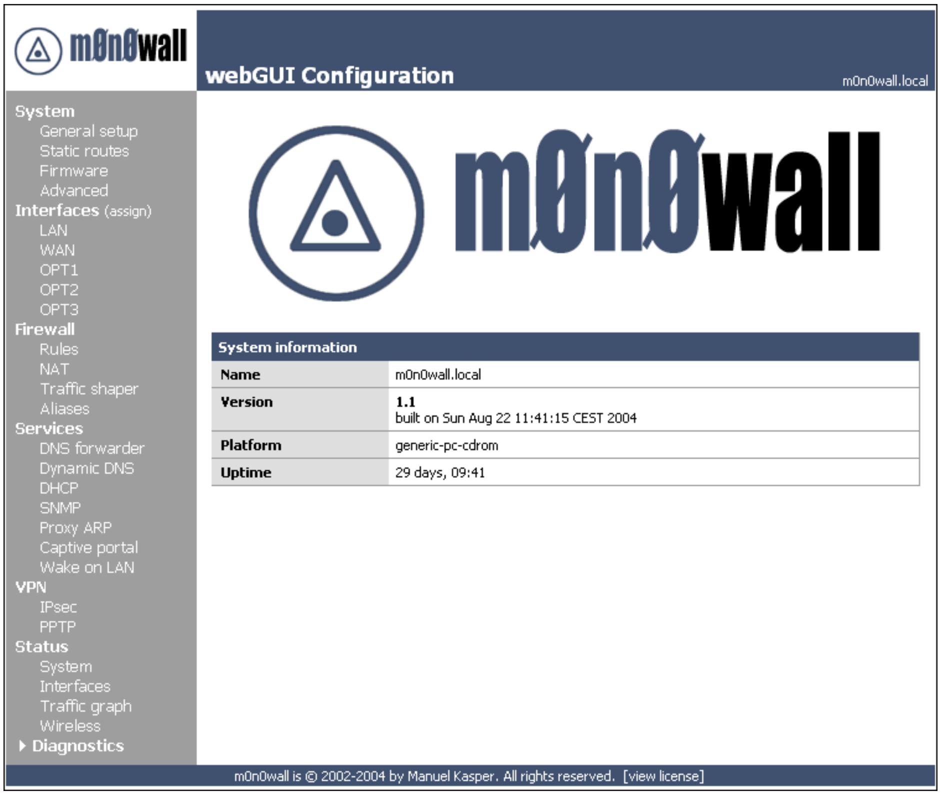
Table of Contents

Now that we have the client machines configured appropriately, the interfaces assigned and LAN IP address configured, and the m0n0wall has rebooted with its new configuration, we will log into the webGUI and finish the configuration.

5.1. Logging into the webGUI

Open your web browser and go to http://192.168.1.1 (if you changed your LAN IP address in the console setup, replace 192.168.1.1 with your m0n0wall PC's LAN IP throughout the remainder of this documentation).

You will be prompted for a username and password. Enter username *admin* and password *mono*. You are now logged into the webGUI.



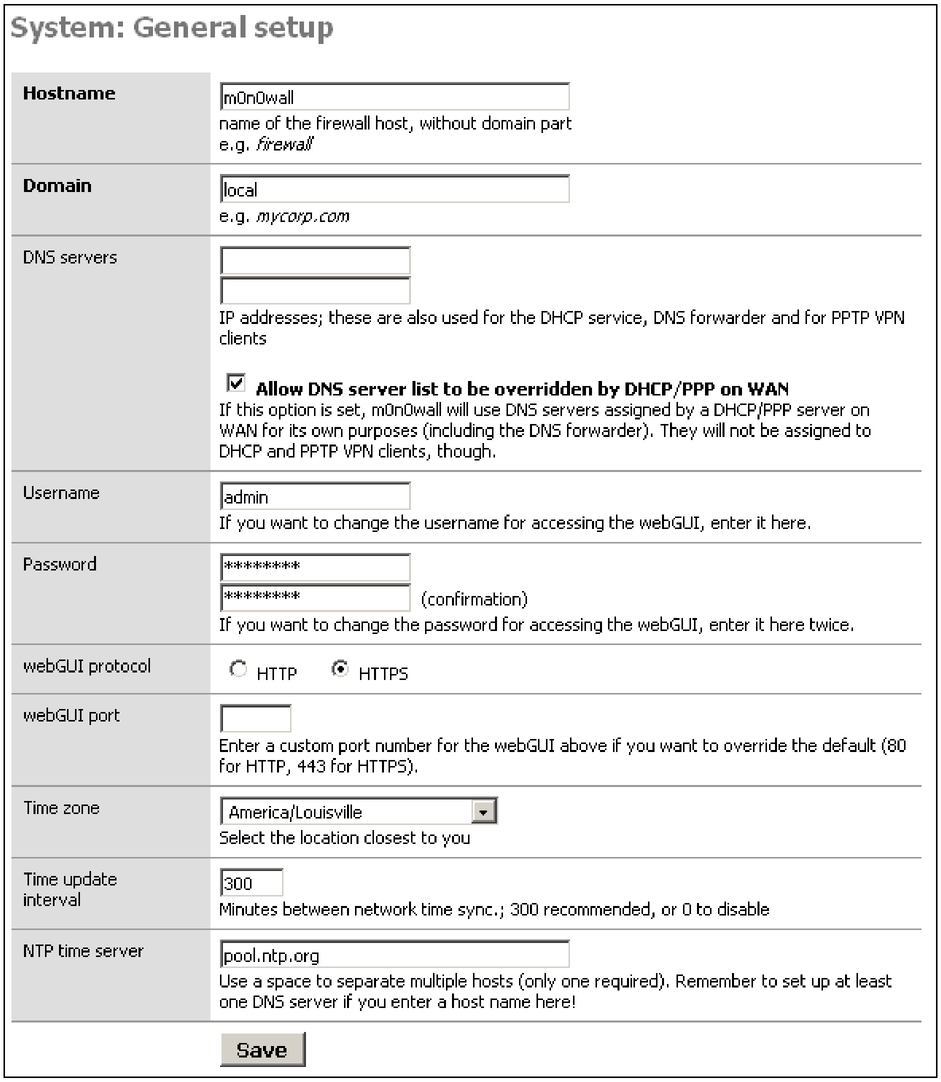
System information

Name	m0n0wall.local
Version	1.1 built on Sun Aug 22 11:41:15 CEST 2004
Platform	generic-pc-cdrom
Uptime	29 days, 09:41

Prev | Home | Next
4.2. Static IP addresses for client machines | | 5.2. webGUI System -> General Setup screen

5.2. webGUI System -> General Setup screen

First click "General Setup".



