

# Appunti configurazione firewall con distribuzione Zeroshell (lan + dmz + internet)



Il sistema operativo multifunzionale  
creato da Fulvio Ricciardi  
[www.zeroshell.net](http://www.zeroshell.net)

lan + dmz + internet  
( Autore: [massimo.giaino@sibtonline.net](mailto:massimo.giaino@sibtonline.net) )

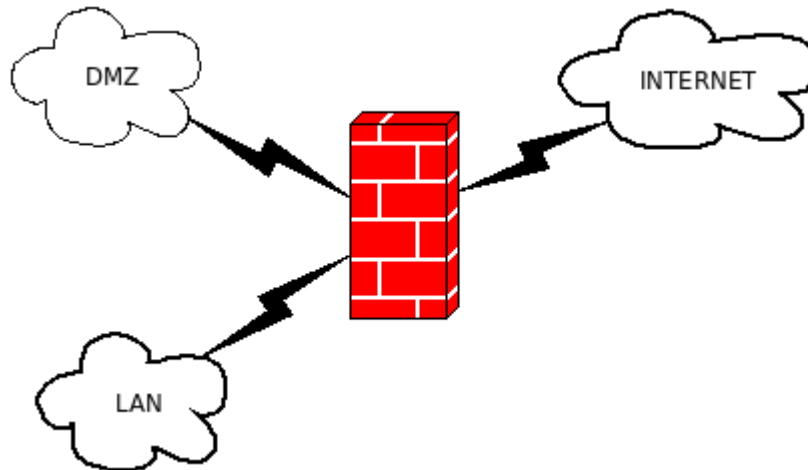
## CONFIGURAZIONE INTERFACCE

La configurazione che andremo a realizzare comprende tre interfacce:

l'interfaccia locale, dove risiedono workstation e server che devono navigare in internet

l'interfaccia esterna che andrà a collegarsi al router fornito dal provider

l'interfaccia della dmz, dove collocheremo i server accessibili dall'esterno (da internet)



Configuriamo le interfacce di rete dall'interfaccia web di Zeroshell (SYSTEM → Setup → Network) in questo modo:

Il screenshot mostra l'interfaccia web di Zeroshell, versione 1.0.beta11b. La pagina è divisa in una sidebar a sinistra con menu per SYSTEM, USERS, NETWORK e SECURITY. La parte principale mostra la configurazione delle interfacce di rete. Sono visibili le seguenti configurazioni:

