

## PF und FTP-Clients

### Aktives FTP:

Der Client initiiert die Kontrollverbindung (Ziel-Port 21).  
Über die Kontrollverbindung wird dem Server ein zufälliger Port des Clients mitgeteilt. Zu diesem Port wird danach vom FTP-Server aus die Datenverbindung (Absende-Port 20) aufgebaut.  
Diese Art der Verbindung bedeutet für eine normale NAT-Firewall, dass eine Verbindung von einem beliebigen Rechner zu einem beliebigen Port auf der Firewall selbst aufgebaut wird. Eine solche Verbindungsanfrage wird selbstverständlich nicht zugelassen.

### Passives FTP:

Auch hier initiiert der Client die Kontrollverbindung (Port 21).  
Der Server wird beim passiven FTP aufgefordert, einen beliebigen Port als Ziel für die Datenverbindung auszuwählen. Zu diesem Port wird dann vom Client aus die Datenverbindung aufgebaut.  
Hier liegt das Problem bei der Firewall, die vor dem FTP-Server steht. Diese muss von beliebigen Clients Verbindungen zu beliebigen Ports auf dem FTP-Server zulassen.

### Modifikationen unter OpenBSD für Aktives FTP

Es wird der unter OpenBSD vorhandene FTP Proxy Server verwendet (ftp-proxy)

#### */etc/services*

```
ftp-proxy 8021/tcp # ftp-proxy
```

#### */etc/inetd.conf*

```
ftp-proxy stream tcp nowait root /usr/libexec/ftp-proxy ftp-proxy \  
-u proxy -m 55000 -M 57000 -t 180
```

-u gibt den User an, unter dem der Proxy-Dienst läuft  
-m ist die untere Grenze für die Ports der Datenverbindung  
-M ist die obere Grenze für die Ports der Datenverbindung  
-t Timeout

Anschließend muss der inetd seine Konfigurationsdatei neu einlesen.

```
kill -HUP `cat /var/run/inetd.pid`
```

Umleiten der Client-Requests auf den FTP-Proxy:

#### */etc/pf.conf*

rdp on \$int\_if proto tcp from \$int\_ip to any port 21 -> 127.0.0.1 port 8021

Zulassen der Antworten des FTP-Servers:

***/etc/pf.conf***

```
pass in on $ext_if inet proto tcp from any port 20 \
    to $ext_if port 55000 >< 57000 user proxy flags S/SA keep state
```

```
pass out on $ext_if inet proto tcp from $ext_if to any \
    port 20 flags S/AUPRFS modulate state
```

Laden der Modifikationen:

***pfctl -f /etc/pf.conf***

Für die Bereitstellung von aktivem FTP wird auf der Firewall weder IP-Forwarding noch NAT benötigt!

### **Modifikationen unter OpenBSD für Passives FTP**

NAT muss auf der Firewall angeschaltet werden, falls dies nicht schon geschehen ist.

Neue Regeln für den Paketfilter:

***/etc/pf.conf***

```
pass out on $ext_if inet proto tcp from $ext_if to any port 21 \
    flags S/AUPRFS modulate state
```

```
pass out on $ext_if inet proto tcp from $ext_if to any port > 1024 \
    flags S/AUPRFS modulate state
```

Der FTP-Proxy braucht die Information, dass er für passive Datenverbindungen nicht als Proxy agiert, wenn NAT eingeschaltet ist:

***/etc/inetd.conf***

```
ftp-proxy stream tcp nowait root /usr/libexec/ftp-proxy ftp-proxy -n \
    -u proxy -m 55000 -M 57000 -t 180
```