System: General setup

Hostname	m0n0wall name of the firewall host, without domain part e.g. *firewall*
Domain	local e.g. *mycorp.com*
DNS servers	 IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients ☑ **Allow DNS server list to be overridden by DHCP/PPP on WAN** If this option is set, m0n0wall will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP VPN clients, though.
Username	admin If you want to change the username for accessing the webGUI, enter it here.
Password	********* ********* (confirmation) If you want to change the password for accessing the webGUI, enter it here twice.
webGUI protocol	○ HTTP ● HTTPS
webGUI port	Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS).
Time zone	America/Louisville Select the location closest to you
Time update interval	300 Minutes between network time sync.; 300 recommended, or 0 to disable
NTP time server	pool.ntp.org Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!
	Save

Hostname and Domain

If you wish to change the hostname and domain of your m0n0wall, you can do so in the first two boxes on this screen. If you use m0n0wall as your DNS server, this name will resolve to your LAN IP address. i.e. you can access your webGUI using http://m0n0wall.local or whatever you set the hostname and domain to be.

DNS Servers

If you have a static IP from your ISP, you need to enter the IP addresses of your ISP's DNS servers in these two boxes. Use one IP address per box. If you get your IP address from your ISP via DHCP, leave these boxes blank. If you want to use DNS servers on your LAN, enter their IP addresses here. You can only use one DNS server by filling in the top box and leaving the bottom one blank.

If your ISP uses DHCP and you wish to use the DNS servers the ISP's DHCP server provides, leave the "Allow DNS server list to be overridden by DHCP/PPP on WAN" box checked. If you are using DHCP on the WAN and wish to use DNS servers other than the ones provided by your ISP, uncheck this box.

Username and Password

If you wish to change the username from the default "admin", change the username box appropriately.

> ## Important
>
> It is important that you change your password from the default "mono" by typing in a password of your choosing in the password field and typing it again to confirm in the second field.

webGUI protocol and port

Here you should change the protocol from HTTP to HTTPS so your username and password and configuration details are encrypted while in transit over your LAN.

If you want to make it a little more difficult to find your webGUI logon page, change the port number here. Just remember you will have to put that port number in the URL when logging into the webGUI. For example, if you set this port to 5555, and switch to HTTPS, you will have to use https://192.168.1.1:5555 to access the webGUI.

Time Zone

Select your time zone from this drop down box. This includes all of the time zones from FreeBSD. I am in Louisville, Kentucky, USA, which has its own entry under America/Louisville that I will select. You can likely find a city in the same time zone, or at least find the name of your time zone.

Time Update Interval

m0n0wall has a NTP client built in that by default will synchronize its time to a NTP server every 300 minutes (5 hours). To change the frequency of this update, change this box. Enter 0 to disable NTP clock synchronization (not recommended).

NTP Time Server

This specifies which NTP server m0n0wall will use to synchronize its time. You can leave it at pool.ntp.org unless you have a reason to change it. You might want to change this, for example, to synchronize to a central NTP server on your LAN.

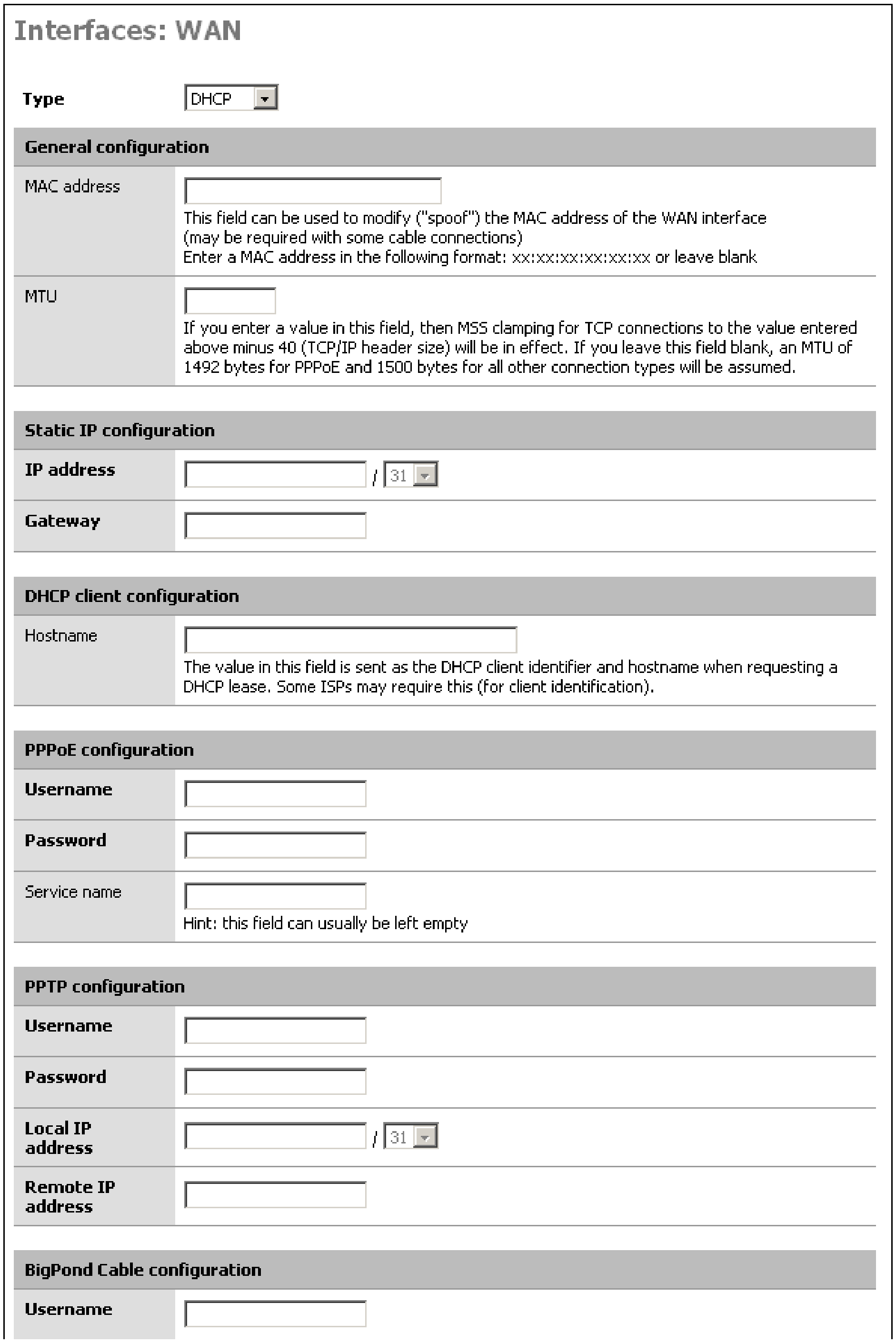
Now review all of your changes on this screen, and when you are satisfied with them, click Save. You'll see notification that the changes were applied successfully.

