



Mini-HOWTO für WWW/FTP Server im maskierten LAN

Author: [Jens Fischer](#)

Creation: 18.04.2001 jf

Last Update: 17.04.2002 jf

VORRAUSSETZUNGEN:

- Ein lauffähiger Fli4l-Router (Version 2.0.3 oder höher) mit folgenden installierten Paketen:
 - OPT_PORTFW (Basis-Paket)
 - OPT_FTPD (inet-Paket)
 - OPT_HTTPD (httpd-paket) Beispiel-IP-Adresse dieses Rechners im HOWTO: 192.168.6.1
- 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
- Optional OPT_DYNDNS (http://www.dummzeuch.de/opt_dyndns/deutsch.html), um mittels statischem Hostnamen für die dynamische IP-Adresse einen leichten Zugriff auf den Router aus dem Internet zu haben.
Beispiel-Hostname im HOWTO: meinserver.darktech.org
- [Dateien zum Howto](#)

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:

Alle Anfragen aus dem Internet an den Router auf den Ports 80 (HTTP) sowie 21 (FTP-Control) 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 ab, sowie läßt Anfragen auf den Ports 8080 und 2121 durch! Die Regeln müssen dahingehend geändert werden, daß die Ports 80 und 21 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='2' # how many portforwardings to set up  
PORTFW_1='21 192.168.6.2:21 tcp' # FTP-CONTROL  
PORTFW_2='80 192.168.6.2:80 tcp' # HTTP
```

Direkte Änderungen an der Datei opt/etc/portfw.sh sind seit der Fli4l Version 2.0.1 nicht mehr nötig!

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.

Weiterhin müssen noch ein paar Änderungen an einer zentralen Datei vorgenommen werden:

Austauschen der Datei opt/etc/rc.d/masq durch folgende Datei:

```
----- [snip] -----  
-----  
#-----  
-----  
# /etc/rc.d/masq - install masquerading modules  
#  
# Creation: 31.03.2000 fm
```

```
# Last Update: 17.04.2002 jf
```

```
#-----  
-----
```

```
/usr/local/bin/colecho "installing masquerading modules ..." gn
```

```
if [ "$MASQ_DO_DEBUG" = yes ]  
then  
set -x  
fi
```

```
idx=1
```

```
while [ "$idx" -le "$MASQ_MODULE_N" ] # masquerading modules (ftp  
etc)
```

```
do  
eval drv='$MASQ_MODULE_'$idx
```

```
case "$drv"
```

```
in
```

```
"udp_dloose")
```

```
echo 1 > /proc/sys/net/ipv4/ip_masq_udp_dloose
```

```
;;
```

```
"ftp")
```

```
options=""
```

```
delim="ports="
```

```
port_idx=1
```

```
while [ "$port_idx" -le "$MASQ_FTP_PORT_N" ]
```

```
do
```

```
eval newport='$MASQ_FTP_PORT_'$port_idx
```

```
options="$options$delim$newport"
```

```
delim=","
```

```
port_idx=`/usr/bin/expr $port_idx + 1`
```

```
done
```

```
delim=" in_ports="
```

```
port_idx=1
```

```
while [ "$port_idx" -le "$MASQ_FTP_IN_PORT_N" ]
```

```
do
```

```
eval newport='$MASQ_FTP_IN_PORT_'$port_idx
```

```
options="$options$delim$newport"
```

```
delim=","
```

```
port_idx=`/usr/bin/expr $port_idx + 1`
```

```
done
```

```

/sbin/insmod ip_masq_ftp $options
;;
*)
/sbin/insmod ip_masq_$drv
;;
esac

```

```

idx=`/usr/bin/expr $idx + 1`
done

```

```
set +x
```

```

-----[ snap]-----
-----

```

Ergänzen der Datei check/base.txt:

```

MASQ_FTP_IN_PORT_N MASQ_NETWORK - NUMERIC
MASQ_FTP_IN_PORT_% MASQ_NETWORK MASQ_FTP_IN_PORT_N NUMERIC

```

Ergänzen der Datei config/base.txt:

```

MASQ_FTP_IN_PORT_N='1'
MASQ_FTP_IN_PORT_1='21'

```

Hiermit wird eine automatische Unterstützung für PASSIVE FTP durch das FTP Masquerading Modul aktiviert. Die Variable MASQ_FTP_IN_PORT_1 gibt jetzt an, auf welchem Port der FTP-Server im maskierten LAN läuft, in unserem Beispiel auf Port 21.

3.)

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, 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:
#
# 21 ftp-control
# 53 dns
# 80 httpd
# 113 auth
#-----
-----
FIREWALL_DENY_PORT_N='10' # no. of ports to reject/deny
FIREWALL_DENY_PORT_1='0:20 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
```

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

(Ich habe es jedoch bisher noch nicht hingekriegt, eine Verbindung über einen FTP Proxy hinzubekommen!)

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

Durch die Verwendung des Parameters `MASQ_FTP_IN_PORT_1='21'` ist es nun auch endlich möglich, den FTP Server im PASSIVE Modus (wie es viele WWW Browser benutzen) zu erreichen. Den Tipp

hierfür habe ich von [Oliver Walter](#) erhalten. Weiterhin hilfreich bei der Lösung des PASSIVE FTP Problems war die

Seite <http://www.slacksite.com/other/ftp.html>

AUSSICHT:

In Zukunft werde ich versuchen, auch FXP mit dem FTP Modul bewerkstelligen zu können. Für den experimentierfreudigen Leser: den Quellcode eines gepatchten ip_masq_ftp Moduls kann man unter http://www.algonet.se/~cyrano/ip_masq_fxp.html herunterladen.

Fragen und Anregungen zu diesem HOWTO an
[Jens Fischer](#)

Klicken Sie hier, um die Seite auszudrucken.