
Proxy, Tallafocs i IDS amb OpenBSD



Marc Serra <nandelbosc@s3os.net>

Copyright © 2005 Solucions i Serveis amb Sistemes Open Source (www.s3os.net)

Després de llegir aquest document hauríem de ser capaços de crear desde zero un tallafocs per a la nostra xarxa, amb funcions de proxy-cache i detector d'intrusions, tot amb el sistema operatiu OpenBSD.

El host en qüestió serà en Musclu.

Table of Contents

Instal·lació del s.o.	2
Aconseguir els fitxers necessaris	2
Arrencada	2
Particionament del disc	2
Configuració de la xarxa	4
Mitjà d'instal·lació	4
Compilant el nucli	5
Notes de seguretat	5
Instal·lació del tallafocs Packet Filter	6
Habilitar PF	6
Engegar i parar PF	6
Algunes ordres addicionals... ..	7
El fitxer de configuració	7
Instal·lació del Proxy-Cache	9
Preparació del disc	9
Descarregar i instal·lar l'aplicació	9
Detalls a tenir en compte	10
Fitxer de configuració	10
Primera inicialització d'squid	12
Permisos d'squid	12
IDS, detector d'intrusions	13
Aconseguir els fitxers necessaris i instal·lació	13
Configuració i arrencada	13

Instal·lació del s.o.

OpenBSD, un sistema operatiu de codi lliure, és un dels sistemes més segurs que podem trobar, un clar exemple: un sol forat de seguretat (remot) en l'instal·lació per defecte en més de 8 anys!

Aconseguir els fitxers necessaris

Per poder instal·lar aquest sistema és necessari que descarreguem els següents fitxers:

- cdXX.iso: l'imatge per a l'instal·lació.
- baseXX.tgz: la base del sistema.
- bsd: el nucli.
- compXX.tgz: el compilador.
- etcXX.tgz: les configuracions bàsiques.
- manXX.tgz: les pàgines dels manuals.
- sys.tar.gz: sistema.
- src.tar.gz: fonts.

XX és la versió, actualment 3.6 (XX=36). Tots ells els podem trobar a <ftp://ftp.rediris.es/mirror/OpenBSD/>. Un cop descarregats, ja els podem grabar a un cd.

Arrencada

Un cop tenim el disc amb els fitxers necessaris podem procedir a l'arrencada del mateix. Ens apareixerà un menú interactiu, anirem apretant les següents tecles:

```
i -> per instal·lar... retorn per escollir el terminal per \\  
defecte (vt220)  
yes -> per escollir el teclat  
es -> teclat espanyol  
yes -> aquí vigilem... esborra tot el disc i el prepara per \\  
instal·lar
```

Ens mostra els discs disponibles, en aquests cas sd0 (per l'SCSI) i wd0 (per l'IDE), li hem de dir quin volem utilitzar...

Particionament del disc

```
wd0 -> en aquest cas s'instal·larà al disc IDE  
yes -> per utilitzar tot l'espai
```

Ara entrem a l'editor d'etiquetes (disk label), podem prémer "?" en qualsevol moment per l'ajuda. Un "bon" exemple de particionament:

```
>aa
offset: [3069360] Enter
size: [36030960] 150M
Rounding to nearest cylinder: 307440
FS type: [4.2BSD] Enter
mount point: [none] /
>ab
offset: [3376800] Enter
size: [35723520] 64M
Rounding to nearest cylinder: 614880
FS type: [swap] Enter
>ad
offset: [3991680] Enter
size: [35108640] 100M
Rounding to nearest cylinder: 245952
FS type: [4.2BSD] Enter
mount point: [none] /tmp
>ae
offset: [4237632] Enter
size: [34862688] 80M
Rounding to nearest cylinder: 164304
FS type: [4.2BSD] Enter
mount point: [none] /var
>ag
offset: [4401936] Enter
size: [34698384] 500M
Rounding to nearest cylinder: 4194288
FS type: [4.2BSD] Enter
mount point: [none] /usr
>ah
offset: [8596224] Enter
size: [30504096] Enter
Rounding to nearest cylinder: 8388576
FS type: [4.2BSD] Enter
mount point: [none] /home
>pm
```

