Sicurezza nelle reti

Configurazione firewall

Menu principale

```
                    LEAF configuration menu

1 ) Network configuration

2 ) System configuration

3 ) Packages configuration

                              b) Back-up a package

                              c) Back-up your LEAF disk

                              h) Help

q) quit
```

Network configuration

```
                Network configuration menu
1) interfaces file       (/etc/network/interfaces)
2) network options file (/etc/network/options)
3) hosts IP addresses    (/etc/hosts)
4) hostname              (/etc/hostname)
5) resolv.conf           (/etc/resolv.conf)
6) super server daemon   (/etc/inetd.conf)
7) hosts.allow           (/etc/hosts.allow)
8) hosts.deny            (/etc/hosts.deny)
9) networks              (/etc/networks)
q) quit
```

Interfaces file – step 1a

```
# Step 1: configure external interface
#         uncomment/adjust one of the following 4 options
# Option 1.1: eth0 / dynamic IP from pump/dhclient
#auto eth0
#iface eth0 inet dhcp
# Option 1.2: eth0 / Fixed IP (assumed to be 1.2.3.4).
#                (broadcast/gateway optional)
auto eth0
iface eth0 inet static
        address 213.198.150.106
        masklen 29
        broadcast 213.198.150.111
        gateway 213.198.150.104
```

Interfaces file – step 1b

```
# Step 1: configure external interface
#         uncomment/adjust one of the following 4 options
# Option 1.3: PPP/PPPOE (modem connected to eth0)
#auto ppp0
#iface ppp0 inet ppp
#       pre-up ip link set eth0 up
#       provider dsl-provider eth0
#
# Option 1.4: PPP modem
#auto ppp0
#iface ppp0 inet ppp
#       provider provider
```

Interfaces file – step 2

```
# Step 2: configure  internal interface
# Default: eth1 / fixed IP = 192.168.1.254
auto eth1
iface eth1 inet static
        address 192.168.1.111
        masklen 24
        broadcast 192.168.1.255
```

Interfaces file – step 3

```
# Step 3 (optionnal): configure DMZ
# Default: eth2 / fixed IP = 192.168.1.100
#auto eth2
#iface eth2 inet static
#       address 192.168.1.100
#       masklen 24
#       broadcast 192.168.1.255
```

Shorwall configuration

```
1) Params     Assign parameter values
2) Zones      Partition the network into Zones
3) Ifaces     Shorewall Networking Interfaces
4) Hosts      Define specific zones
5) Policy     Firewall high-level policy
6) Rules      Exceptions to policy
7) Maclist    MAC Verification
8) Masq       Internal MASQ Server Configuration
9) ProxyArp   Proxy ARP Configuration
```

Shorwall configuration

```
10) Stopped   Hosts admitted after 'shorewall stop'
11) Nat       Static NAT Configuration
12) Tunnels   Tunnel Definition (ipsec)
13) TCRules   FWMark Rules
14) Config    Shorewall Global Parameters
15) Modules   Netfilter modules to load
16) TOS       Type of Service policy
17) Blacklist Blacklisted hosts
18) RFC1918   Defines 'norfc1918' interface option
```

Shorewall params use

```
# Assign any variables that you need here.

# It is suggested that variable names begin with an upper
  case letter to distinguish them from variables used
  internally within the Shorewall programs

# Example:

#       NET_IF=eth0

#       NET_BCAST=130.252.100.255

#       NET_OPTIONS=noping,norfc1918

# Example (/etc/shorewall/interfaces record):

#  net $NET_IF $NET_BCAST $NET_OPTIONS

# The result will be the same as if the record had been
  written

#  net eth0 130.252.100.255 noping,norfc1918
```

Shorewall params where

```
# Variables can be used in the following places in the
  other configuration
# files:
# /etc/shorewall/interfaces:
# /etc/shorewall/hosts
#       All except the first column.
# /etc/shorewall/rules
#       First column after ":" and all remaining columns
# /etc/shorewall/tunnels
# /etc/shorewall/proxyarp
# /etc/shorewall/nat
#       All columns
```

Shorewall zones

```
# This file determines your network zones. Columns are:
#
#       ZONE                Short name of the zone
#       DISPLAY             Display name of the zone
#       COMMENTS            Comments about the zone
#
#ZONE   DISPLAY             COMMENTS
net     Net                 Internet
loc     Local               Local networks
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT
  REMOVE
```

Shorewall interfaces

```
# You must add an entry in this file for each network
# interface on your firewall system.
# Columns are:
#       ZONE            Must match the short name of a zone
#                       defined in /etc/shorewall/zones.
#       INTERFACE       Name of interface.
#       BROADCAST       The broadcast address for the
#                       subnetwork to which the
#                       interface belongs.
#       OPTIONS         A comma-separated list of options
#                       including the following:
#           dhcp    - interface is managed or used by DHCP
```

Shorewall interfaces options

```
# noping - icmp echo-request (ping) packets addressed to the
#          firewall should be ignored on this interface
# filterping   - icmp echo-request (ping) packets addressed
#                to the firewall should be controlled by the
#                rules file
# routestopped - When the firewall is stopped, allow and
#                route traffic to and from this interface.
# norfc1918    - This interface should not receive any
#                packets whose source is in one of the ranges
#                reserved by RFC 1918
# multi        - This interface has multiple IP addresses and
#                you want to be able to route between them.
```

