

Shorewall

Esempio di firewall dual-homed

Firewall con due schede di rete, una sulla rete locale e l'altra su internet con IP pubblico (verso il router del provider).

Dobbiamo scrivere 6 file in **/etc/shorewall/**:

zones

Elenca le *zone* gestite dal firewall:

net	ipv4	# Internet
loc	ipv4	# Rete locale

interfaces

Associa ciascuna zona all'interfaccia di rete relativa:

net	eth1	detect
loc	eth0	detect

policy

Policy predefinite tra le varie zone:

\$FW	all	ACCEPT	
loc	net	ACCEPT	
net	\$FW	DROP	info
all	all	REJECT	info

rules

Eccezioni alle policy predefinite. Esempio: accetta traffico Samba (condivisione cartelle) da un singolo indirizzo IP internet e da tutta la rete locale. Accetta traffico web da qualunque origine (NOTA: vedere il file **/etc/services** per la corrispondenza tra nome di un servizio e le porte usate):

ACCEPT	net:88.57.16.26	\$FW	tcp	445
ACCEPT	loc	\$FW	tcp	445
ACCEPT	all	\$FW	tcp	80

masq

Tutti i computer della rete locale saranno mascherati con l'indirizzo IP pubblico del firewall quando escono su internet (eth1):

eth1	192.168.9.0/24
------	----------------

shorewall.conf

Abilita il forwarding dei pacchetti IP (funzione tipica di un router/firewall):

```
IP_FORWARDING=Yes
```

Da riga di comando

Vedere le regole iptables attive in questo momento:

```
iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

From:
<https://www.rigacci.net/wiki/> - **Rigacci.Net**

Permanent link:
https://www.rigacci.net/wiki/doku.php/formazione/linux_sysadmin/shorewall?rev=1302700235

Last update: **2011/04/13 15:10**