La teoria del què hem fet...

```
p m -> mostra l'actual etiquetatge
d a -> esborra la partició "a"
d b -> esborra la partició "b"
d d -> esborra la partició "d"
...
a a -> crea la primera partició
a b -> crea la segona partició
...
```

Si tot és correcte, sortim i guardem...

```
>q
Write new label?: [y] Enter
The root filesystem will be mounted on wd0a.
wd0b will be used for swap space.
Mount point for wd0d (size=122976k), none or done? [/tmp] Enter
Mount point for wd0e (size=82152k), none or done? [/var] Enter
Mount point for wd0g (size=2097144k), none or done? [/usr] Enter
Mount point for wd0h (size=4194288k), none or done? [/home] Enter
Mount point for wd0d (size=122976k), none or done? [/tmp] done
Done - no available disks found.
You have configured the following partitions and mount points:
```

```
wd0a /
wd0d /tmp
wd0e /var
wd0g /usr
wd0h /home
```

```
The next step creates a filesystem on each partition, ERASING \\
existing data.
Are you really sure that you're ready to proceed? [no] yes
/dev/rwd0a:      307440 sectors in 305 cylinders of 16 tracks, 63 \\
sectors 150.1MB in 20 cyl groups (16 c/g, 7.88MB/g, 1920 i/g)
/dev/rwd0d:      245952 sectors in 244 cylinders of 16 tracks, 63 \\
sectors 120.1MB in 16 cyl groups (16 c/g, 7.88MB/g, 1920 i/g)
/dev/rwd0e:      164304 sectors in 163 cylinders of 16 tracks, 63 \\
sectors 80.2MB in 11 cyl groups (16 c/g, 7.88MB/g, 1920 i/g)
/dev/rwd0g:      4194288 sectors in 4161 cylinders of 16 tracks, 63 \\
sectors 2048.0MB in 261 cyl groups (16 c/g, 7.88MB/g, 1920 i/g)
/dev/rwd0h:      8388576 sectors in 8322 cylinders of 16 tracks, 63 \\
sectors 4096.0MB in 521 cyl groups (16 c/g, 7.88MB/g, 1920 i/g)
/dev/wd0a on /mnt type ffs (rw, asynchronous, local, ctime=Thu Oct \\
10 21:50:36 2 002)
/dev/wd0h on /mnt/home type ffs (rw, asynchronous, local, nodev, \\
nosuid, ctime=Thu Oct 10 21:50:36 2002)
/dev/wd0d on /mnt/tmp type ffs (rw, asynchronous, local, nodev, \\
nosuid, ctime=Thu Oct 10 21:50:36 2002)
/dev/wd0g on /mnt/usr type ffs (rw, asynchronous, local, nodev, \\
ctime=Thu Oct 10 21:50:36 2002)
/dev/wd0e on /mnt/var type ffs (rw, asynchronous, local, nodev, \\
nosuid, ctime=Th u Oct 10 21:50:36 2002)
```

Configuració de la xarxa

Per configurar la xarxa seguim els següents passos:

```
System hostname? musclu
Configure the network? [yes] Return
Li diem quina NIC volem configurar "rll"
Configure the network? [yes] Enter
Which one do you wish to initialize? (or 'done') [rll] Enter
Symbolic (host) name for rll? [musclu] Enter
The default media for rll is media: Ethernet autoselect \\
(100baseTX full-duplex)
Do you want to change the default media? [no] Enter
IP address for rll? (or 'dhcp') 192.168.1.5
Netmask? [255.255.255.0] Enter
Done - no available interfaces found.
DNS domain name? (e.g. 'bar.com') [my.domain] s3os.net
DNS nameserver? (IP address or 'none') [none] 80.58.0.97
Use the nameserver now? [yes] Enter
Default route? (IP address, 'dhcp' or 'none') 192.168.1.1
add net default: gateway 192.168.1.1
Edit hosts with ed? [no] Enter
Do you want to do any manual network configuration? [no] Enter
Password for root account? (will not echo) cOnTRasenya
Password for root account? (again) cOnTRasenya
```

