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

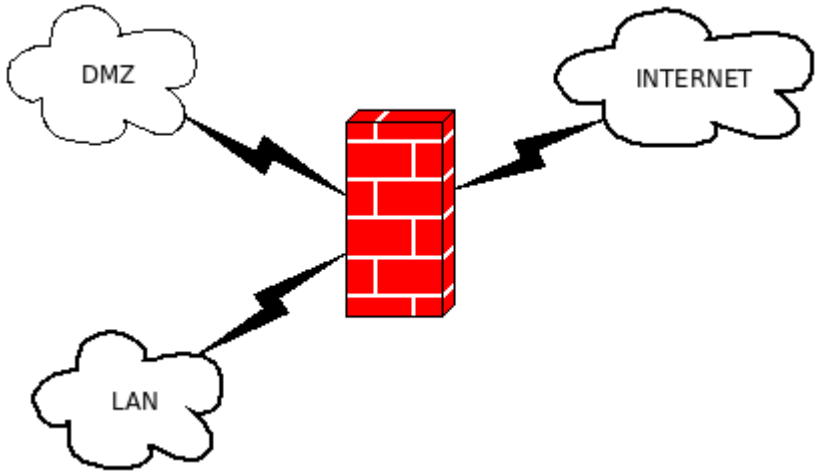
Il sistema operativo multifunzionale
creato da Fulvio Ricciardi
www.zeroshell.net

lan + dmz + internet
(Autore: massimo.giaimo@sibtonline.net)

