Politeknik Elektronika Negeri Surabaya

Firewall: Shorewall

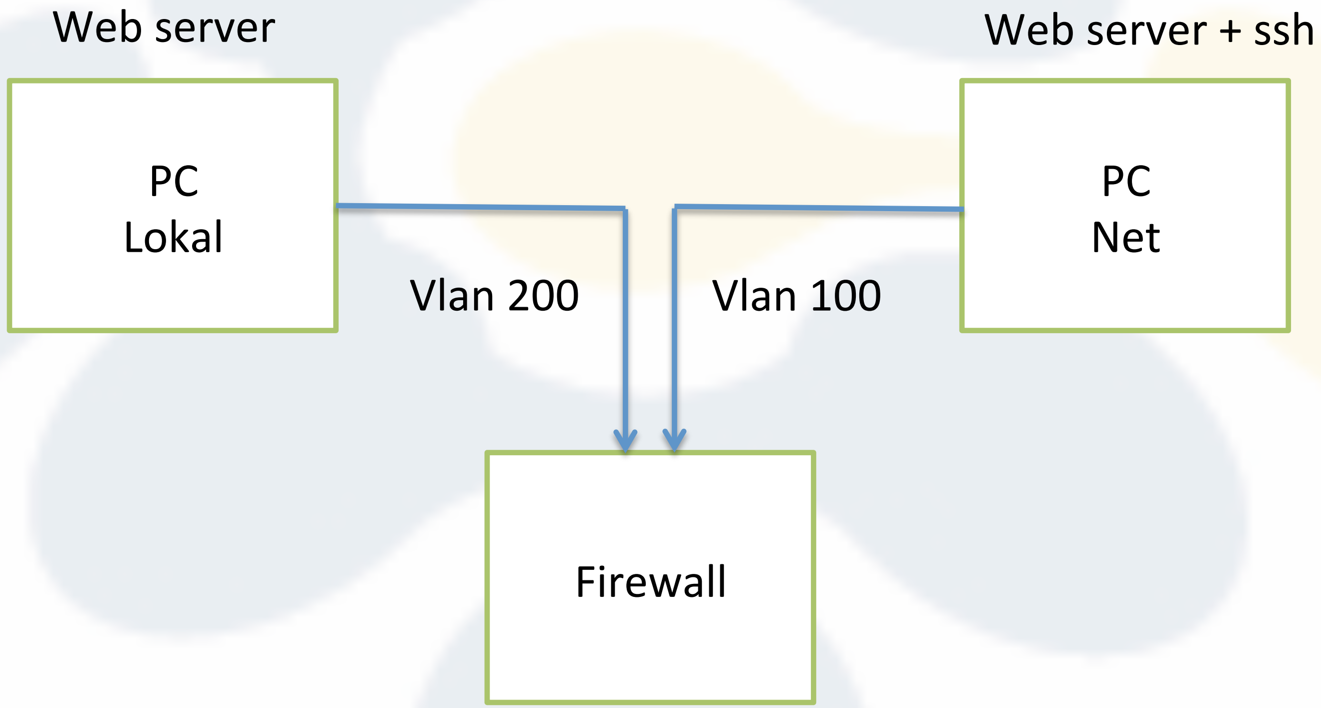
Oleh:

Idris Winarno

Tentang Shorewall….

- Aplikasi administrasi dan manajemen firewall (iptables)
- Parameter/variabel:
  - interface
  - zone
  - policy
  - rules

Topologi praktikum



Interface

- # ifconfig

  → eth0 / enp2s0 / dsb

Zones

- Intranet / LAN → loc
- Internet → net
- Komputer/mesin Firewall → fw

Policy

- Dari **fw** ke **net** → Allowed/Accept
- Dari **net** ke **fw** → Denied/Drop
- Lainnya → Denied/Drop

Rules

- Dari **loc:10.252.108.100/32** ke **net** → Accept
- Dari **net** ke **loc:10.252.108.100/32 tcp/80**→ Accept

Instalasi (1)

- Hapus paket yang tidak digunakan
  - :~# apt-get remove portmap
  - :~# apt-get remove nfs-common
  - :~# apt-get remove pidentd

Instalasi (2)

Shorewall

- # apt-get install shorewall
- # apt-get install shorewall-doc

VLAN

- # apt-get install vlan

Konfigurasi (1)

VLAN:

- # vconfig   add eth0   100
- # vconfig   add eth0   200
- # ifconfig   eth0.100 192.168.xyz.1 netmask 255.255.255.0
- # ifconfig   eth0.200 172.16.xyz.1 netmask 255.255.255.0

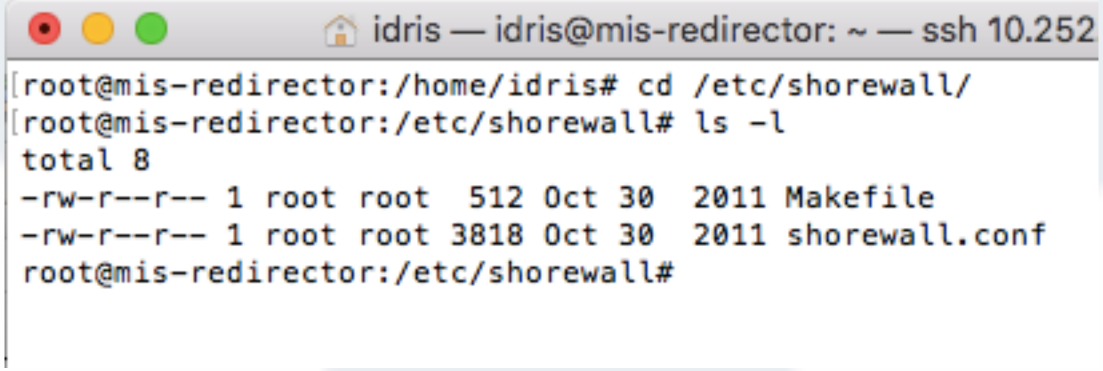
Packet Forwarding:

- # sysctl   -w   net.ipv4.ip_forward=1

Konfigurasi (2)

- Masuk ke direktori /etc/shorewall
  - # cd /etc/shorewall

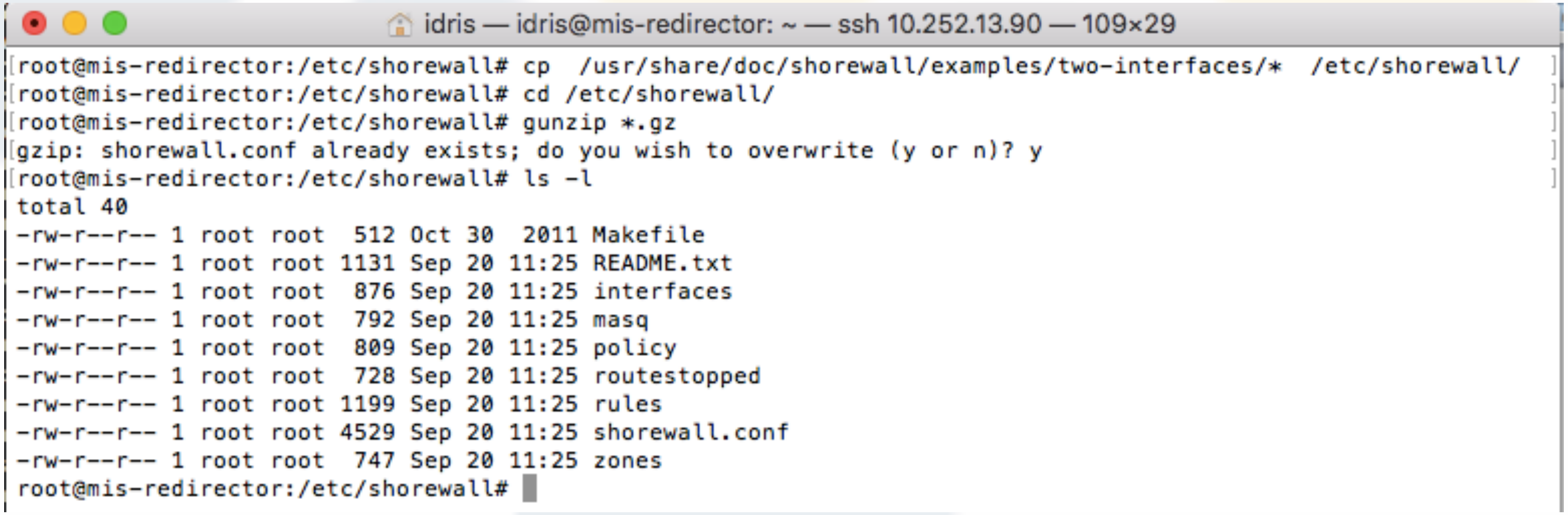
- Lihat filenya
  - # ls



```
[root@mis-redirector:/home/idris# cd /etc/shorewall/
[root@mis-redirector:/etc/shorewall# ls -l
total 8
-rw-r--r-- 1 root root  512 Oct 30  2011 Makefile
-rw-r--r-- 1 root root 3818 Oct 30  2011 shorewall.conf
root@mis-redirector:/etc/shorewall#
```