Prev	Up	Next
Chapter 5. Initial webGUI Configuration	Home	5.3. Configuring your WAN interface

5.3. Configuring your WAN interface

Now we will configure your WAN interface. At this point, you will need some information from your ISP. The WAN connection types available are DHCP, static IP, PPPoE, PPTP, and BigPond. Chances are you will be using DHCP, static IP, or PPPoE.

5.3.1. WAN configuration screen



Interfaces: WAN

Type DHCP

General configuration

MAC address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

Static IP configuration

IP address / 31

Gateway

DHCP client configuration

Hostname
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

PPPoE configuration

Username

Password

Service name
Hint: this field can usually be left empty

PPTP configuration

Username

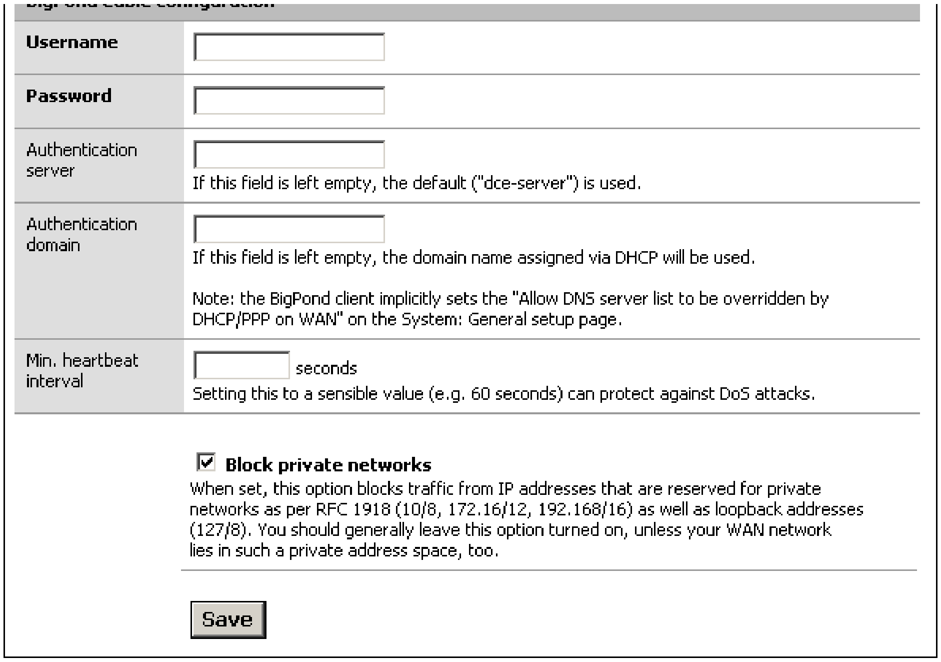
Password

Local IP address / 31

Remote IP address

BigPond Cable configuration

Username



Username	
Password	
Authentication server	If this field is left empty, the default ("dce-server") is used.
Authentication domain	If this field is left empty, the domain name assigned via DHCP will be used. Note: the BigPond client implicitly sets the "Allow DNS server list to be overridden by DHCP/PPP on WAN" on the System: General setup page.
Min. heartbeat interval	seconds Setting this to a sensible value (e.g. 60 seconds) can protect against DoS attacks.

☑ **Block private networks**
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

5.3.2. Type

In the Type drop down box, you have five choices. Choose accordingly for the information you gathered earlier, and fill in any necessary information for your connection type.

5.3.3. General configuration options

Under "General configuration" on this screen, you can change the MAC address of the WAN interface and change the MTU.

MAC address

Some ISP's keep the MAC address of the device you have connected to their network, and only allow that device access. There is typically a process to register a new device, though sometimes that may require contacting the ISP. To avoid this, you can enter the MAC address of the network card you previously used on your broadband connection to make your ISP think you still have the same device connected.

MTU

Unless you have a very good reason for changing it, leave the MTU alone.

5.3.4. Block private networks

Unless your WAN subnet lies in private IP address space, leave this box checked. It protects you from some IP spoofing attempts.

5.3.5. Save and Apply Changes

Now click Save at the bottom of the WAN page. Your changes will immediately take effect, and you should immediately be able to browse the Internet from your LAN. If you cannot, see the troubleshooting section.

Prev	Up	Next
5.2. webGUI System -> General Setup screen	Home	5.4. What next?

5.4. What next?

So you now have m0n0wall configured and working - now what next?

5.4.1. m0n0wall Announcements List

If you are running m0n0wall, we strongly suggest subscribing to the announcements mailing list by sending a blank email to <m0n0wall-announce-subscribe@lists.m0n0.ch>. This is a very low volume list that can only be posted to by Manuel Kasper. It might get 10 messages a year. It's **important to subscribe** so you are kept up to date on any new releases, and will know if any security issues are discovered.