Mitjà d'instal·lació

Podem instal·lar desde xarxa (http, ftp), desde cd, ... En aquest cas ho farem desde el mateix cd que hem

arrencat.

```
c -> desde cd
cd0 -> quin dels possibles lectors de la nostra màquina
/ -> si tenim els fitxers a l'arrel del disc
```

Responem "yes" a totes les qüestions fins:

```
Sets can be located on a (m)ounted filesystem; a (c)drom, (d)isk or (t)ape
device; or a (f)tp, (n)fs or (h)ttp server.
Where are the install sets? (or 'done')
```

Escriurem "done" i seguim...

```
Do you wish sshd(8) to be started by default? [yes] y
Do you expect to run the X Window System? [yes] n
What timezone are you in? ('?' for list) [US/Pacific] Europe
What sub-timezone of 'US' are you in? ('?' for list) Andorra
"Halt"
```

Reiniciem...

Compilant el nucli

Ja tenim el sistema apunt, ara recompilem el kernel segons el nostre "hard".

```
# mkdir /mnt/cdrom
# mount /dev/cd0a /mnt/cdrom
# cd /usr/src
# tar -xzf /mnt/cdrom/sys.tar.gz
# umount /mnt/cdrom
# cd sys/arch/$ARCH/conf/
# vi GENERIC
```

Triem la CPU i comentem les línies que calgui (fitxer GENERIC.txt, a la versió Online)

```
# config GENERIC
# cd ../compile/GENERIC
# make depend
# make
# cp /bsd /bsd-original
# cp bsd /bsd
```

Nucli compilat!

Notes de seguretat

El nostre sistema ja està apunt, però mai estàn de més uns apunts de seguretat... No volem que l'usuari root es connecti via SSH, hi ha scripts que "fàcilment" ens podrien comprometre el nostre tallafocs.

```
# adduser admin -group wheel
# vi /etc/ssh/sshd_config
    Permitrootlogin no
```

Si la data no és la correcte...

```
# date AAAAMDDHHMM
```

Activem el reenviament de paquets entre interfícies...

```
# vi /etc/sysctl.conf
    net.inet.ip.forwarding=1
# sysctl -w net.inet.ip.forwarding=1 (perquè els canvis tinguin efecte)
```

A partir d'ara, si només volem tenir ip fixa...

```
# vi /etc/hostname.r10
    inet 192.168.1.10 255.255.255.0 NONE
# vi /etc/hostname.r11
    inet 192.168.10.1 255.255.255.0 NONE
```

o bé...

```
dhclient r10
dhclient r11
```

o bé...

```
# echo>/etc/hostname.r10 dhcp
# echo>/etc/hostname.r11 dhcp
```

Servidors de dominis, porta d'enllaç...

```
# nano /etc/resolv.conf
    dns1
    dns2
# nano /etc/mygate
    192.168.1.1
# sh /etc/netstart
```

Ara si, ja hem acabat amb el S.O., anem a convertir-lo en tallafocs.

Instal·lació del tallafocs Packet Filter

OpenBSD utilitza Packet Filter (aka PF) enlloc del conegut IpTables; veurem que les normes segueixen una sintaxis molt semblant. Aquesta distribució ja porta per defecte el tallafocs (és a nivell de nucli), per tant no necessitarem paquets addicionals per instal·lar-lo.

Habilitar PF

Simplement editem el fitxer /etc/rc.conf

```
# vi /etc/rc.conf
```

i canviem "pf=NO" per "pf=YES"

Engegar i parar PF

Com a mínim hem de saber aquestes dues comandes:

```
# pfctl -e -> engega el pf
# pfctl -d -> para el pf
```

Algunes ordres addicionals...