Konfigurasi (3)

- Salin contoh konfigurasi
  - # cp /usr/share/doc/shorewall/examples/two-interface/*   /etc/shorewall
  - # cd /etc/shorewall
  - # gunzip *.gz



```
root@mis-redirector:/etc/shorewall# cp  /usr/share/doc/shorewall/examples/two-interfaces/*  /etc/shorewall/
root@mis-redirector:/etc/shorewall# cd /etc/shorewall/
root@mis-redirector:/etc/shorewall# gunzip *.gz
gzip: shorewall.conf already exists; do you wish to overwrite (y or n)? y
root@mis-redirector:/etc/shorewall# ls -l
total 40
-rw-r--r-- 1 root root  512 Oct 30  2011 Makefile
-rw-r--r-- 1 root root 1131 Sep 20 11:25 README.txt
-rw-r--r-- 1 root root  876 Sep 20 11:25 interfaces
-rw-r--r-- 1 root root  792 Sep 20 11:25 masq
-rw-r--r-- 1 root root  809 Sep 20 11:25 policy
-rw-r--r-- 1 root root  728 Sep 20 11:25 routestopped
-rw-r--r-- 1 root root 1199 Sep 20 11:25 rules
-rw-r--r-- 1 root root 4529 Sep 20 11:25 shorewall.conf
-rw-r--r-- 1 root root  747 Sep 20 11:25 zones
root@mis-redirector:/etc/shorewall# 
```

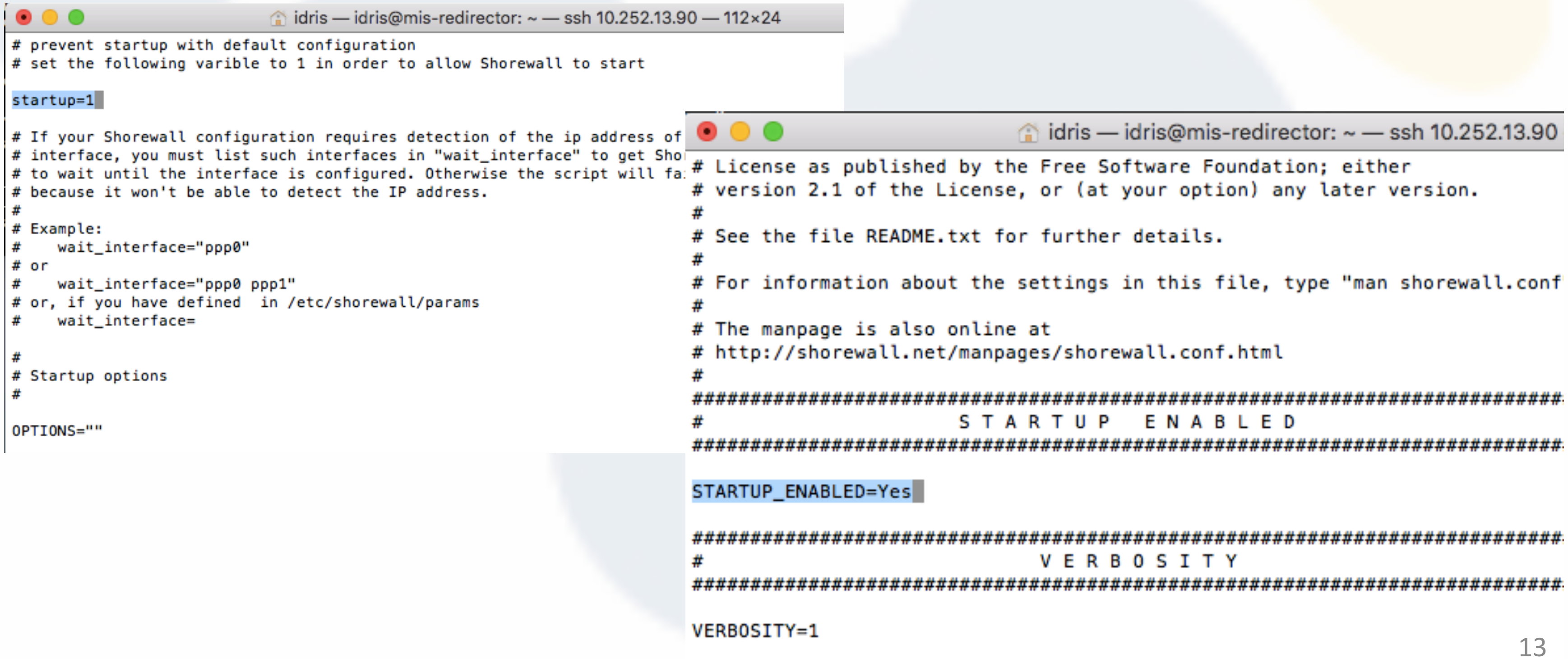
Konfigurasi (4)