5.4.2. m0n0wall Documentation Announcements List

You might also wish to subscribe to the documentation updates list if you want to keep up to date on major changes to the m0n0wall documentation. Send a blank email to <m0n0wall-doc-announce-subscribe@lists.m0n0.ch> to subscribe. This list can only be posted to by Chris Buechler, and is very low volume with typically less than 10 messages per year.

5.4.3. Explore the Possibilities

m0n0wall is capable of much more than the basic two interface LAN/WAN setup you now have running. Peruse the m0n0wall Handbook for information on implementing more of m0n0wall's capabilities.

Prev Next

Chapter 6. Troubleshooting

Some of the problems you may run into in the process of following this guide, and their associated troubleshooting steps follow.

Prev		Next
5.4. What next?	Home	Glossary

Glossary

DHCP

Dynamic Host Configuration Protocol.

LAN

Local Area Network. A network that typically includes computers which are physically close, such as in one office, usually connected with hubs and switches rather than routers.

NIC

Network Interface Card. A.k.a. network card, or Ethernet card.

NAT

Network Address Translation. A technique whereby IP traffic from multiple IP addresses behind a firewall are made to look to the outside as if they all come from a single public IP address.

See Also Wikipedia Network Address Translation page .

WAN

Wide Area Network. A network that spans a large area, typically including routers, gateways, and many different IP networks.

In the context of firewalls, the WAN interface is the one directly connected to the Internet.

Prev

Chapter 6. Troubleshooting Home

Chapter 19. Troubleshooting

Table of Contents

This chapter outlines some of the more common problems you may experience when using m0n0wall, and how to troubleshoot and resolve them.

19.1. Interfaces are not detected

First check your BIOS settings for a "Plug and Play OS" or "OS" setting. For "Plug and Play OS", set it to "no" or "disable". If there is an "OS" setting, typically you can and should set it to "other". This most always fixes the problem.

If that doesn't resolve it, try to upgrade your system BIOS.

Resetting the BIOS to default settings might help. There have been instances in the past where this has resolved this problem, likely due to some strange BIOS setup from past use of the hardware.

Occasionally other hardware like sound cards, and similar, can prevent some or all of your cards from being detected. Try removing any cards in the system that aren't required, and disabling any unused hardware (USB, parallel port, serial ports, any onboard sound, etc.) in the system BIOS.

Most all Ethernet cards are supported by m0n0wall, but if you still cannot see the network cards, ensure they are supported.

Prev Next

18.9. Historical Interface Graphing Using MRTG on Windows

Home

19.2. After replacing my current firewall with m0n0wall using the same public IP, m0n0wall cannot get an Internet connection.

18.9. Historical Interface Graphing Using MRTG on Windows

If you would like historical graphing of your m0n0wall interfaces, but don't have a Unix box of any sort available, MRTG for Windows is a good solution. There is a howto guide available on the MRTG website.

Before starting that guide, you must enable SNMP on your m0n0wall on the Services -> SNMP screen.

18.8. Automated config.xml backup solutions

The following offers two different ways to automatically back up your m0n0wall configuration. Keep in mind either one requires you saving your firewall password in clear text. This isn't the best idea from a security standpoint, and may not be a risk you are willing to take, depending on your environment. Keep this in mind. At a minimum, make sure you have strong permissions on the .sh file.

18.8.1. Backing up and committing to CVS

Jim Gifford posted the following shell script to the list on January 29, 2004 that automatically backs up the m0n0wall config.xml file and commits it into a CVS repository.

```
#!/bin/sh
# m0n0back -- backup up a m0n0wall config and puts it into
cvs
# depends on: sh, curl, cvs, date, rm

CVSROOT=/cvs
export CVSROOT
CVSPROJ=backup
M0N0IP=192.168.1.1
PROTO=http
USER=admin
PASS=XXXXXX
TMPDIR=/tmp/$$

mkdir $TMPDIR
cd $TMPDIR

cvs -Q co $CVSPROJ
cd $CVSPROJ

curl -s -o config.xml -F Submit=download -u ${USER}:${PASS}
${PROTO}://$M0N0IP/diag_backup.php
```

```
NOW=`date +%Y-%m-%d@%H:%M:%S`
cvs -Q commit -m "backup of config.xml [$NOW]"

cd /tmp
rm -rf $TMPDIR
```

18.8.2. Backing up to the current directory

Chris Buechler wrote a shell script to just back up the file with the filename DATE-config.xml, without committing it into CVS.

```
#!/bin/sh
USER=admin
PASS=XXXXXX
PROTO=http
M0N0IP=192.168.1.1
NOW=`date +%Y-%m-%d@%H:%M`
curl -s -o ${NOW}-config.xml -F Submit=download -u ${USER}:
${PASS} ${PROTO}://$M0N0IP/diag_backup.php
```

Prev Up Next

18.7. Opening Ports for BitTorrent in m0n0wall Home 18.9. Historical Interface Graphing Using MRTG on Windows

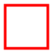
18.7. Opening Ports for BitTorrent in m0n0wall

For maximum performance when using BitTorrent behind NAT, you should open ports 6881-6889 to your PC. As of version 3.2 and later, BitTorrent uses 6881-6999 though you should be fine with the smaller range.

To open these ports, create an Inbound NAT rule matching the following, changing 192.168.1.22 to the IP address of the system using BitTorrent.

Note

If you aren't already using a static IP or static DHCP reservation, you should set one up for that machine now so its IP address will never change.



18.7.1. Opening BitTorrent for Multiple LAN Hosts

BitTorrent starts at port 6881 and will sequentially try higher ports if it cannot use that port. It uses one port for each client session you open. To use BT on multiple hosts on your LAN, open a few ports in the range of 6881-6999 to each host.

18.6. Configuring Apache for Multiple Servers on One Public IP

If you only have one public IP but run multiple web servers, you can set up the others on other port numbers. However giving out URL's like http://www.example.com:81 isn't exactly ideal. You're bound to have people trying to get to http://www.example.com, and since your port 80 points to another web server, the person will get the wrong web page.

