



Mini-HOWTO für Portforwarding auf einem Ethernet Router (FLI4L ohne Einwahl)

Author: Andreas Rasztovits (andreas.rasztovits@justiz.gv.at)

Als Vorlage diente das [WWW/FTP Server HOWTO von Jens Fischer \(soth@gmx.net\)](#).
Vielen Dank daß ich das HOWTO verwenden durfte.

Creation: 28.03.2002 ar

Last Update: 05.04.2002 ar

VORRAUSSETZUNGEN:

Ein lauffähiger Fli4l-Router (Version 2.0.1 oder höher) mit folgenden installierten Paketen:

OPT_PORTFW (Basis-Paket)

OPT_PORTFWUP (OPT-Paket)

Ein Rechner mit installiertem WWW und/oder FTP Server, der bereits aus dem LAN erreichbar ist und dort diese Dienste erfolgreich anbietet. Dieser Rechner muß auch für den Internetzugang über den Router konfiguriert sein. Das bedeutet, als Gateway und als DNS muß die IP des Routers (192.168.6.1) eingetragen sein.

Beispiel-IP-Adresse dieses Rechners im HOWTO: 192.168.6.2

Beispiel-IP-Adresse des Routers im HOWTO: INTERN 192.168.6.1 EXTERN 10.4.202.1

ZIEL:

Einen WWW und/oder FTP Server auf einem Rechner im maskierten LAN aus dem Internet erreichbar zu machen.

Die lokalen WWW-/FTP-Dienste auf dem Router sollen weiterhin im LAN (und nur von dort!) erreichbar sein.

HINTERGRUND:

Bei dem Einsatz von FLI4L als Router ohne Einwahl (also ohne ISDN,xDSL..) wird das Portforwarding Script nicht gestartet. Das Script würde erst bei der Einwahl aktiv. Da wir aber keine Einwahl verwenden wird das Script nicht ausgeführt und das Portforwarding nicht aktiv. Dafür gibt es das OPT-PORTFUP Paket. Dieses führt das Script bereits beim Boot aus und setzt somit das Portforwarding aktiv.

Alle Anfragen aus dem Internet an den Router auf den Ports 80 (HTTP) sowie 21 (FTP-Control) und 20 (FTP-Data, für ACTIVE FTP) sollen nicht von dem Router beantwortet werden, sondern an einen Rechner im LAN weitergereicht werden, der sich dann um die Beantwortung dieser Anfragen kümmert. Dieses Verfahren nennt man Port-Forwarding. Nun können diese weitergeleiteten Ports aber nicht mehr für OPT_HTTPD bzw. OPT_FTPD auf dem Router genutzt werden. Deshalb werden diese Dienste auf andere (höhere) Ports verlagert, nämlich (beispielsweise) auf Port 8080 für OPT_HTTPD sowie auf Port 2121 für OPT_FTPD. Desweiteren müssen die Firewall Regeln angepasst werden, denn standardmäßig blockt Fli4l alle Anfragen aus dem Internet auf den Ports 80 bzw. 21 und 20 ab, sowie läßt Anfragen auf den Ports 8080 und 2121 durch! Die Regeln müssen dahingehend geändert werden, daß die Ports 80, 21 und 20 durchgelassen werden und die Ports 8080 und 2121 geblockt werden.

EINRICHTUNG:

1.)

Es wird OPT_PORTFW benötigt, also ist die Datei config/base.txt anzupassen:

```
#-----  
-----  
# Optional package: PORTFW  
#  
# If you set OPT_PORTFW='yes', you can also edit opt/etc/portfw.sh  
#-----  
-----  
OPT_PORTFW='yes' # install port forwarding tools/modules  
PORTFW_N='0' # how many portforwardings to set up
```

Direkte Änderungen an der Datei opt/etc/portfw.sh sind nötig damit das Portforwarding funktioniert, deshalb PORTFW_N='0'!

2.)

Wenn ein maskierter FTP-Server betrieben werden soll, dann müssen noch folgende Zeilen in der config/base.txt gegeben sein:

```
#-----  
-----  
# Masquerading:  
#-----  
-----  
MASQ_NETWORK='192.168.6.0/24' # networks to masquerade (e.g. our LAN)  
MASQ_MODULE_N='1' # load n masq modules (default: only ftp)  
MASQ_MODULE_1='ftp' # ftp
```

Evtl. sind noch weitere Module hinzuzuladen, allerdings ist das Modul 'ftp' zwingend.

Wenn auf dem Router die Dienste OPT_HTTPD und/oder OPT_FTPD genutzt werden sollen, müssen die entsprechenden Ports in der config/inet.txt bzw. config/httpd.txt angepasst werden:

config/inet.txt:

```
#-----  
-----  
# Optional package: FTPD  
#-----  
-----  
OPT_FTPD='yes' # install ftpd: yes or no  
FTPD_PORT='2121' # ftp port, see also FIREWALL_DENY_PORT_x
```

config/httpd.txt:

```
#-----  
-----  
# Optional package: HTTP-Server for Monitoring  
#-----  
-----  
OPT_HTTPD='yes' # install mini web server: yes or no  
HTTPD_PORT='8080' # http port, see also FIREWALL_DENY_PORT_x !
```

4.)