- Aktifkan shorewall pada /etc/default/shorewall

    `startup=0` **menjadi** `startup=1`

- Dan juga pada /etc/shorewall/shorewall.conf

    `STARTUP_ENABLED=No` **menjadi** `STARTUP_ENABLED=yes`

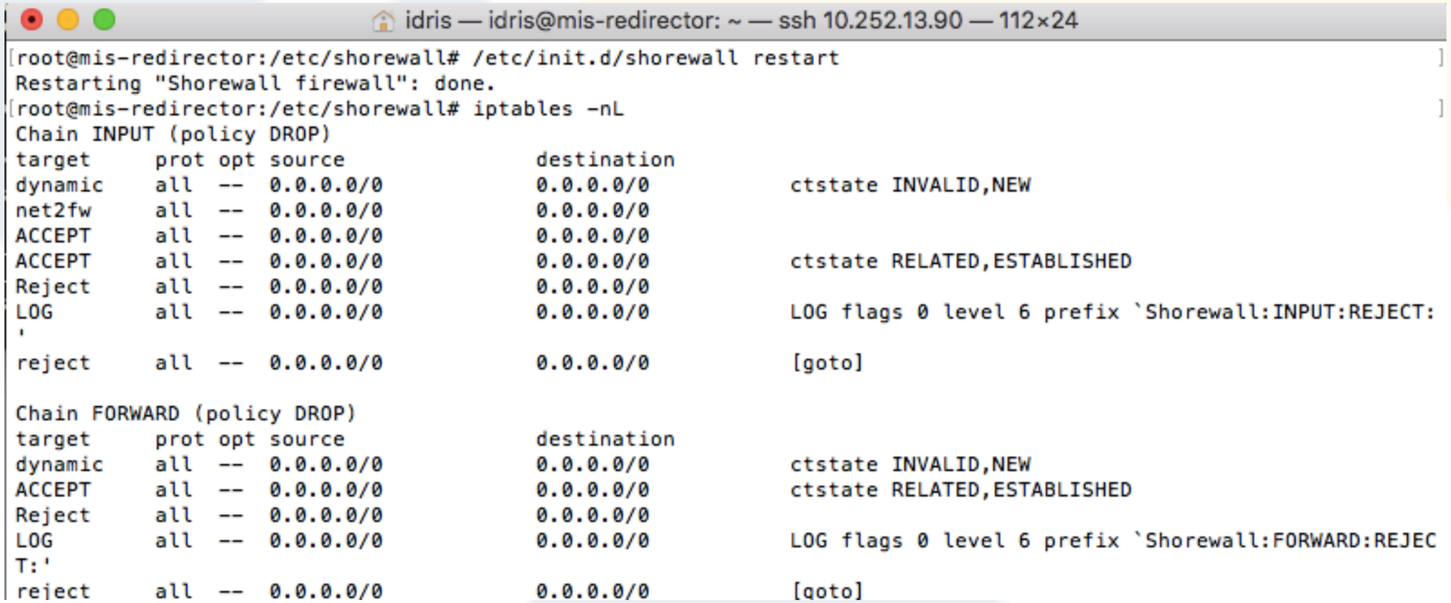

idris — idris@mis-redirector: ~ — ssh 10.252.13.90 — 112×24
idris — idris@mis-redirector: ~ — ssh 10.252.13.90

```
# prevent startup with default configuration
# set the following varible to 1 in order to allow Shorewall to start

startup=1

# If your Shorewall configuration requires detection of the ip address of
# interface, you must list such interfaces in "wait_interface" to get Sho
# to wait until the interface is configured. Otherwise the script will fa
# because it won't be able to detect the IP address.
#
# Example:
#    wait_interface="ppp0"
# or
#    wait_interface="ppp0 ppp1"
# or, if you have defined  in /etc/shorewall/params
#    wait_interface=

#
# Startup options
#

OPTIONS=""
```

```
# License as published by the Free Software Foundation; either
# version 2.1 of the License, or (at your option) any later version.
#
# See the file README.txt for further details.
#
# For information about the settings in this file, type "man shorewall.conf
#
# The manpage is also online at
# http://shorewall.net/manpages/shorewall.conf.html
#
###############################################################################
#                          S T A R T U P   E N A B L E D
###############################################################################