You can get around this by using name-based virtual hosting on the web server on port 80. This configuration will work with any web server that supports name-based virtual hosting (most any does), but this section will describe how to configure Apache for this purpose.

For this configuration, port 80 is www.example.com, port 81 is www.whatever.com and port 82 is www.example.net. These are three separate physical web servers.

At the bottom of your httpd.conf (in /usr/local/etc/apache/ in FreeBSD, the location of your configuration file may vary) add the following lines. This is on the server that is accessed via port 80 from the internet.

```
NameVirtualHost 192.168.1.12

<VirtualHost 192.168.1.12>
    UseCanonicalName off
    ServerName www.example.com
    DocumentRoot /usr/local/www/data/
</VirtualHost>

<VirtualHost 192.168.1.12>
    UseCanonicalName off
    ServerName www.whatever.com
    Redirect / http://www.whatever.com:81
</VirtualHost>

<VirtualHost 192.168.1.12>
    UseCanonicalName off
    ServerName www.example.net
    Redirect / http://www.example.net:82
```

```
        </VirtualHost>
```

That configuration will keep www.example.com local, with the site's files in /usr/local/www/data/, and will redirect any requests to www.whatever.com to www.whatever.com:81 and www.example.net to www.example.net:82.

It's not an ideal setup, but if you're stuck with multiple web servers and a single public IP to reference all of them, it's better than people getting the wrong page when forgetting to put the port after the URL.

Prev	Up	Next
18.5. Using MultiTech's Free Windows RADIUS Server	Home	18.7. Opening Ports for BitTorrent in m0n0wall

18.5. Using MultiTech's Free Windows RADIUS Server

In this post to the m0n0wall list on September 30, 2004, Barry Mather explains how to set up MultiTech RADIUS server for use with m0n0wall.

> Get the software (just google radius200.exe and download from multi-tech) Install onto you win32 machine, I have it working on both winxp sp2, and win2k3 server.
>
> If you installed to a default location, open c:\program files\multi-tech systems\radius server2.00
>
> Open the users file with notepad.
>
> Remove all the users in there, I have the following line for a user:
>
> Username   Auth-Type = Local, Password = "userspassword"
>
> The username is the 'username' in the line above is the actual username you want to use.
>
> The realms file can be empty.
>
> The radius program will create a my-users file based on the users file you just edited, leave this alone.
>
> Dictionary file can be left as is.
>
> The clients file needs to be edited to include the ip address of the m0n0wall, and the radius access password, my file looks like this :
>
> 172.16.1.1 password
>
> That's it, v simple
>
> No more files to edit.

It installs itself as a win32 service, just stop the service, restart it, and it loads all the settings / users ..

Now enable the captive portal, telling it to use the ip address of the win32 machine this radius server is installed on, and the password to use, in this case password.

Make sure that your local win32 firewall is either not on, or is allowing port 1812 through for radius!

Prev Up Next

18.4. Updating more than one Dynamic DNS hostname with ddclient

Home

18.6. Configuring Apache for Multiple Servers on One Public IP

18.4. Updating more than one Dynamic DNS hostname with ddclient

m0n0wall updates the dynamic hostname of the external interface with the program ez-ipupdate which is lightweight and does its job. However, it is not capable of updating more than one hostname (like if you host your domain at DynDNS). If you want or need to do this, your best bet is using another system (you'll probably have a server running in the background anyway).

The ddclient project website can be found here.

DynDNS has a list of supported clients. Most of these will work with any dynamic DNS provider, not only with DynDNS.

See what DynDNS offers as services. This is vital in understanding the config file of ddclient.

This document describes the setup for updating several hostnames with ddclient. I chose that particular beast because it can read the external address from status pages of several hardware and software firewalls and routers so I thought I might check if it works out of the box with the m0n0wall status_interfaces.php page. It does.

The config is pretty easy:

```
        # Configuration file for ddclient generated by debconf
        #
        # /etc/ddclient.conf

        pid=/var/run/ddclient.pid
        protocol=dyndns2
        server=members.dyndns.org
        login=YourDynDNSLogin
        password=YourDynDNSPassword
        fw-login=admin
        fw-password=Yourm0n0Password
        use=fw,  fw=http://Yourm0n0IPOrHostname/
    status_interfaces.php
        custom=yes
        yourdomain.org,mail.yourdomain.org,somehost.yourdomain.
    org,yourdomain.com
```

If you only want to update Dynamic DNS entries with DynDNS, remove the

```
    custom=yes
```

directive. If you want to update a DynDNS Static DNS record, replace the

```
    custom=yes
```

with

```
    static=yes
```

If you manage your m0n0wall with TLS, the setup is slightly different as you should run an external command to access the status page:

```
    # Configuration file for ddclient generated by debconf
    #
    # /etc/ddclient.conf

    pid=/var/run/ddclient.pid
    protocol=dyndns2
    server=members.dyndns.org
    login=YourDynDNSLogin
    password=YourDynDNSPassword
    # fw-login=admin
    # fw-password=Password
    # use=fw,  fw=http://Yourm0n0IPOrHostname/
status_interfaces.php
    use=cmd
    cmd='curl -k -s https://admin:
Yourm0n0Password@Yourm0n0IPOrPassword/status_interfaces.php'
    custom=yes
    yourdomain.org,mail.yourdomain.org,somehost.yourdomain.
org,yourdomain.com
```

Now setup ddclient to run as a daemon. Mine checks the status page every 5 minutes and updates the DynDNS records if necessary.

```
        /usr/sbin/ddclient -daemon 300 -syslog
```

Prev | Up | Next
18.3. Collecting and Graphing m0n0wall Interface Statistics with ifgraph | Home | 18.5. Using MultiTech's Free Windows RADIUS Server

18.3. Collecting and Graphing m0n0wall Interface Statistics with ifgraph

ifgraph is a nice utility that you can run on a machine on your LAN to query SNMP on your m0n0wall and graph its interfaces. Note that you may be able to hack m0n0wall to run this locally, but if you have a connection with moderate bandwidth and are running on low end hardware like a Soekris 4501, this could limit the device's throughput.

