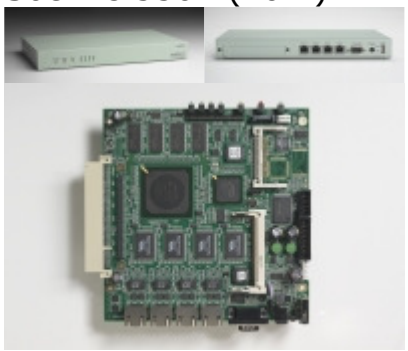
| | | |
|---|---|---|
| Hardware | => | Soekris 5501 (10W) |



| | | |
|---|---|---|
| Tools | => | USB naar Serial Adapter voor Console<br>Putty voor Terminal sessie middels USB Serial Adapter |
| Operating System | => | OpenBSD 4.8 |
| Software | => | PF |

Inleiding:

Voor alle interfaces wordt hierin bepaald welk verkeer mogelijk is, van buiten naar binnen en van binnen naar buiten.
Aangezien het een Statefull Firewall is zullen alle verbindingen ook weer in teruggaande richting worden doorgelaten.
Alle Rules noodzakelijk voor de services die op de CF zijn geïnstalleerd worden hier beschreven.
In dit document wat noodzakelijk ter verbetering van de basisinstallatie, alle andere toevoegingen worden besproken waar noodzakelijk in de betreffende HowTo.

Behalve dit komt het natuurlijk voor dat bepaalde applicaties alleen naar buiten toe goed functioneren indien de benodigde poort(en) worden opengezet.
Het kan dan gaan om een UDP of TCP poort, of beide.
Ter voorkoming van misbruik dienen geen overbodige poorten open te staan, let daar dus goed op.

Installatie PF:

PF is reeds geïnstalleerd tijdens de basisinstallatie.
Zie volgende stap voor configuratie.

Houdt de ingevulde variabelenlijst van de **Bijlage Variabelen** in het inleidende document **HowTo OpenBSD Firewall met Secure Anonymous Access** bij de hand tijdens instalatie/configuratie.
Zodra je een variabele ziet, bv `%HOST%` vervang dit dan in zijn geheel door wat je had ingevuld, dus zeker geen %-tekens achterlaten.

Configuratie PF:

Bewaar eerst kopie van de originele configuratie.

```
root @ 10.0.10.1 - PuTTY [ksh]
# cp -p /etc/pf.conf /etc/pf.conf.org
```