STARTUP_ENABLED=Yes

###############################################################################
#                                 V E R B O S I T Y
###############################################################################

VERBOSITY=1
```

Aktifkan shorewall

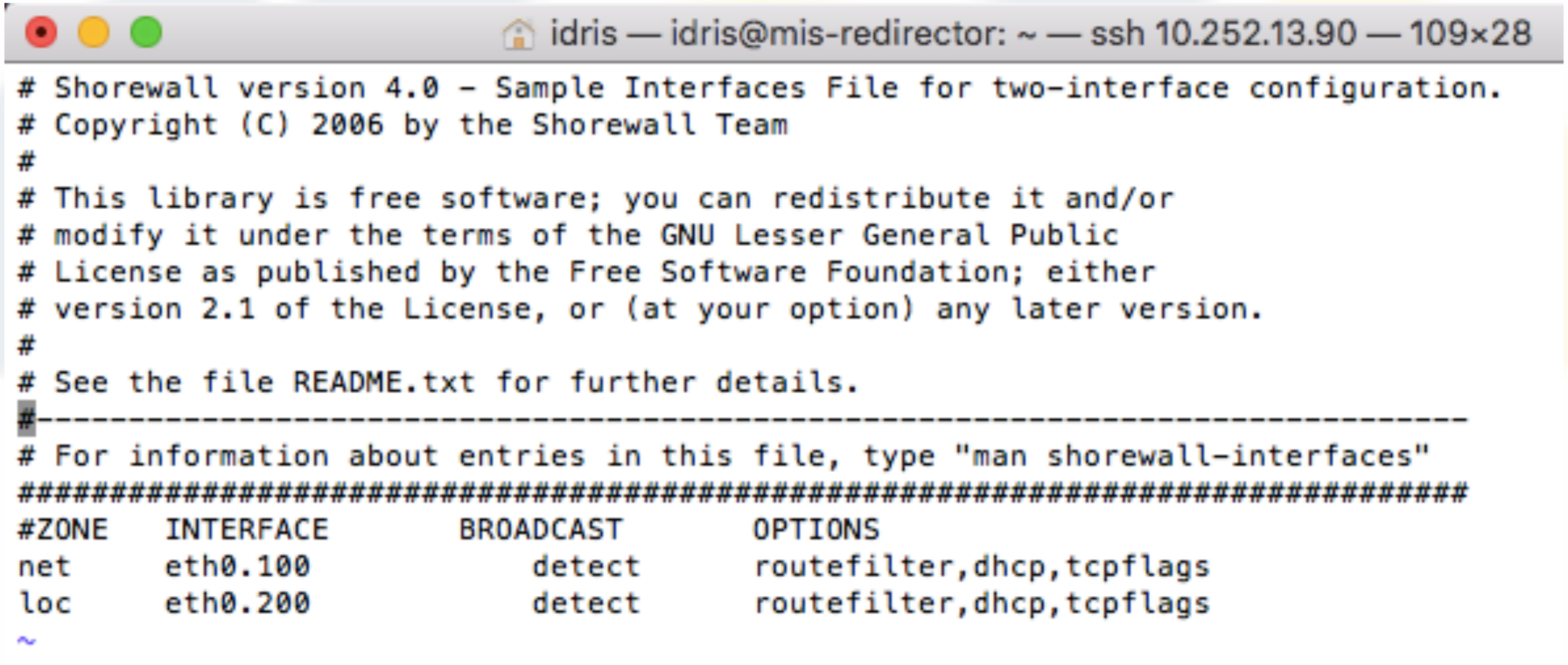
- `# /etc/init.d/shorewall  start`
- `# iptables -nL`



```
root@mis-redirector:/etc/shorewall# /etc/init.d/shorewall restart
Restarting "Shorewall firewall": done.
root@mis-redirector:/etc/shorewall# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
dynamic    all  --  0.0.0.0/0            0.0.0.0/0            ctstate INVALID,NEW
net2fw     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED
Reject     all  --  0.0.0.0/0            0.0.0.0/0
LOG        all  --  0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 6 prefix `Shorewall:INPUT:REJECT:
 '
reject     all  --  0.0.0.0/0            0.0.0.0/0            [goto]

Chain FORWARD (policy DROP)
target     prot opt source               destination
dynamic    all  --  0.0.0.0/0            0.0.0.0/0            ctstate INVALID,NEW
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED
Reject     all  --  0.0.0.0/0            0.0.0.0/0
LOG        all  --  0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 6 prefix `Shorewall:FORWARD:REJEC
T:'
reject     all  --  0.0.0.0/0            0.0.0.0/0            [goto]
```

