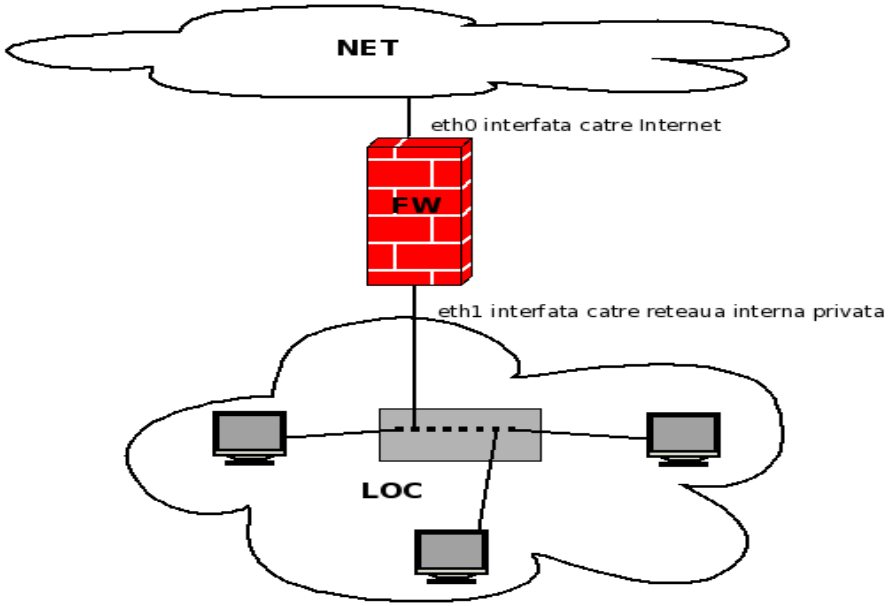
CONFIGURARE SHOREWALL

-Autor:Marius Strâcnă-

Data: 23.03.2009
Versiunea: 1.1

Ce este **Shorewall**?
Shorewall este un instrument **free software firewall** pentru Linux, ce oferă o mare usurință în configurarea Netfilter (iptables/ipchains, modul ce construiește schema în kernel-ul Linux).



De unde putem obtine **Shorewall**?
Pagina oficiala este: http://www.shorewall.net

In următoarea procedură aveți descrisă configurarea minimală a unui FIREWALL/ROUTER cu ajutorul aplicației Shorewall.

1.Definirea interfețelor de rețea se efectuează în: /etc/shorewall/interfaces ; **eth0** fiind interfața către Internet denumită **net**, iar **eth1** interfața către rețeaua privată internă denumită **loc** ;

joe /etc/shorewall/interfaces:

```
# http://www.shorewall.net/manpages/shorewall-interfaces.html
#
###############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
net     eth0            detect          norfc1918
loc     eth1            detect          dhcp, routeback
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Optiunea norfc1819, semnifică faptul că adresă IP alocată interfeței eth0 nu se află în standardul RFC-1918 (http://tools.ietf.org/html/rfc1918),din acest standard fac parte doar adresele folosite in rețelele private, acestea sunt cuprinse între:

-10.0.0.0 - 10.255.255.255
-172.16.0.0 - 172.31.255.255
-192.168.0.0 - 192.168.255.255

2.Definirea zonelor si tipul acestora se efectuează in: /etc/shorewall/zones ; **loc** este zona privata (rețeaua privată internă), **net** este zona dinspre internet, **fw** semnifică insuși router-ul ce conține cele două interfețe de rețea

joe /etc/shorewall/zones:

```
# http://www.shorewall.net/manpages/shorewall-zones.html http://www.google.ro/
#
###############################################################################
#ZONE   TYPE            OPTIONS         IN                      OUT
#                                       OPTIONS                 OPTIONS
fw      firewall
loc     ipv4
net     ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

3.Politica se seteaza în: /etc/shorewall/policy, acest fisier definește politica de conexiuni intre zonele de acces, vezi zonele definite in /etc/shorewall/zones;

joe /etc/shorewall/policy:

```
# http://www.shorewall.net/manpages/shorewall-policy.html
#
###############################################################################
#SOURCE          DEST            POLICY          LOG             LIMIT:BURST
#                                                LEVEL
$FW             all             ACCEPT
loc             $FW             ACCEPT
loc             net             REJECT          info
net             all             REJECT          info
all             all             REJECT          info
#LAST LINE -- DO NOT REMOVE
```

4.Regulile se setează in: /etc/shorewall/rules, prin aceste reguli se stabilesc exceptii de la politica stabilita in: /etc/shorewall/policy;

joe /etc/shorewall/rules:

```
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#ACTION          SOURCE              DEST        PROTO    DEST
#                                                         PORT

#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
```

```
#Următoarea regulă oferă posibilitatea utilizatorilor aflați in rețeaua privată internă (loc) să trimită pachete catre
orice IP de oriunde
Ping/ACCEPT:info  loc                 all

#Această regulă ofera utilizatorilor aflați în zona net (internet), posibilitatea de a trimite pachete doar către router.
Ping/ACCEPT:info  net                 $FW

Trcrt/ACCEPT:info loc                 all
Trcrt/ACCEPT:info net                 $FW

Web/ACCEPT:info   loc                 all

IMAP/ACCEPT:info  loc                 all

POP3/ACCEPT:info  loc                 all

SMTP/ACCEPT:INFO  loc                 all

SSH/ACCEPT:info   loc                 all
SSH/ACCEPT:info   net                 $FW

DNS/ACCEPT:info   loc                 all

#Regula aceasta permite utilizatorilor din net (internet) sa trimita pachete in zona loc (reteaua privata internă)
DNS/ACCEPT:info   net                 all

FTP/ACCEPT:info   loc                 all
FTP/ACCEPT:info   net                 $FW

NTP/ACCEPT:info   loc                 $FW
NTP/ACCEPT:info   loc                 net

NNTP/ACCEPT:info  loc                 net
```

```
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

5.In: /etc/shorewall/masq se adauga IP-ul public, ce mascheaza rețeaua internă privată,

joe /etc/shorewall/masq:

```
# http://www.shorewall.net/manpages/shorewall-masq.html
#
#############################################################################
#INTERFACE              SOURCE          ADDRESS         PROTO   PORT(S) IPSEC   MARK
eth0                    0.0.0.0/0       (adresa IP publica)
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

6. In fisierul: /etc/shorewall/shorewall.conf se seteaza pornirea automata la restart a aplicatiei shorewall;

joe /etc/shorewall/shorewall.conf

```
##############################################################################
#                                S T A R T U P E N A B L E D                 #
##############################################################################
STARTUP_ENABLED=Yes
```