Sample of the web page output of ifgraph on a m0n0wall.

FreeBSD is used in the demonstrated installation as the OS performing the monitoring and hosting the graphs. This will work on other BSD's, Linux or any other Unix OS, but the installation procedures and configuration file locations may vary.

Prerequisites:

- Installed and functioning Apache server
- m0n0wall SNMP enabled following the instructions in the Users Guide.

1. Install ifgraph.

We'll install ifgraph from FreeBSD ports using binary packages, unless you want to wait for it to compile (doesn't take horribly long). It'll automatically install all the prerequisites either way you do it.

From binary packages

```
        su-2.05b# pkg_add -r ifgraph
```

Compiling yourself

```
        su-2.05b# cd /usr/ports/net-mgmt/ifgraph
        su-2.05b# make install clean
```

2. Query for interfaces

After the successful ifgraph installation, we will use ifgraph's find-if.pl to find the interface numbers on your m0n0wall. Replace 192.168.1.1 with the LAN IP of your m0n0wall, and 'public' with the SNMP community of your firewall.

```
    su-2.05b# /usr/local/bin/find-if.pl -mi 192.168.1.1
public
    OK: session created, getting info from 192.168.1.1
    Showing up interfaces of: 192.168.1.1
    Interface total: 8
    OK: Collecting info on each interface, wait...
    Warn: Could NOT get ifPhysAddress table
    OK: Data collected
    System Description: FreeBSD m0n0wall.local 4.10-RELEASE
FreeBSD 4.10-RELEASE #0: Fri Au i386
    System Uptime: 3 days, 06:10:58.33
    | If #     | Description | Stat | Octets In     |
Errors  | Octets Out    | Errors  | IP Address       | MAC
Address     |
    | ------- | ----------- | ---- | ------------- |
------- | ------------- | ------- | ---------------- |
--------------- |
    | (1)     | wi0         | up   | 0             |
0       | 11538828      | 0       | not set          | not
set         |
    | (2)     | sis0        | up   | 3234568017    |
0       | 1783247523    | 0       | 62.22.130.150    | not
set         |
    | (3)     | sis1        | up   | 0             |
0       | 42            | 0       | 10.1.0.1         | not
set         |
    | (4)     | sis2        | up   | 1743313091    |
0       | 3020545424    | 0       | 192.168.1.1      | not
set         |
    | (5)     | lo0         | up   | 732           |
0       | 732           | 0       | 127.0.0.1        | not
set         |
```

You'll see the names of your interfaces under the description column. Make note of the interface number (first column) for your interfaces.

3. Edit ifgraph.conf file.

Copy the sample ifgraph.conf file (ifgraph.conf.sample) to ifgraph.conf.

```
    su-2.05b# cp /usr/local/etc/ifgraph.conf.sample /usr/
local/etc/ifgraph.conf
```

Use the following ifgraph.conf as a template. You will need to replace 192.168.1.1 with the LAN IP address of your m0n0wall, "public" with the SNMP community configured on your m0n0wall, and the "interface=" line to the number of the interface to be graphed.

```
    # [global] target
    # This target is mandatory
    # The directives of this target are:
    # rrdtool = /path/to/rrdtool - full path to rrdtool
    # rrddir = /path/to/rrddir - full path to a writeable
dir, where
    #                     rrd files and logs will be created
    # graphdir = /path/to/public_html - full path to a
writeable dir,
    #                     where png and html will be created
    # template = /path/to/template_dir - full path to a
directory
    #                     containing template files
    # imgformat = the image format. You may choose:
    #               PNG - Portable Network Graphics
    #               GIF - Graphics Interchange Format
    #               iGIF - Interlaced GIF
    #               GD - Boutell GD
    # Defaults: You can define default configurations in
the global
    # target, but, for this to work, it must be the first
target always.
    # If [global] is after another target, default
configurations
    # will not work as expected.

    [global]
    rrdtool = /usr/local/bin/rrdtool
    rrddir = /usr/local/var/ifgraph
    graphdir = /usr/local/ifgraph/htdocs
```

```
        template = /usr/local/ifgraph/templates/en
        imgformat=PNG
        # those are the default configurations, should be
        # overriden in each target

        host = your.main.router.com
        community = public
        port =161
        max=100M
        dimension=550x200
        colors=back#000000,font#FFFFFF,shadea#212121,
    canvas#232323,mgrid#FF0000,out#FFFFFF
        options=noerror
        hbeat=600
        retry=2
        timeout=5


        [m0n0wall-wan]
        host=192.168.1.1
        community=public
        port=161
        interface=2
        max=100M
        dimension=550x200
        title=In/Out data for m0n0wall WAN interface
        colors=back#000000,font#FFFFFF,shadea#212121,
    canvas#232323,mgrid#FF0000,out#FFFFFF
        options=noerror
        ylegend=kbits per second
        legends=kbits entering our network,kbits leaving our
    network
        shortlegend=kbits/sec
        hbeat=600
        retry=2
        timeout=5
        step = 300
        periods = -1day, -1week, -1month, -1year


        [m0n0wall-dmz]
        host=192.168.1.1
        community=public
        port=161
        interface=3
        max=100M
        dimension=550x200
        title=In/Out data for m0n0wall DMZ interface
        colors=back#000000,font#FFFFFF,shadea#212121,
    canvas#232323,mgrid#FF0000,out#FFFFFF
        options=noerror
        ylegend=kbits per second
        legends=kbits entering DMZ network,kbits leaving DMZ
    network
        shortlegend=kbits/sec
        hbeat=600
        retry=2
        timeout=5
        step = 300
        periods = -1day, -1week, -1month, -1year



        [m0n0wall-lan]
        host=192.168.1.1
        community=public
        port=161
        interface=4
        max=100M
        dimension=550x200
        title=In/Out data for m0n0wall LAN interface
        colors=back#000000,font#FFFFFF,shadea#212121,
    canvas#232323,mgrid#FF0000,out#FFFFFF
        options=noerror
        ylegend=kbits per second
        legends=kbits entering our LAN network,kbits leaving
    our LAN network
        shortlegend=kbits/sec
        hbeat=600
        retry=2
        timeout=5
        step = 300
        periods = -1day, -1week, -1month, -1year
```

