

pf FTP ftp-proxy rules question for a firewall

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.bsd.openbsd.misc/2006-03/msg00108.html>

- *From:* "none" <mikem891@xxxxxxxxxxxxx>
 - *Date:* 30 Mar 2006 11:14:50 -0800
-

Hi, I'm trying to configure my openbsd 3.8 firewall to allow FTP access to only certain hosts on my network. I want to filter which host will be able to access certain services (like HTTP, FTP) on the internet instead of using a ALLOW everything OUT setup.

I really had a hard time with FTP, at first I wanted to deny by default everything on the int_if (in) from the network and allow access only to certain hosts, but I was not able to make it work with FTP. So what I did instead is allow everything in/out to int_if but block everything in/out by default on ext_if and only allow out (keep state) on ext_if to selected hosts.

Now it works with FTP but I'm concern that my rules are too permissive. I'm a bit concern with the pass from \$ext_if port > 49151 to any rule. I don't understand why I need it for passive mode to work, everytime I saw this rule on the internet it was for active mode, but my active mode works without it and passive mode do not work without it. Why the pass pass out ext_if user proxy rule do not work for passive mode?

Anyway, do you have any suggestions, tips?
I'm I too permissive for what I want to do (allow access to the internet services only to selected hosts)?

Thanks in advance.

Here's a sample of my configurations and rules set:

```
/etc/inetd.conf:  
127.0.0.1:8021 stream tcp nowait root /usr/libexec/ftp-proxy ftp-proxy  
-n -u proxy
```

/etc/pf.conf sample:

pf FTP ftp-proxy rules question for a firewall

```
ext_if = "ne1"
int_if = "ne0"

ALLOWEDFTPHOSTS = "192.168.1.2"

nat on $ext_if inet from $MYNETWORK to any -> ($ext_if)

rdr on $int_if proto tcp from any to any \
port 21 -> 127.0.0.1 port 8021

# Block INPUT from WAN
block in log on $ext_if all

# Block OUTPUT from WAN
block out log on $ext_if all

# Allow LAN out
pass out on $int_if all keep state

# Allow LAN in
pass in on $int_if all keep state

# Allow DNS UDP traffics from all machines
pass out quick on $ext_if \
inet proto udp from any to any \
port 53 keep state

# FTP proxy to allow passive connections to go out:
pass out quick on $ext_if \
inet proto tcp \
from ($ext_if) to any \
port ftp flags S/SAFRUP keep state
pass out quick on $ext_if \
inet proto tcp \
from ($ext_if) to any \
user proxy flags S/SAFRUP keep state

# FTP Proxy to allow active connections to get in:
pass in quick on $ext_if \
inet proto tcp from \
any to ($ext_if) \
user proxy flags S/SAFRUP keep state

# I need this to make use passive mode, I don't know why
# And I don't know if it's too permissif
pass out quick on $ext_if \
inet proto tcp \
from $ext_if port > 49151 to any \
flags S/SA modulate state
```

pf FTP ftp-proxy rules question for a firewall

```
# Only allow FTP access to specific hosts
pass in quick on $int_if \
inet proto tcp \
from $ALLOWEDFTPHOSTS to 127.0.0.1 \
port 8021 keep state
```

```
# Block FTP access by default
block in log quick on $int_if \
inet proto tcp from any to 127.0.0.1 port 8021
```