Sempre poden ser útils:

```
# pfctl -f /etc/pf.conf          -> Carrega el fitxer pf.conf
# pfctl -nf /etc/pf.conf        -> Analitza el fitxer, però no el carrega
# pfctl -Nf /etc/pf.conf        -> Només NAT
# pfctl -Rf /etc/pf.conf        -> Només normes de filtrat
# pfctl -sn                     -> Mostra normes NAT
# pfctl -sr                     -> Mostra normes filtrat
# pfctl -ss                     -> Mostra la taula d'estat
# pfctl -si                     -> Mostra estadístiques i contadors de filtrat
# pfctl -sa                     -> Mostra tot
```

El fitxer de configuració

Quan engeguem/carreguem el PF, si no li diem el contrari, va a buscar el fitxer pf.conf al directori /etc. Aquí tenim un exemple de configuració, els comentaris són suficients per entendre-ho...

```
#MACROS (variables)
ext_if="rl0"
int_if="rl1"

tcp_services="{22, 80, 20986, 5222, 113, 53, 25, 143, 443, 993, 21}" \
    #Ports TCP que podrà anar la LAN a internet
udp_services="{53, 123, 32783, 32786, 32785, 32784, 32842}" \
    #Ports UDP que podrà anar la LAN a internet
icmp_types = "echoreq" #Tipus paquets icmp que acceptem

servers="{192.168.0.2, 192.168.0.3, 192.168.0.4}" #Llista dels \
    servidors de la LAN
router="192.168.1.1" #Router que ens dóna accés a internet
router_w="192.168.123.1" #Router que ens subministra xarxa sense fils
#all_routers="{ $router $router_w }" #Exemple de llista de variables
#priv_nets="{127.0.0.0/8, 192.168.1.0/24, 192.168.0.0/24}" #Xarxes \
    privades (podrien ser útils)
s_ssh="192.168.0.2" #Servidor ssh (peixglobo)
s_web="192.168.0.3" #Servidor web (cangreju)
s_dns="192.168.0.4" #Servidor dns (pop)
s_correu="192.168.0.6" #Servidor de correu (bacallà)
s_cvs="192.168.0.6" #Servidor cvd (bacallà)
#lan_net="192.168.0.0/24" #La nostra LAN
tracerouteUDP="{ 33434 >< 33525 }" #D'aquesta manera podrem \
    utilitzar el traceroute desde la nostra LAN
IpsExtAllow="{213.97.38.x, 213.97.38.x, 192.168.1.111, 80.33.92.x}" \
    #Ip's privilegiades (per ssh i cvs)
IpsExtAllowPlus="{213.97.38.x, 213.97.38.x, 80.59.247.49, 80.33.92.x, \
    192.168.1.111}" #Ip's privilegiades exteses (per ssh i cvs)
```

```

#OPCIONES
set block-policy return #S'estableix política de bloquejar
set loginterface $ext_if #Logging a la interfície exterior

#NORMALITZACIÓ DE PAQUETS
scrub in all

#NAT/REDIRECCIONAMENT
nat on $ext_if from $int_if:network to any -> $ext_if
rdr on $ext_if proto tcp from $IpsExtAllow to $ext_if port 22 -> \
    $s_ssh port 22 #Servei accessible dsd internet al server SSH1
rdr on $ext_if proto tcp from any to $ext_if port 21 -> $s_ssh port 21 \
    #Servei accessible dsd internet al server FTP
rdr on $ext_if proto tcp from any to $ext_if port 80 -> $s_web port 80 \
    #Servei accessible dsd internet al server WEB
rdr on $ext_if proto tcp from any to $ext_if port 8080 -> $s_web port \
    8080 #Servei accessible dsd internet al server WEB
rdr on $ext_if proto udp from any to $ext_if port 53 -> $s_dns port \
    53 #Servei accessible dsd internet al server DNS (udp)
rdr on $ext_if proto tcp from any to $ext_if port 53 -> $s_dns port \
    53 #Servei accessible dsd internet al server DNS (tcp)
rdr on $ext_if proto tcp from any to $ext_if port 3306 -> $s_web port \
    3306 #Servei accessible dsd internet al server MySQL
rdr on $ext_if proto tcp from $IpsExtAllowPlus to $ext_if port 222 -> \
    $s_web port 22 #Servei accessible dsd internet al server SSH2
rdr on $ext_if proto tcp from $IpsExtAllow to $ext_if port 223 -> \
    $s_cvs port 22 #Servei accessible dsd internet al server CVS
rdr on $ext_if proto udp from any to $ext_if port 143 -> $s_correu \
    port 143 #Servei accessible dsd internet al server IMAP

#FILTRAT
block in all #Política de bloquejar tot el que entra, si abans no \
    troba alguna coincidència
block out all #Política de bloquejar tot el que surt

pass quick on lo0 all #Al loopback, via lliure
antispoof quick for $int_if inet #No fos cas que tinguessim algú \
    molt dolent entre nosaltres ;)

#DE LA LAN AL FIREWALL
pass in on $int_if proto tcp from $int_if:network to $int_if port 22 \
    #Només ens podem connectar al tallafocs desde la LAN
pass out on $int_if from $int_if to $int_if:network #Del tallafocs a \
    la xarxa local, passa tot

#TRAFIC INTERN LLIURE
pass in quick on $int_if all
pass out quick on $int_if all

#SERVEIS QUE PODRÀ ANAR LA LAN A INTERNET
#pass out quick on $ext_if inet from any to any flags S/SA modulate \
    state #Si comentem les dues següents, descomentem aquesta
pass out quick on $ext_if inet proto tcp from any to any port \
    $tcp_services flags S/SA modulate state #La LAN pot anar \
    als ports de la llista TCP
pass out quick on $ext_if inet proto udp from any to any port \
    $udp_services keep state #La LAN pot anar als ports de la llista U

#PERMETEM TRACERROUTE DE DINS A FORA
pass out quick on $ext_if inet proto udp from any to any port \
    $tracerouteUDP keep state #Com s'ha comentat abans, podem fer tra

#PERMETEM PING CAP A L'EXTERIOR