4. Run tests.

First we'll run ifgraph.pl to collect the data. Run this at least three times, and wait a few seconds in between runs.

```
su-2.05b# ifgraph.pl -c /usr/local/etc/ifgraph.conf
```

Now we'll run makegraph.pl to make the html pages and graphs.

```
su-2.05b# makegraph.pl -c /usr/local/etc/ifgraph.conf
```

Check the ifgraph htdocs directory to make sure it contains the png and html files.

```
    su-2.05b# ls /usr/local/ifgraph/htdocs
    index.html m0n0wall-lan-1day.png m0n0wall-wan-1month.png
    m0n0wall-dmz-1day.png m0n0wall-lan-1month.png m0n0wall-
wan-1week.png
    m0n0wall-dmz-1month.png m0n0wall-lan-1week.png m0n0wall-
wan-1year.png
    m0n0wall-dmz-1week.png m0n0wall-lan-1year.png m0n0wall-
wan.html
    m0n0wall-dmz-1year.png m0n0wall-lan.html
    m0n0wall-dmz.html m0n0wall-wan-1day.png
```

5. Edit Apache config

In the mod_alias section of your httpd.conf file (/usr/local/etc/apache/httpd.conf in FreeBSD)

```
Alias /ifgraph/ "/usr/local/ifgraph/htdocs/"
```

Restart Apache for the changes to take effect.

```
su-2.05b# apachectl restart
```

6. Open web browser to view graphs.

Open up your web browser and go to http://server/ifgraph/. You should see graphs there, though they probably will not contain any data at this time. If you can't get any web page to appear, you likely have Apache issues. If you see broken images instead of graphs, check step 4 for problems.

7. Add to cron to update automatically.

Open up /etc/crontab in your text editor, and add the following two lines to the bottom of this file.

```
    * * * * * root /usr/local/bin/ifgraph.pl -c /usr/local/
etc/ifgraph.conf > /dev/null
    */5 * * * * root /usr/local/bin/makegraph.pl -c /usr/
local/etc/ifgraph.conf > /dev/null
```

This will run the data collection every minute, and make the graphs every 5 minutes. You can change these if you like, but these values generally work out well.

Note that you likely don't have to run this as root. If you want to be cautious, you should create an account with the appropriately limited permissions to run this under.

Make cron re-read its configuration files:

```
    su-2.05b# killall -HUP cron
```

Prev Up Next

18.2. Installing SVG Viewer on Mozilla Firefox   Home   18.4. Updating more than one Dynamic DNS hostname with ddclient

18.2. Installing SVG Viewer on Mozilla Firefox

The SVG viewer doesn't work "out of the box" after an install like it does in Internet Explorer. See this page on mozilla.org for instructions on installing it.

Prev | Up | Next

Chapter 18. Using Third Party Software with m0n0wall | Home | 18.3. Collecting and Graphing m0n0wall Interface Statistics with ifgraph

Chapter 18. Using Third Party Software with m0n0wall

Table of Contents

18.1. Introduction

There are a number of third party software packages that provide functionality that m0n0wall does not include. These applications are not installed on m0n0wall, but rather on another system on your LAN. This section of the handbook will document how to use several of these packages.

If you know of other third party applications appropriate for this section of the documentation, please email the editor at m0n0wall@chrisbuechler.com.

17.3. Wireless

Home

18.2. Installing SVG Viewer on Mozilla Firefox

17.3. Wireless

Setting Up a Community Hotspot with m0n0wall (PDF) - NYCwireless

Prev Up Next

17.2. VPN/IPsec/PPTP Home Chapter 18. Using Third Party Software with m0n0wall

17.2. VPN/IPsec/PPTP

Authenticating m0n0wall's PPTP VPN with an Active Directory Server - Michael Iedema

Configuring a Wireless Network to Network IPSEC bridge using m0n0wall - Michael Iedema

Wireless inSecurity (bottom of page) - Michael Iedema

Chapter 17. Other Documentation

Table of Contents

There are many people who have written additional documentation for m0n0wall which are beyond the scope of this manual, or which have not yet been incorporated into this manual. This chapter provides a reference to some of those sources to help you when you find yourself in a situation not covered in detail in this manual.

17.1. Installation

m0n0wall Live Installer - FreeBSD Live CD (built using FreeSBIE) including all m0n0wall 1.11 and 1.2b3 images and instructions on using it.

Installing m0n0wall over a network - Roberto Pereyra

16.46. How can I increase the size of the state table?

m0n0wall's default firewall state table is limited to 30,000 states. This is sufficient for the vast majority of firewalls, and extra states may require more RAM than exists in some m0n0wall installations.

Unfortunately, to increase the size of the state table you have to recompile the kernel. See The complete guide to building a m0n0wall image from scratch in the m0n0wall Developers' Handbook.

> ### Note
>
> This is *rarely* necessary. Unless you have a very fast and heavily loaded Internet connection, or 10+ Mb of certain types of peer to peer traffic, chances are you will never exceed 30,000 states. The number of states required by a given environment will vary dramatically. 50 Mbps of HTTP, SMTP, POP3, and IMAP traffic might only take 20,000 states, but 50 Mbps of peer to peer traffic from dozens of machines might take more than a million states.

If you find you cannot create new connections to the Internet from any machine, but existing connections all work properly, you may have exhausted your state table.

Prev Up Next

16.45. Is there any extra Captive Portal RADIUS functionality available? Home Chapter 17. Other Documentation

16.45. Is there any extra Captive Portal RADIUS functionality available?

Jonathan De Graeve has implemented a number of new RADIUS features for Captive Portal that will be implemented in a future beta version. For now, these features are available on test images available for download from http://inf.imelda.be/downloads/m0n0wall/.