Shorewall interfaces options

```
# routefilter  - turn on kernel route filtering for this
#                interface (anti-spoofing measure).
# dropunclean  - Logs and drops mangled/invalid packets
# logunclean   - Logs mangled/invalid packets but does
#                not drop them.
# blacklist    - Check packets arriving on this interface
#                against the /etc/shorewall/blacklist file.
# maclist      - Connection requests from this interface
#                are compared against the contents of maclist.
# proxyarp     - Sets
#            /proc/sys/net/ipv4/conf/<interface>/proxy_arp.
```

Shorewall interfaces example

```
# Example: Suppose you have eth0 connected to a DSL modem and
  eth1 connected to your local network and that your local
  subnet is 192.168.1.0/24. The interface gets it's IP
  address via DHCP from subnet 206.191.149.192/27 and you
  want pings from the internet to be ignored. You interface a
  DMZ with subnet 192.168.2.0/24 using eth2. You want to be
  able to access the firewall from the local network when the
  firewall is stopped. Your entries for this setup would look
  like:

# net      eth0    206.191.149.223 noping,dhcp

# local    eth1    192.168.1.255   routestopped

# dmz      eth2    192.168.2.255
```

Shorewall policy

```
# This file determines what to do with a new connection
  request if we don't get a match from the rules file or from
  the common[.def] file. Columns are:

# SOURCE        Source zone. Must be the name of a zone,$FW or

#               "all".

# DEST          Destination zone. Must be the name of a zone,

#               $FW or "all"

# POLICY        Policy if no match from the rules file is found.

#               Must be "ACCEPT","DROP","REJECT" or "CONTINUE"

# LOG LEVEL     If supplied, each connection handled under the

#               default POLICY is logged at that level.

# LIMIT:BURST   If passed, specifies the maximum TCP connection

#                rate and the size of an acceptable burst.
```

Shorewall default policy

```
#       As shipped, the default policies are:
#       a) All connections from the local network to the
#          internet are allowed
#       b) All connections from the internet are ignored
#          but logged at syslog level KERNEL.INFO.
#       d) All other connection requests are rejected and
#          logged at level KERNEL.INFO.
#SOURCE DEST POLICY  LOG LEVEL       LIMIT:BURST
loc     net  ACCEPT
#fw     net  ACCEPT
net     all  DROP    info
all     all  REJECT  info
```

Shorewall rules

```
# Rules in this file govern connection establishment. Requests
  and responses are automatically allowed using connection
  tracking. Columns are:

# ACTION   ACCEPT, DROP, REJECT, DNAT or REDIRECT

#          ACCEPT   -- allow the connection request

#          DROP     -- ignore the request

#          REJECT   -- disallow the request and return an

#                      icmp-unreachable or an RST packet.

#          DNAT     -- Forward the request to another

#                      system (and optionally another port).

#          REDIRECT -- Redirect the request to a local

#                      port on the firewall.
```

Shorewall rules

```
# SOURCE   Source hosts to which the rule applies. May be a
#          zone or $FW to indicate the firewall itself
# DEST     Location of Server. May be a zone or $FW to
#          indicate the firewall itself.
# PROTO    Protocol - Must be "tcp", "udp", "icmp", a number,
#          "all" or "related". If "related", the remainder of
#          the entry must be omitted and connection requests
#          that are related to existing requests will be
#          accepted.
```

Shorewall rules

```
# DEST PORT(S) Destination Ports. A comma-separated list of
#              Ports; if the protocol is "icmp", this
#              column is interpreted as the destination
#              icmp-type(s).
# CLIENT PORT(S) (Optional) Port(s) used by the client.
#                If omitted any source port is acceptable.
# ORIGINAL DEST  (Optional -- only allowed if ACTION is DNAT
#                or REDIRECT) If included this is an address
#                on some interface on the firewall and
#                connections to that address will be forwarded
#                to the IP and port specified in the DEST
#                column.
```

Shorewall sample rules

```
#ACTION   SOURCE    DEST   PROTO    DEST     SOURCE      ORIGINAL
# Accept DNS connections from the firewall to the network
ACCEPT    fw        net    tcp      53
ACCEPT    fw        net    udp      53
# Accept SSH connections from the local network for admin
ACCEPT    loc       fw     tcp      22
# Bering specific rules:
# allow   loc to fw udp/53 for dnscache to work
# allow   loc to fw tcp/80 for weblet to work
ACCEPT    loc       fw     udp      53
ACCEPT    loc       fw     tcp      80
DNAT net loc:192.168.1.150 tcp 80 - 213.198.150.106
```

Shorewall masquerade

```
# Use this file to define dynamic NAT (Masquerading) and to
  define Source NAT (SNAT). Columns are:

# INTERFACE -- Outgoing interface. This is usually your
  internet interface. This may be qualified by adding the
  character ":" followed by a destination host or subnet.

# SUBNET -- Subnet that you wish to masquerade. You can
  specify this as a subnet or as an interface. If you give
  the name of an interface, you must have iproute installed
  and the interface must be up before you start the firewall.

# ADDRESS -- (Optional).  If you specify an address here, SNAT
  will be used and this will be the source address. If
  ADD_SNAT_ALIASES is set to Yes or yes in
  /etc/shorewall/shorewall.conf then Shorewall will
  automatically add this address to the INTERFACE named in
  the first column.

#INTERFACE          SUBNET          ADDRESS

eth0                eth1
```