```

```
pass out quick on $ext_if inet proto icmp all icmp-type 8 code 0 \\  
    keep state  
  
#PERMETEM TRÀFIC FINS ALS SERVERS  
pass in quick proto tcp from $IpsExtAllow to $s_ssh port = 22 keep state  
pass in quick proto tcp from any to $s_ssh port = 21 keep state  
pass in quick proto tcp from any to $s_web port = 80 keep state  
pass in quick proto tcp from any to $s_web port = 8080 keep state  
pass in quick proto udp from any to $s_dns port = 53 keep state  
pass in quick proto tcp from any to $s_dns port = 53 keep state  
pass in quick proto tcp from any to $s_web port = 3306 keep state  
pass in quick proto tcp from $IpsExtAllowPlus to $s_web port = 22 keep \\  
    state  
pass in quick proto tcp from $IpsExtAllow to $s_cvs port = 22 keep \\  
    state  
pass in quick proto udp from any to $s_correu port = 143 keep state
```

Instal·lació del Proxy-Cache

Squid és el nom de l'aplicació que utilitzarem per tenir un proxy-cache a la nostra xarxa local.

Preparació del disc

Squid pot treballar amb la cache ubicada a una partició lògica, però us recomano que si teniu un disc diferent del què hi ha el S.O. instal·lat, l'utilitzeu per a la cache. En aquest cas farem servir un disc SCSI d'1GB. Editem el disc:

```
# disklabel -E /dev/sd0c  
  
UN COP DINS L'ETIQUETADOR, QUÈ HEM DE SABER:  
  
d x ("x" son les particions a eliminar (a, b, d,... la c no \\  
    la borrem))  
a a # creem partició "a"  
"return" # on comença  
"return" # on acaba (en aquest cas tot \\  
    el disc)  
"return" # triem sistema de fitxers  
w # guardem  
q # sortim
```

