

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/**:

/etc/shorewall/zones

Elenca le *zone* gestite dal firewall:

```
fw      firewall # Il firewall stesso
net     ipv4    # Internet
loc     ipv4    # Rete locale
vpn     ipv4    # Accessi via VPN
```

/etc/shorewall/interfaces

Associa ciascuna zona all'interfaccia di rete relativa:

```
net     eth1     detect
loc     eth0     detect
vpn     tun0     detect
```

/etc/shorewall/policy

Policy predefinite tra le varie zone:

```
fw      all     ACCEPT
loc     net     ACCEPT
vpn     loc     ACCEPT
net     fw      DROP    info
all     all     REJECT  info
```

/etc/shorewall/rules

Eccezioni alle policy predefinite.

Esempio:

1. Accetta connessioni SSH sul firewall da qualunque provenienza
2. Accetta dal rete locale le connessioni Webmin (TCP/10000) sul firewall
3. Accetta traffico Samba (condivisione cartelle) da un singolo indirizzo IP internet
4. Accetta Samba da tutta la rete locale
5. Accetta traffico web da qualunque origine
6. Ridirigi il traffico rdp (porta 3389) da 88.57.16.26 verso il server interno 192.168.3.4

NOTA: vedere il file **/etc/services** per la corrispondenza tra nome di un servizio e le porte usate

```
ACCEPT all fw tcp 22
ACCEPT loc fw tcp 10000
ACCEPT net:88.57.16.26 fw tcp 445
ACCEPT loc fw tcp 445
ACCEPT all fw tcp 80
DNAT net:88.57.16.26 loc:192.168.3.4 tcp 3389
```

/etc/shorewall/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
```

/etc/shorewall/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 (nessuna regola in questo esempio):

```
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
```

Verificare le regole prima di attivarle, quindi attiva le regole

```
shorewall check
shorewall restart
```

From:

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

Permanent link:

https://www.rigacci.net/wiki/doku.php/formazione/linux_sysadmin/shorewall?rev=1302702675



Last update: **2011/04/13 15:51**