Pas nu aan zoals onderstaand.

```
root @ 10.0.10.1 - PuTTY [vi /etc/pf.conf]
#########################################################################
#######
###                                pf.conf
###
#########################################################################
#######

###                        Firewall Configuratie
###
#
# Geen ONNODIGE tcp/udp poorten openen
# Poort 3544 voor teredo ip6to4 tunnel NIET aanzetten, verkeer
onduidelijk, gaat dwars door firewall...

# 465  = Secure SMTP Poort XS4ALL     # 4000 = TWS
# 995  = Secure POP Poort XS4ALL      # 4001 = TWS SSL
# 1626 = Shockwave                    # 8021 = FTP Client Redirection
# 3128 = SQUID Proxy

### Macro's
#
ext_if                  = "vr0"
int_if                  = "vr1"
localnet                = $int_if:network
#nameservers            = "10.0.10.1" # Activeer zodra Local DNS
Actief
```

```
nameservers             = "{ %NS1%, %NS2% }" # Eigen Provider
udp_services            = "{ domain, ntp }"
netbios_services        = "{ netbios-ns, netbios-dgm, netbios-ssn }"
bootp_services          = "{ bootps, bootpc }"
icmp_types              = "{ echoreq, unreach }"
local_services          = "{ smtp, auth }"
messenger_udp_services = "{ 9, 1863, 7001 }"
messenger_tcp_services = "{ 1863, 1935, 5061, 7001 }"
skype_services          = "{ 4831, 5351 }"
octoshape_services      = "{ 554, 5060, 6970, 8247 }" # Voor flash
(bv tbv cnn)
client_out              = "{ ftp-data, ssh, domain, smtp, pop3, auth,
nntp, cvspserver, 465, 995, 1626, 4000, 4001, http, https }"

### Settings
#
set block-policy return
set skip on lo                          # Sta alle verkeer toe onder
localhost(s)

### Sodemieters Aanpakken en Opschonen
#
antispoof for $ext_if
antispoof for $int_if
match in all scrub (no-df max-mss 1472) # ping -c 1 -s 1472 -D
89.31.96.40

### Rules
#
block log all                           # Eerst deuren dicht, dan
kiertjes openen
block drop in log on $ext_if            # Drop op wan IN, rest reject

# NAT Uitgaande Verbindingen
match out on $ext_if from !$ext_if to any nat-to $ext_if

# Local broadcast toelaten in int_if ter voorkoming vollopen log,
zolang het maar in localnet blijft
```

```
pass in  quick on $int_if inet proto udp from $localnet to {
$localnet, 10.0.10.255/32 }
pass in  quick on $int_if inet proto udp from $localnet to $localnet
port $netbios_services
pass in  quick on $int_if inet proto udp from $localnet to {
$localnet, 224.0.0.0/4 } # Local Broadcast voor Routing/Name
Resolution/ e.d.

# BOOTP/DHCP indien ext adres via Router
pass out quick on $ext_if inet proto udp from $ext_if to 10.0.0.1/32
port $bootp_services

# FTP Redirection
anchor "ftp-proxy/*"
pass in  quick on $int_if inet proto tcp from $localnet to any port
ftp rdr-to lo0 port 8021
pass out quick on $ext_if inet proto tcp from lo0 to any port ftp

# HTTP/HTTPS tbv pkg_add en wget
pass out quick on $ext_if inet proto tcp from lo0 to any port {
http, https }

# Diverse ICMP Services
pass     quick inet proto icmp all icmp-type $icmp_types

# Diverse Lokale Services
pass in  quick inet proto tcp from $ext_if to lo0 port
$local_services

# Name Service
pass in  inet proto { tcp, udp } from $nameservers to any port
domain
pass out inet proto { tcp, udp } from any to $nameservers port
domain

# Diverse UDP Services
pass     quick inet proto udp from { $localnet, $ext_if } to any
port $udp_services
```

```
# Diverse Client Services
pass in  quick inet proto tcp from $localnet to any port $client_out
pass out quick inet proto tcp from { $localnet, $ext_if } to any
port $client_out

# Messenger Audio/Video
pass     quick inet proto tcp from $localnet to any port
$messenger_tcp_services
pass     quick inet proto udp from $localnet to any port
$messenger_udp_services

# Skype Audio/Video
pass     quick inet proto tcp from $localnet to any port
$skype_services

# Octoshape Audio/Video
pass     quick inet proto tcp from $localnet to any port
$octoshape_services
```

Instellen startparameters en zorgt voor opstarten bij boot.

```
root @ 10.0.10.1 - PuTTY [vi /etc/rc.conf.local]
ftpproxy_flags=""            # FTP Client Achter Firewall
```

Post-Configuratie PF:

Opnieuw inlezen configuratie na aanpassing `pf.conf`.
Eerst middels –n kijken of er geen fouten zijn gemaakt, indien je niets op het scherm ziet is de syntax ok.

```
root @ 10.0.10.1 - PuTTY [ksh]
# pfctl -nf /etc/pf.conf
```

Indien syntax ok nogmaals uitvoeren met werkelijk resultaat.

```
root @ 10.0.10.1 - PuTTY [ksh]
# pfctl -f /etc/pf.conf
```

Controle werking:

Kijk of je browser werkt met pagina naar keuze.
Doe hetzelfde met https pagina.
Download een bestand middels ftp.
Bekijk de firewall log op de console, deze bevat wat wordt tegengehouden.

```
root @ 10.0.10.1 - PuTTY [ksh]
# tcpdump -s 1500 -Xlnettti pflog0
```

Alle verkeer van de interface kun je zien als je deze gebruikt ipv `pflog0`.

```
root @ 10.0.10.1 - PuTTY [ksh]
# tcpdump -s 1500 -Xlnettti vr0
```

Links:

http://www.openbsd.org/
http://home.nuug.no/~peter/pf/en/
http://www.chiark.greenend.org.uk/~sgtatham/putty/

Boeken:

The book of PF