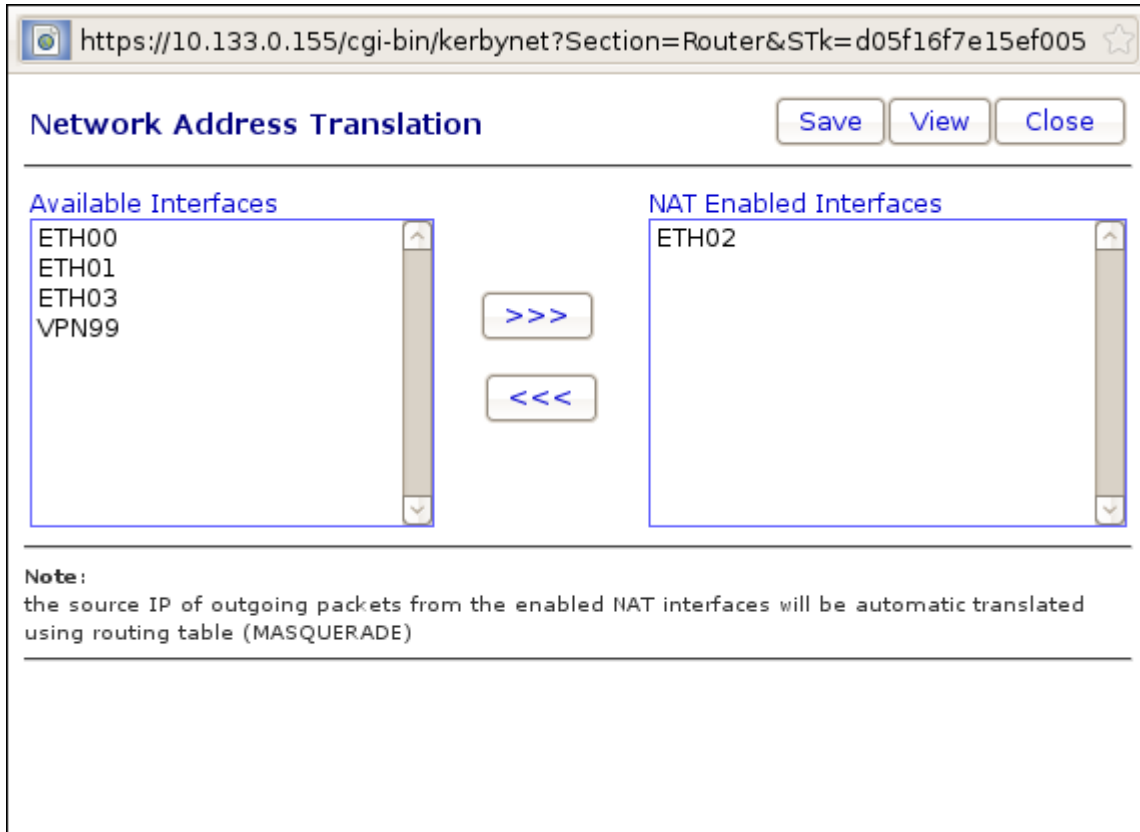
Interfaccia	Stato	Descrizione	IP	Operazioni
ETH00	UP	1000Mb/s Full Duplex Realtek Semiconductor Co., Ltd. RTL8111/8168 PCI Express Gigabit Ethernet controller (rev 02)	10.133.0.155	Dynamic IP: 0.0.0.0, MAC: 003018A86D93
ETH01	UP	No link detected Realtek Semiconductor Co., Ltd. RTL-8110SC/8169SC Gigabit Ethernet (rev 10)	192.168.0.155	Dynamic IP: 0.0.0.0, MAC: 003018AD3E79
ETH02	UP	100Mb/s Full Duplex Realtek Semiconductor Co., Ltd. RTL-8110SC/8169SC Gigabit Ethernet (rev 10)	255.255.255.113 - 255.255.255.117	Dynamic IP: 0.0.0.0, MAC: 003018AD3E71
ETH03	Down	Realtek Semiconductor Co., Ltd. RTL-8110SC/8169SC Gigabit Ethernet (rev 10)		Dynamic IP: 0.0.0.0, MAC: 003018AD3E72

Come possiamo vedere, è stato aggiunto un ip all'interfaccia della rete locale, (ETH00/10.133.0.155) e un ip all'interfaccia della rete dmz (ETH01/192.168.0.155). Invece all'interfaccia della rete pubblica sono stati aggiunti tutti gli indirizzi pubblici che ci sono stati forniti dal nostro provider (ETH02/da xxx.xxx.xxx.113 a xxx.xxx.xxx.117).

## NAT

Per consentire alle macchine dietro la rete locale e dietro alla dmz di navigare, è stato impostato il NAT sull'interfaccia esterna (ETH02).

Anche questa operazione è possibile eseguirla direttamente dall'interfaccia web di Zeroshell:



Sono state poi configurate le seguenti NAT 1:1 tra l'interfaccia di rete esterna e la dmz:

xxx.xxx.xxx.114 porta a 192.168.0.114 che avrà un server http e un server https in ascolto  
xxx.xxx.xxx.115 porta a 192.168.0.115 che avrà un server http in ascolto

ed è stato poi configurato il SNAT per far uscire i server dalla DMZ verso l'esterno con l'indirizzo corretto.

La configurazione delle NAT 1:1 va inserita nel file di startup (SYSTEM → Setup → Startup/Cron) nella sezione "Nat and Virtual Servers":

```
# fa il nat tra ip xxx.xxx.xxx..114 e ip 192.168.0.114 per le connessioni dall'esterno verso
# porta 443
iptables -t nat -A PREROUTING -p tcp -i ETH02 -d xxx.xxx.xxx..114 --dport 443 -j DNAT --
to-destination 192.168.0.114
# fa il nat tra ip xxx.xxx.xxx.114 e ip 192.168.0.114 per le connessioni dall'esterno verso
# porta 80
iptables -t nat -A PREROUTING -p tcp -i ETH02 -d xxx.xxx.xxx.114 --dport 80 -j DNAT
--to-destination 192.168.0.114
# fa uscire il server http/https 192.168.0.114 come xxx.xxx.xxx.114
iptables -t nat -A POSTROUTING -o ETH02 -s 192.168.0.114 -j SNAT --to
xxx.xxx.xxx.114
```

```

#
#
# fa il nat tra ip xxx.xxx.xxx.115 e ip 192.168.0.115 per le connessioni dall'esterno verso
# porta 80
iptables -t nat -A PREROUTING -p tcp -i ETH02 -d xxx.xxx.xxx.115 --dport 80 -j DNAT
--to-destination 192.168.0.115
# fa uscire il server http 192.168.0.115 come xxx.xxx.xxx.115
iptables -t nat -A POSTROUTING -o ETH02 -s 192.168.0.115 -j SNAT --to
xxx.xxx.xxx.115