Modifikasi interface

- # vim /etc/shorewall/interfaces



idris — idris@mis-redirector: ~ — ssh 10.252.13.90 — 109×28

```
# Shorewall version 4.0 - Sample Interfaces File for two-interface configuration.
# Copyright (C) 2006 by the Shorewall Team
#
# This library is free software; you can redistribute it and/or
# modify it under the terms of the GNU Lesser General Public
# License as published by the Free Software Foundation; either
# version 2.1 of the License, or (at your option) any later version.
#
# See the file README.txt for further details.
#------------------------------------------------------------------------------
# For information about entries in this file, type "man shorewall-interfaces"
###############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
net     eth0.100            detect      routefilter,dhcp,tcpflags
loc     eth0.200            detect      routefilter,dhcp,tcpflags
~
```

Aktifasi beberapa *rules*

- Ijinkan koneksi http ke server
  - #vim /etc/shorewall/rules

- Pindah kursor dipaling bawah dan tambahkan *rules* berikut:
  - ACCEPT loc net icmp
  - ACCEPT net loc:192.168.1.1 tcp 80

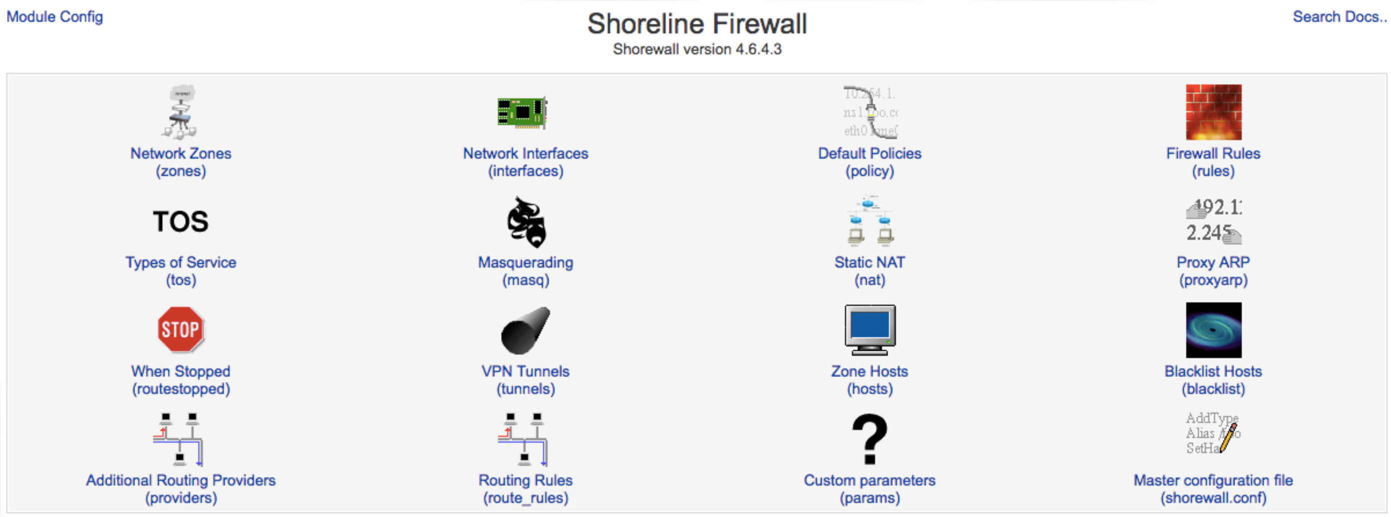
```
ACCEPT      loc      net                  icmp
ACCEPT      net      loc:192.168.1.1      tcp     80
```