Nun ganz wichtig: die Ports 80 sowie 21 und 20, die an den maskierten Rechner im LAN weitergeleitet werden sollen, müssen aus den Firewall Regeln herausgenommen werden und (noch wichtiger!) die Ports, auf denen OPT_HTTPD und OPT_FTPD laufen, müssen mit in die Firewall Regeln aufgenommen werden (config/base.txt):

```
#-----  
-----  
# Firewall: ports to reject/deny from outside (all served ports)  
#  
# here we leave five ports untouched:  
#  
# 20 ftp-data  
# 21 ftp-control  
# 53 dns  
# 80 httpd  
# 113 auth  
#-----  
-----  
FIREWALL_DENY_PORT_N='10' # no. of ports to reject/deny  
FIREWALL_DENY_PORT_1='0:19 REJECT' # privileged ports: reject or deny  
FIREWALL_DENY_PORT_2='22:52 REJECT' # privileged ports: reject or  
deny
```

```

FIREWALL_DENY_PORT_3='54:79 REJECT' # privileged ports: reject or
deny
FIREWALL_DENY_PORT_4='81:112 REJECT' # privileged ports: reject or
deny
FIREWALL_DENY_PORT_5='114:1023 REJECT' # privileged ports: reject or
deny
FIREWALL_DENY_PORT_6='2121 REJECT' # local ftpd
FIREWALL_DENY_PORT_7='5000:5001 REJECT' # imond/telmond ports: reject
or deny
FIREWALL_DENY_PORT_8='8000 REJECT' # proxy access: reject or deny
FIREWALL_DENY_PORT_9='8080 REJECT' # local httpd
FIREWALL_DENY_PORT_10='20012 REJECT' # vbox server access: reject or
deny

```

5.)

Es wird OPT_PORTFWUP benötigt, also ist die Datei config/portfwup.txt anzupassen:

```

#-----
-----
# Optional package: PORTFWUP
#-----
-----
OPT_PORTFWUP='yes' # install PortFWup: yes or no

```

6.)

Nun müssen die Ports die weitergeleitet werden sollen in der opt/etc/portfw.sh Datei eingegeben werden.

```

#-----
-----
# Define your PCs to forward ports to:
#-----
-----
externip1=10.4.202.1 # ip of router outside
hiddenhost1=192.168.6.2 # ip of PC in LAN: change here!

/usr/sbin/ipmasqadm portfw -a -P tcp -L $externip1 80 -R $hiddenhost1 80 #example http forwarding
/usr/sbin/ipmasqadm portfw -a -P tcp -L $externip1 20 -R $hiddenhost1 20 #example http forwarding
/usr/sbin/ipmasqadm portfw -a -P tcp -L $externip1 21 -R $hiddenhost1 21 #example http forwarding

```

7.)

Zum Abschluß noch schnell eine neue Fli4l-Floppy gebacken und ab geht's!

VERBINDUNGEN ZUM ROUTER:

Die WWW und FTP Dienste auf dem Router können jetzt nur noch über die geänderten (höheren) Ports erreicht werden:

WWW (lokal auf Router):

http://192.168.6.1:8080/

FTP (lokal auf Router):

ftp://login:password@192.168.6.1:2121/

VERBINDUNGEN ZUM HIDDENHOST:

Aus dem Internet kann nun unter der öffentlichen IP-Adresse des Routers (oder bei Benutzung von OPT_DYNDNS z.B. unter meinserver.darktech.org) auf die Dienste des maskierten Rechners zugegriffen werden. Hierzu müssen keine speziellen Portangaben gemacht werden, da die Standard-Ports für WWW bzw. FTP weitergeleitet werden:

WWW (auf maskiertem Rechner):

http://meinserver.darktech.org/

FTP (auf maskiertem Rechner):

ftp://meinserver.darktech.org/

Ich denke, es ist einem selbst zumutbar, z.B. zur Netzwartung seines Routers den benutzten Port explizit anzugeben, während man für die Internetnutzer die Standardports benutzt, damit auf deren Seite nur wenige Parameter (in diesem Falle nur öffentliche IP-Adresse bzw. Hostname) einzugeben sind.

EINSCHRÄNKUNGEN:

Wenn man versucht, von einem Rechner im LAN auf den maskierten Server mittels der öffentlichen IP-Adresse des Routers zuzugreifen, wird das nicht klappen! Abhilfe schafft hier die Benutzung eines WWW bzw. FTP Proxy im Internet. T-Online z.B. bietet für seine Kunden solch einen Proxy an:

WWW-Proxy: www-proxy.btx.dtag.de:80

FTP-Proxy: ftp-proxy.btx.dtag.de:80

Der benutzte WWW bzw. FTP Client muß für die Verwendung dieser Proxys konfiguriert werden.

Fragen und Anregungen zu diesem HOWTO an
Andreas Rasztovits [Andreas Rasztovits](mailto:Andreas.Rasztovits@t-online.de)

Klicken Sie hier, um die Seite auszudrucken.