```

## ROUTING

Come default gateway di Zeroshell è stato impostato l'indirizzo del router del nostro provider xxx.xxx.xxx.118

## MANAGEMENT

Abbiamo impostato la possibilità di fare management del firewall via https solamente attraverso l'interfaccia della rete interna. Stessa cosa è stata impostata per l'accesso ssh. L'operazione è possibile eseguirla da SYSTEM → Setup → https e da SYSTEM → Setup → ssh.

https://10.133.0.155/cgi-bin/kerbynet?Section=https&STk=d05f16f7e15ef00522443087c4300b8796f90be8

### HTTPS Web Interface Settings

Save Close

Allow access only from IP  Interface  + -

Interface ETH00

**Notes:** the IP addresses can be a single IP (ex. 192.168.0.15) or a subnet (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24). If the server becomes unreachable you could need to put the system into Fail-Safe mode using the local console to disable the Firewall.

### X.509 Configuration

View Cancel

X.509 Host Certificate

Local CA  OU=Hosts, CN=zeroshell.example.com

Status: OK Imported Trusted CAs

**Notes:** The new X.509 settings will be active only after a system reboot. You could need to close and reopen your http browser.

https://10.133.0.155/cgi-bin/kerbynet?Section=SSH&STk=d05f16f7e15ef00522443c

### Secure Shell Settings

Enabled Save Close

Allow access only from IP  Interface  + -

Subnet 10.133.0.0/24 from Interface ETH00

**Notes:**  
 The IP addresses can be a single IP (ex. 192.168.0.15) or a subnet (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24).  
 To login with SSH you must use the user **admin** and its Kerberos 5 password.

## REGOLE FIREWALL

Le policy di default per le catene di input e di output sono state impostate a DROP.  
 La policy di default per la catena di output è stata impostata ad ACCEPT.

Per la tabella di input sono state impostate le seguenti regole:

1 \* \* ACCEPT all opt -- in \* out \* 0.0.0.0/0 -> 0.0.0.0/0 state RELATED,ESTABLISHED

che consente tutti i pacchetti relativi a connessioni già stabilite o relativi e connessioni già esistenti.

2 ETH00 \* ACCEPT all opt -- in ETH00 out \* 10.133.0.0/24 -> 0.0.0.0/0

che consente tutti i pacchetti che provengono dall'interfaccia interna ETH00

Per la tabella di forward sono state impostate le seguenti regole:

1 \* \* ACCEPT all opt -- in \* out \* 0.0.0.0/0 -> 0.0.0.0/0 state RELATED,ESTABLISHED

che consente tutti i pacchetti relativi a connessioni già stabilite o relativi e connessioni già esistenti.

2 ETH00 \* ACCEPT all opt -- in ETH00 out \* 10.133.0.0/24 -> 0.0.0.0/0

che consente tutti i pacchetti che provengono dall'interfaccia interna ETH00

3 ETH01 ETH02 ACCEPT all opt -- in ETH01 out ETH02 192.168.0.0/24 -> 0.0.0.0/0

che consente tutti i pacchetti che provengono dall'interfaccia della dmz, diretti verso internet

4 ETH02 ETH01 ACCEPT tcp opt -- in ETH02 out ETH01 0.0.0.0/0 -> 192.168.0.114 tcp dpt:443

che consente di raggiungere la macchina 192.168.0.114 della dmz da internet, sulla porta 443

5 ETH02 ETH01 ACCEPT tcp opt -- in ETH02 out ETH01 0.0.0.0/0 -> 192.168.0.114 tcp dpt:80

che consente di raggiungere la macchina 192.168.0.114 della dmz da internet, sulla porta 80

6 ETH02 ETH01 ACCEPT tcp opt -- in ETH02 out ETH01 0.0.0.0/0 -> 192.168.0.115 tcp dpt:80

che consente di raggiungere la macchina 192.168.0.115 della dmz da internet, sulla porta 80