I el formatem...

```
# newfs /dev/sd0c
```

Muntem el dispositiu al directori on tindrem els fitxers de la cache i ho afegim a /etc/fstab, d'aquesta manera es muntarà a l'inici

```
# mount /dev/sd0c /var/squid/cache  
# echo>>/etc/fstab /dev/sd0c /var/squid/cache ffs rw 1 1
```

Ja tenim el disc apunt ;))

Descarregar i instal·lar l'aplicació

OpenBSD fa servir un sistema de paquets anomenat "ports", si sabem instal·lar squid, sabrem instal·lar qualsevol altre paquet. Primer el descarreguem...

```
# wget http://ftp.scarlet.be/pub/openbsd/3.6/packages/i386/squid-x.x.tgz
```

Ara l'instal·lem...

```
# pkg_add ./squid-2.5.STABLE6.tgz
Adding ./squid-2.5.STABLE6.tgz
=> Creating _squid group for Squid
=> Creating _squid user for Squid
```

Si no hem vist cap missatge d'error, ja el tenim al nostre sistema.

Detalls a tenir en compte

Abans de continuar hauríem de conèixer quins fitxers utilitza squid, així com on els podem trobar.

- Fitxers de configuració /etc/squid
- Fitxers d'exemple /usr/local/share/examples/squid
- Fitxers amb missatges d'error /usr/local/share/squid/errors
- Fitxers d'error d'exemple /usr/local/share/examples/squid/errors
- Icones que mostrarà squid /usr/local/share/squid/icons
- Icones d'exemple /usr/local/share/examples/squid/icons
- La cache la trobem a /var/squid/cache
- Els logs /var/squid/logs
- L'"ugid" d'squid corre com _squid:_squid

Fitxer de configuració

Com amb el paquet filter, donem un cop d'ull a aquest fitxer de configuració i als seus comentaris. Aquest el trobem a /etc/squid/squid.conf

```
http_port 192.168.0.5:8000
# interfície i port on escoltarà squid
hierarchy_stoplister cgi-bin ? s3os
# no guardarà URLs amb aquest text
cache_mgr admin@s3os.net
# mail de administrador de la xarxa
ftp_user squid@s3os.net
# mail per defecte al connectar ftp public
#dead_peer_timeout
# timeout
forward_timeout 4 minutes
# timeout
connect_timeout 1 minute
# un altre...
```

```
cache_mem 16 MB
# RAM per squid
maximum_object_size 40960 KB
# fitxer més gran que guardarem
maximum_object_size_in_memory 8 KB
# a la RAM fitxers més petits
#cache_replacement_policy lru
# política de reemplaç dels fitxers al disc
#memory_replacement_policy lru
# política de reemplaç dels fitxers a la RAM
#cache_dir ufs /var/squid/cache 800 16 256
# tipus de fitxers, on és la cache, tamany, directoris de 1r nivell, \\
    directoris de 2n nivell, que farà servir squid
ftp_passive on
# ftp passiu
hosts_file /etc/hosts
# el fitxer de hosts
#cache_effective_user squid
# usuari per a la cache
#cache_effective_group squid
# grup per a la cache
visible_hostname musclu.s3os.net
# ;-)

auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
refresh_pattern ^ftp:          1440 20% 10080
refresh_pattern ^gopher:      1440 0% 1440
refresh_pattern .              0 20% 4320

#LLISTES
acl manager proto cache_object
acl totes src 0.0.0.0/0.0.0.0
acl lan src 192.168.0.0/255.255.255.0
acl QUERY urlpath_regex cgi-bin \?
# no guardarà aquestes cadenes
acl lleig url_regex -i sex.*\.$
# no ens deixa accedir a fitxers que continguin "sex" i acabin ".avi"
acl ports_permesos port 80 21 443 563 70 210 280 488 591 777 1025-65535
# llista de ports premesos
#acl ftp proto FTP
# exemple de llista per protocol
acl CONNECT method CONNECT
# mètode de connexió

no_cache deny QUERY
# ara no guardarà les cades de la llista QUERY
http_access deny lleig
# denega la llista lleig
http_access allow lan
# permet la LAN
http_access deny !ports_permesos
# denega els que no són ports premesos
#http_access deny ftp
# per tallar ftp
http_access deny totes
# denega tot, excepte el d'abans
httpd_accel_host virtual
# acceleracions al servidor web
httpd_accel_port 80
# al port 80
httpd_accel_with_proxy on
```

```
# necessari
httpd_accel_uses_host_header on
# canvia peticions http a http-proxy TOTS NECESSARIS PER TRANSPARÈNCIA

#ALGUNS PORTS INTERESSANTS
#port 80 # http
#port 21 # ftp
#port 443 563 # https, snews
#port 70 # gopher
#port 210 # wais
#port 1025-65535 # unregistered ports
#port 280 # http-mgmt
#port 488 # gss-http
#port 591 # filemaker
#port 777 # multiling http
```