Features currently implemented in the test images include:

- RADIUS-defined URL redirection taking precedence over URL redirection parameter in captive portal setup page.
- Multiple RADIUS server support
- Failure message on captive portal login error page, plus logging to the captive portal log on why authentication failed (user account exceeded bandwidth limit, bad password, etc.).
- Cisco-compatible feature (sending calling-station-id with clientip and called-station-id with clientmac instead of standard behavior calling-station-id and clientmac).
- Timeout parameter and max authentication retries parameter
- retrieval of user bandwidth settings
- retrieval of user group
- retrieval of session-timeout

Note

Retrieval means the variable is present and CAN be used, but there is no action bound to it yet.

To do - GUI implementation and enhancements.

16.44. When will m0n0wall be available on a newer FreeBSD version?

Beta versions 1.2b5 through b7 were based on FreeBSD 5.3, after much demand. This brought greatly improved wireless card support, but that's it. Many other, more important things were a major step back from the current FreeBSD 4.x. Network performance was anywhere from 20-50% of the speed it used to be on embedded platforms, and stability was poor in comparison in some environments.

We consulted with members of the FreeBSD Core Team on the issues we were seeing with performance, and their answer was basically "yes, we know it is slower, and are working on improving it." FreeBSD 6 is already much improved, and the funded TCP optimization work currently being done will improve things much more.

It was decided to revert back to 4.x to finish the 1.2 release, and hence get it done much faster than would be possible on 5.x and with a much better end result.

After 1.2 is released, discussion will be started on the list as to which operating system and firewall software is best suited for the next m0n0wall release. At this point, FreeBSD 6 looks like the most likely candidate, and will bring back Atheros support amongst many other enhancements not available in FreeBSD 4 or 5.

Prev	Up	Next
16.43. Where can I get a high-resolution version of the m0n0wall logo?	Home	16.45. Is there any extra Captive Portal RADIUS functionality available?

16.43. Where can I get a high-resolution version of the m0n0wall logo?

An EPS version of the logo is available here.

Prev Up Next
16.42. Can I sell m0n0wall (or use it in a commercial product)? Home 16.44. When will m0n0wall be available on a newer FreeBSD version?

16.42. Can I sell m0n0wall (or use it in a commercial product)?

m0n0wall is under the BSD license, which basically means that you can do whatever you want with it (including modifying and selling it) for free, as long as the original copyright notice and license appear somewhere in the documentation and/or the software itself. There are no warranties of any kind though.

For the full copyright notice/license text, see http://m0n0.ch/wall/license.php.

Although you don't have to pay anything for m0n0wall even if you sell it, if you do find yourself making money by selling m0n0wall-based products, a donation would be very much appreciated.

Prev Up Next
16.41. Can I have more than 16 simultaneous PPTP users? Home 16.43. Where can I get a high-resolution version of the m0n0wall logo?

16.41. Can I have more than 16 simultaneous PPTP users?

Yes, though this is not officially supported. See this page on Chris Buechler's website for images and further information.

Prev Up Next
16.40. Why doesn't m0n0wall have a log out button? Home 16.42. Can I sell m0n0wall (or use it in a commercial product)?

16.40. Why doesn't m0n0wall have a log out button?

m0n0wall uses HTTP authentication. For every page you request from m0n0wall, your browser sends the username and password from its cache. There is no reliable way to force the browser to "forget" the username and password, and session management to work around that would introduce potential security vulnerabilities, so m0n0wall does not provide log out functionality. To safely log out, close your browser.

Your web browser may have a way to clear cached HTTP credentials. Check your browser's documentation for further information.

Prev Up Next
16.39. Why can't my IPsec VPN clients connect from behind NAT? Home 16.41. Can I have more than 16 simultaneous PPTP users?

16.39. Why can't my IPsec VPN clients connect from behind NAT?

That's because FreeBSD doesn't support NAT-T, which is required for IPsec to work behind NAT on the remote end.

Reference

Unfortunately, there's no way to fix that at this point. OpenVPN, which is in the current beta versions, might be a good solution.

Prev Up Next
16.38. Why am I seeing "IP Firewall Unloaded" log/console messages? Home 16.40. Why doesn't m0n0wall have a log out button?

16.38. Why am I seeing "IP Firewall Unloaded" log/console messages?

Nothing to worry about. ipfw is only used for traffic shaping in m0n0wall - you probably enabled and later disabled the traffic shaper (the module is only loaded on demand). The real packet filtering is done with ipfilter, which is compiled into the kernel and cannot be unloaded.

Prev Up Next

16.37. Why isn't the reply address of the list set to the list? Home 16.39. Why can't my IPsec VPN clients connect from behind NAT?

16.37. Why isn't the reply address of the list set to the list?
Prev **Chapter 16. FAQ** Next

16.37. Why isn't the reply address of the list set to the list?

The ezmlm FAQ explains why this is not recommended.

Manuel posted the following explanation to the list on May 12, 2003.

```
It will stay this way because I read this:
http://www.ezmlm.org/faq-0.40/FAQ-9.html#ss9.8
and found that they're right - I can live with the fact
that people have
to think twice before posting anything to the list. :)
Besides, other
lists behave in the same way, too (including soekris-tech
and
freebsd-small), and every better MUA has got a "Reply All"
function, so
that issue is settled as far as I'm concerned.
```

Also see The Great Reply-to Debate in the book Producing Open Source Software.

Prev Up Next
16.36. Why do my SSH sessions time out after two hours? Home 16.38. Why am I seeing "IP Firewall Unloaded" log/console messages?

16.36. Why do my SSH sessions time out after two hours?

As of 1.2b2, the TCP idle timeout for the firewall is 2.5 hours instead of the ipfilter default of 10 days (!) to keep the state table from filling up with dead connections. This value can be modified on the advanced setup page, though that is not recommended. So of course if your SSH connection doesn't transfer a single byte for two hours, the ipfilter state table entry is deleted and the connection breaks. Turning on keep-alives in your SSH client is the recommended means of avoiding broken sessions.

Prev Up Next
16.35. Can I run Captive Portal on more than one interface? Home 16.37. Why isn't the reply address of the list set to the list?

16.35. Can I run Captive Portal on more than one interface?

No. Because of the way Captive Portal is implemented, it cannot be used on more than one interface.

Prev Up Next
16.34. Can Captive Portal be used on a bridged interface? Home 16.36. Why do my SSH sessions time out after two hours?