

by mcpat, adapted by MeisterEder & MrAlvin

## Contents

- 1 ProFTPD included in web-GUI
  - ◆ 1.1 FTP Option - allow WAN FTP access (outdated since 19550)
  - ◆ 1.2 FTP Option - allow WAN FTP access including passive modes
  - ◆ 1.3 FTP Option - allow anonymous FTP access to all or part of the data drive
- 2 Optware ProFTPD versions
  - ◆ 2.1 Preface
  - ◆ 2.2 First: install optware
  - ◆ 2.3 Install xinetd
  - ◆ 2.4 Install proftpd
  - ◆ 2.5 Configure xinetd
  - ◆ 2.6 Configure proftpd
  - ◆ 2.7 Setting up users
  - ◆ 2.8 Start the xinet-superserver
  - ◆ 2.9 Test the service

## ProFTPD included in web-GUI

As of version v24TNG - Eko svn11218 - Dec 17, 2008 (recommended version is svn11296) Mega and Mini\_usb\_ftp versions have built-in FTP server option.

In latest firmwares with ProFTPD embedded, go to the WEB GUI, and under SERVICES>NAS, you can configure your ftp server this

way:

## ProFTPD

In the web-GUI select:

tab: Services -> tab: NAS -> section: ProFTPD ->

- option: ProFTPD = enable
- option: Server Port - 21 - is recommended
- option: Files Directory - can be any rw-able drive space
- option: Allow Write - enable - is needed if you want to be able to FTP-write to the drive
- option: User Password List -> any *name* [space] *password* can be entered

◊ Name and password must be separated by a space.

◊ You should enter at least one *user name* and *password*,  
so you do not need to use the "root-user" to get FTP access.

Click "Save" and "Apply Settings"

And you should now have FTP LAN access to your data drive

### FTP Option - allow WAN FTP access (outdated since 19550)

To allow WAN access using FTP protocol run the following line in a terminal window:

```
/usr/sbin/iptables -I INPUT 1 -p tcp --dport 21 -j logaccept
```

Note: FTP is a clear text protocol, so your FTP username and password can be sniffed, so you should think twice before enabling WAN FTP access.

### FTP Option - allow WAN FTP access including passive modes

Allowing WAN access was not so simple for me. Here is what I did to make the ftp work for the WAN.

1 - First proftpd has to be configured properly for incoming connection for both Active and Passive modes.

For that purpose a couple of lines need to be added to /tmp/proftpd/etc/proftpd.conf.

Add this if using a domain name(needless to say replace the domain name or IP with your domain name or IP):

```
MasqueradeAddress      xxx.mydomain.com # DNS name
#OR this if not using a domain name
MasqueradeAddress      123.45.67.89     # WAN IP
```

Other line to add is the Passive ports on which proftpd will be listening. I chose the port range 60000 to 61000 opening 1000 ports. Change this range to your requirement.

```
PassivePorts 60000 61000
```

The problem is that /tmp/proftpd/etc/proftpd.conf gets overwritten every time router is restarted. So add these lines using a startup[Administration->commands->startup] script. Here is how I did it:

```
#----- for proftpd passive WAN access -----
echo 'MasqueradeAddress xxxxx.dyndns.org'>> /tmp/proftpd/etc/proftpd.conf #Masquerade the respo
echo 'PassivePorts 60000 61000'>> /tmp/proftpd/etc/proftpd.conf #Set the passive ports range
killall -HUP proftpd #restart the ftp server
```

## ProFTPd

2 - Now forward these passive ports to the internal IP address of your router e.g. 192.168.1.1. I forwarded the ports using the UI. It can also be done using the iptables. However I feel comfortable with the UI

2.1 - The Iptables command to open the passive ports for the firewall are:

```
/usr/sbin/iptables -I INPUT -p tcp -m tcp --dport 60000:61000 --syn -j logaccept
```

(If using this it is unnecessary to forward the range of ports in the GUI to the router, I could not use the GUI to get passive mode to work correctly but this did the trick).

### FTP Option - allow anonymous FTP access to all or part of the data drive

You can allow anyone on your LAN to *read* all or a specific folder-tree on your data drive. If you enable WAN access, the anonymous settings will also apply to all WAN users ( = all of the internet users )

- option: Anonymous Login (Read-only)

Can be enabled if you want anyone to be able to *read* files on your data drive.