- Restart shorewall
  - # /etc/init.d/shorewall restart

Tugas

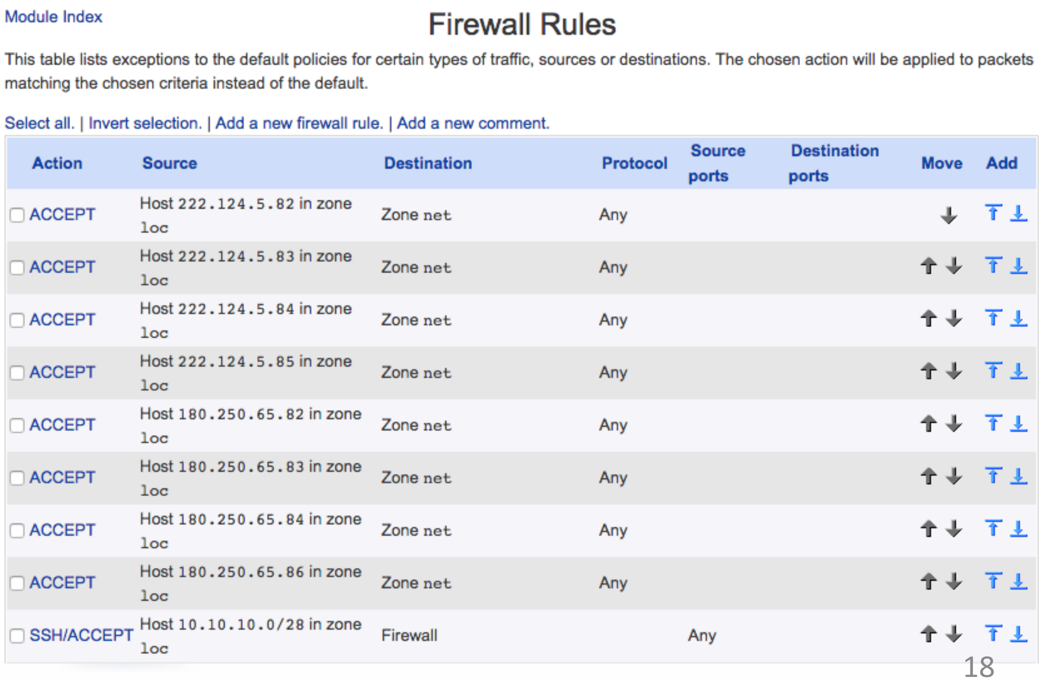
- Integrasikan shorewall dengan webmin
- Integrasikan shorewall, webmin dan apache2/ nginx

Contoh hasil integrasi shorewall dengan webmin



Shoreline Firewall

Shorewall version 4.6.4.3



Firewall Rules

This table lists exceptions to the default policies for certain types of traffic, sources or destinations. The chosen action will be applied to packets matching the chosen criteria instead of the default.

Select all. | Invert selection. | Add a new firewall rule. | Add a new comment.

Action	Source	Destination	Protocol	Source ports	Destination ports	Move	Add
□ ACCEPT	Host 222.124.5.82 in zone loc	Zone net	Any			↓	⤒ ⤓
□ ACCEPT	Host 222.124.5.83 in zone loc	Zone net	Any			↑ ↓	⤒ ⤓
□ ACCEPT	Host 222.124.5.84 in zone loc	Zone net	Any			↑ ↓	⤒ ⤓
□ ACCEPT	Host 222.124.5.85 in zone loc	Zone net	Any			↑ ↓	⤒ ⤓
□ ACCEPT	Host 180.250.65.82 in zone loc	Zone net	Any			↑ ↓	⤒ ⤓
□ ACCEPT	Host 180.250.65.83 in zone loc	Zone net	Any			↑ ↓	⤒ ⤓
□ ACCEPT	Host 180.250.65.84 in zone loc	Zone net	Any			↑ ↓	⤒ ⤓
□ ACCEPT	Host 180.250.65.86 in zone loc	Zone net	Any			↑ ↓	⤒ ⤓
□ SSH/ACCEPT	Host 10.10.10.0/28 in zone loc	Firewall		Any		↑ ↓	⤒ ⤓