Primera inicialització d'squid

Abans d'engegar squid... inicialitzem la cache:

```
# squid -z
```

Ara si, podem engegar per primera vegada el proxy:

```
# squid
```

Si volem (com és lògic) que s'enguegui automàticament a l'arrencada del sistema:

```
# vi /etc/rc.local
    if [ -x /usr/local/sbin/squid ]; then
        echo -n ' squid';          /usr/local/sbin/squid
    fi
# squid -k reconfigure (perquè els canvis tinguin efecte)
```

Permisos d'squid

Squid necessita poder treballar conjuntament amb el tallafocs, doncs li afegim la següent línia al fitxer /etc/pf.conf

```
# vi /etc/pf.conf

    #A LA TAULA NAT:
    rdr on $int_if inet proto tcp from any to any port www -> 127.0.0.1 \\  
    port 8000

    #A LA TAULA FILTRAT:
    pass in on $int_if inet proto tcp from any to 127.0.0.1 port 8000 \\  
    keep state
    pass out on $ext_if inet proto tcp from any to any port www keep state
```

També necessita permisos especials sobre el dispositiu pf...

```
# chgrp squid /dev/pf
```

```
# chmod g+rw
```

Hem de pensar a configurar els nostres clients perquè fagin ús del proxy. Ja estem, en aquest cas disposem d'1GB d'un disc SCSI per a "guardar" totes les nostres dades d'internet.

IDS, detector d'intrusions

La xarxa ens ofereix múltiples aplicacions per poder observar els atacs que pot patir el nostre tallafocs, en veurem unes quantes i explicarem el perquè triem SNORT.

- - Tripwire: verifica l'integritat de fitxers importants del sistema, així evita addició de codi "dolent" o altres canvis.
- - PortSentry: aquesta utilitat ens adverteix que hem patit un escaneig de ports.
- - LogSentry: anàlisi de bitàcores, ens avisarà al trobar anomalies als logs.

Aquestes aplicacions formen una 'suite' bastant bona, però no ofereix les possibilitats d'un IDS dedicat com és SNORT. SNORT funciona de tres maneres: sniffer, packet logger i IDS (la que es centrarà aquest document)

- - sniffer: a l'estil 'tcpdump', mostra per pantalla el paquets que passen per la xarxa.

```
# snort -v (mostra ip's i capçaleres dels paquets)
# snort -dv (l'anterior, i hi afegeix les dades que passen)
# snort -dev (l'anterior, però més detallat)
```

- - packet logger: ens guarda les dades recollides per l'sniffer dins un fitxer o directori concret.

```
# snort -dv -l ./log (guarda les dades al directori 'log')
```

- - IDS: és la part més interessant d'aquesta aplicació, ens avisarà d'scans de ports, atacs DoS, xploits, etc. Es basa en normes... però tot això ho anirem veient després de l'instal·lació..