- option: Anonymous Home Sub-directory

Can be set to a sub-folder where you keep your public files and folders, like: /mnt/public - so your private and public files and folders can be kept separate.

#### Anonymous example

You must create the public folder in a terminal or using the normal FTP user.

```
cd /mnt  
mkdir public
```

In Anonymous Home Sub-directory text field write: **/public**  
Click "Save" and "Apply Settings"

## Optware ProFTPd versions

### Preface

To run a ftp-server you need appropriate free space on your device. So its best you have sd-card-modded your device (or you can connect an HD). This tutorial points on an installed sd-card mounted to "/mmc". It is also possible to replace every occurrences of (/mmc) with (/jffs) if you have it enabled.

### First: install optware

If you dont have installed this wonderful system, so do it now! It easy and described in [Optware](#) (up to 2.2).

## ProFTPD

### Install xinetd

Xinetd is a so called super-server. It receives requests on configurable ports and then starts an appropriate serverprocess. In our case xinetd should manage the ftp-requests and start proftpd. So install xinetd:

```
/opt/bin/ipkg update xinetd
/opt/bin/ipkg install xinetd
```

### Install proftpd

Also install the proftpd-server:

```
/opt/bin/ipkg install proftpd
```

Because of the good work of the optware-people there is only a little bit configuration to do:

### Configure xinetd

In default-configuration xinet only listens to requests from network 192.168.1.0/24 If your network does not meet this netmask you have to change the value:

Open the file `/opt/etc/xinetd.conf` with you favorite editor (maybe "nano")

```
nano opt/etc/xinetd.conf
```

Change the value for "only\_from" to your netmask (something like 192.168.4.0/24?) To allow request from everywhere you can comment this line out (note "#" at beginning of the line)

### Configure proftpd

Open the file `/opt/etc/proftpd.conf` with you favorite editor (maybe "nano")

```
nano opt/etc/proftpd.conf
```

We have to change some values for meeting the standards of dd-wrt: Replace the lines:

```
User          nobody
Group         nobody
```

with

```
User          root
Group         root
```

Also you can change the "DefaultRoot" to "/mmc" if you want.

If you dont want to allow anonymous access delete the entire "<Anonymous>" section!

If proftpd doesn't start when you connect to it, try deleting/commenting "Anonymous" section.

## Setting up users

In orthodox, proftpd uses system passwd file to define users access. That means ftp users are system users. Buuum! It's not possible to define more than one user in dd-wrt. However, there is a way out.

Find this option:

```
AuthUserFile /etc/passwd
```

in proftpd.conf file and define a different file for passwords. Let's put in near proftpd.conf itself:

```
AuthUserFile /opt/etc/passwd
```

From now on, the ftp server will look up user passwords in /opt/etc/passwd rather than /etc/passwd

We can edit the /opt/etc/passwd file and add users to it. The format is common linux passwd file, the passwords are MD5. I was way too lazy to create it manually, so you may use the same trick:

1. Change your dd-wrt web gui username and password to the user you would like to have on ftp, then reboot.
2. Copy the /etc/passwd to /opt/etc/passwd
3. Change the gui login credentials back

Open /opt/etc/passwd . Let us assume the username is "ftp" and the password is "test". You should see 2 lines inside /opt/etc/passwd , the second one starting with reboot. Delete the second one. The one left will look something like this:

```
ftp:$1IBcY2cN82WXH9/vq/:0:0:Root User,,,:/root/tmp:/bin/sh
```

You may want to change the user home dir to /jffs/ftp . Change the /root/tmp to /jffs/ftp

```
ftp:$1IBcY2cN82WXH9/vq/:0:0:Root User,,,:/jffs/ftp:/bin/sh
```

So, now we have a ftp user "ftp" with his home dir in /jffs/ftp . If you want this to be his upper (root) folder, enable DefaultRoot as described above. I would recommend enabling this function for security reasons.

Add additional lines to this file to create more users.

## Start the xinet-superserver

```
/opt/etc/init.d/S10xinetd start
```

## Test the service

Connect with your favorite ftp-client to the new server. Login with your wrt-"root"-Login (or another existing user) Maybe the login takes a while - the proftpd-server have to start for every connect!