Aconseguir els fitxers necessaris i instal·lació

Snort no te dependències extra, pesa 2.047KB...

```
# wget http://ftp.scarlet.be/pub/openbsd/3.6/packages/i386/snort-x.x.tgz
# pkg_add ./snort-x.x.tgz
Adding ./snort-x.x.tgz
```

Configuració i arrencada

Només hem de fer un petit canvi al fitxer de configuració d'snort:

```
# vi /etc/snort/snort.conf
var RULE_PATH /etc/snort/rules
```

Abans de continuar, un petit apunt... els servidors d'snort actualitzen les normes (rules) cada hora, per tant seria interessant fer un petit script que ens actualitzés les normes cada 3600 segons...

```
# vi normes_snort.sh
#!/bin/sh
cd /tmp/
rm -f snortrules*
wget www.snort.org/dl/rules/snortrules-snapshot-2_2.tar.gz
tar -zxvpf snortrules-snapshot-2_2.tar.gz
mv -f ./rules /etc/snort/
```

Guardem, sortim (esc, :, w, q, !) i li donem permisos d'execució.

```
# chmod 700 normes_snort.sh
```

La versió del fitxer de normes varia segons la versió d'SNORT, actualment en tenim per a les versions: 2.0, 2.1 i 2.2. Només falta afegir-ho al crontab perquè s'executi cada hora. Bé ja el tenim instal·lat i configurat, per engegar-lo:

```
# snort -c /etc/snort/snort.conf
```

Com a dimoni:

```
# snort -c /etc/snort/snort.conf -D
```

A partir d'aquest moment ja estem "loggejant" els paquets sospitosos i revisant les connexions. Si no li diem el contrari ens guardarà a informació a: '/var/log/snort/' i podem llegir-ho amb un simple:

```
# cat /var/log/snort/alert (per un resum)
```

```
o...
```

```
# cat /var/log/snort/www.xxx.yyy.zzz (per a cada una de les ip's enregistrades)
```

Evidentment és una manera poc 'amable' de llegir els resultats, cap problema...

Analitzar les intrusions

Tenim diferents possibilitats per llegir els resultats: banyard, acid, snortsnarf,...

- - banyard (fast output system): distribuït dese www.snort.org; poc pràctic i encara menys 'de bon llegir'
- - acid: molt complet, però necessita apache, mysql, i coneixement de php. No crec que valgui la pena, tenim una màquina petita.
- - snortsnarf: senzill, no necessita tantes aplicacions exteriors, mysql, php,... Però potent
- - Webmin?: Doncs si, hi ha un mòdul de tercers (no estàndard) per afegir snort a webmin, pot ser molt útil al moment d'activar normes, però no ens serveix per visualitzar els resultats.
- Hi ha altres aplicacions: pisSentry, snortalog, ...

Com es pot deduir farem servir 'snortsnarf'... Snortsnarf és una aplicació feta amb Perl que processa els

logs d'SNORT i els converteix a html's. Només ocupa 385KB i no depenem de MySQL ni PHP, tan sols necessitarem un servidor web, evidentment apache (aquest document no explicarà com muntar apache, es reserva per a altres 'peixos') Ara veurem com funciona snortsnarf...

```
# wget http://ftp.scarlet.be/pub/openbsd/3.6/packages/i386/snortsnarf-x.x.tgz
# pkg_add ./snortsnarf-x.x.tgz
```

Ara el podem executar:

```
# snortsnarf.pl -d /var/log/snortsnarf /var/log/snort/alert
```

Aquesta comanda ens crearà, a /var/log/snortsnarf, un directori anomenat 'snout.alert' i dins aquest, a part de molts altres, trobarem el fitxer 'index.htm'. Seria interessant afegir l'anterior comanda al crondaily, d'aquesta manera farem una rotació del log diària. Per poder llegir aquests fitxers, hem de configurar apache (també ho podríem fer desde un altre 'peix' que tinguis servidor web, en 'cangreju', per exemple)...

Configurant apache

Editem el fitxer de configuració per defecte i hi afegim:

```
# nano /etc/apache2/conf/apache2.conf

    Alias /snort/ /var/log/snortsnarf/
    <Directory "/var/log/snortsnarf/">
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
```

Reiniciem apache

```
# /etc/rc.d/rc.apached restart
```

Escribin "http://localhost/snort/" al navegador web preferit veurem els registres d'SNORT de manera molt entenedora.