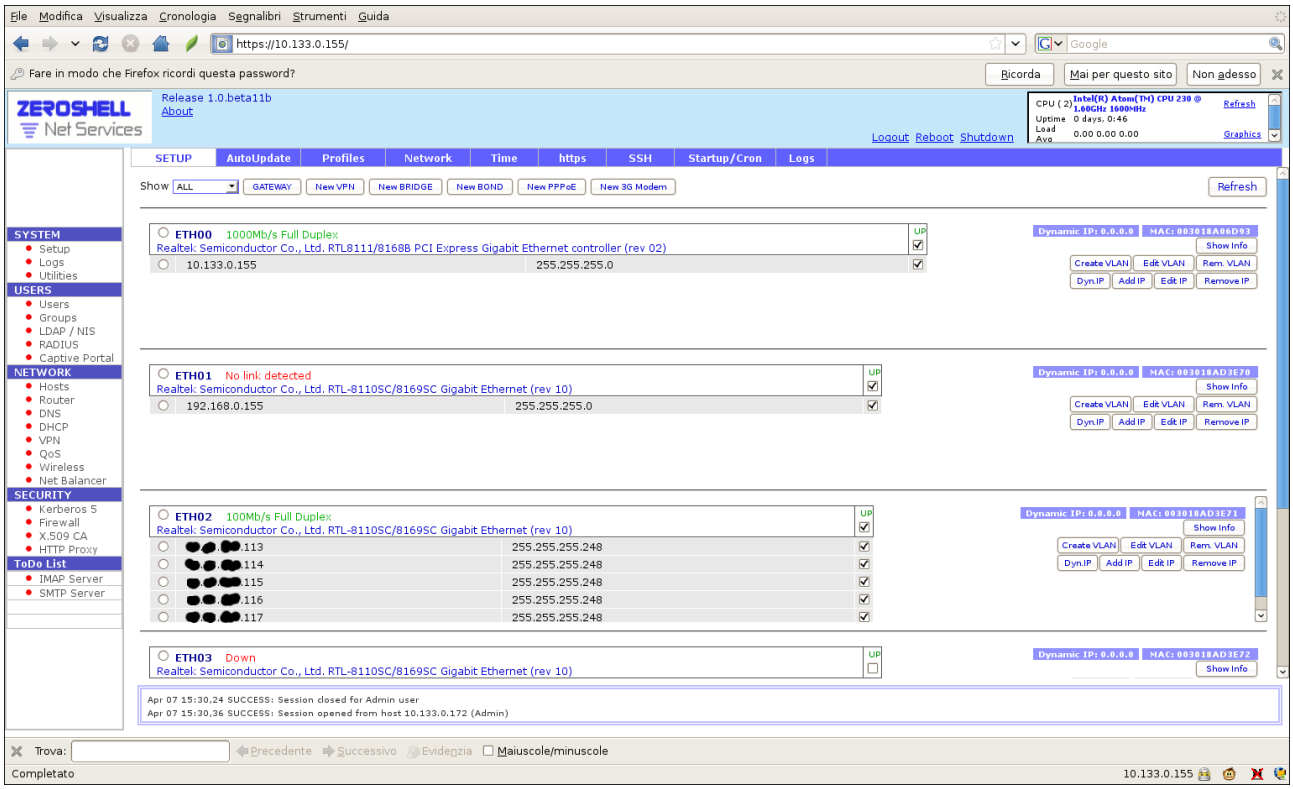
CONFIGURAZIONE INTERFACCE

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)



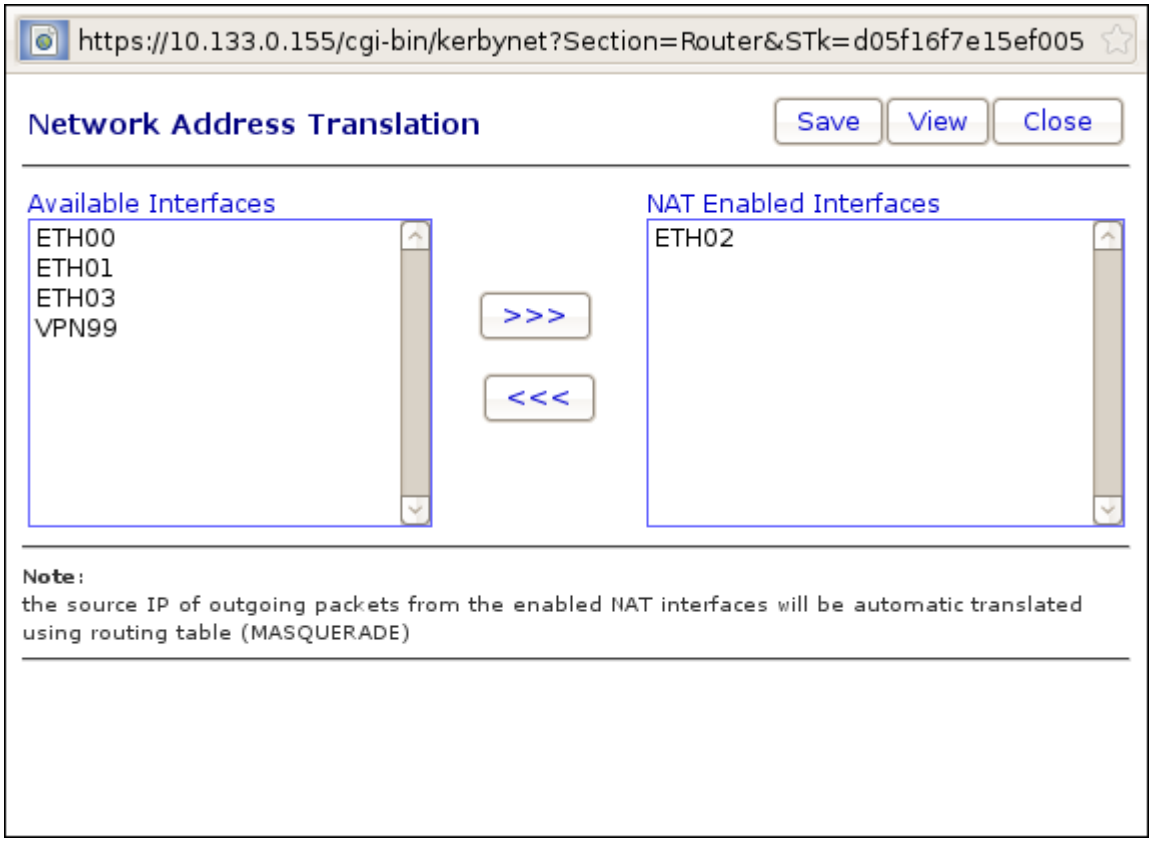
Configuriamo le interfacce di rete dall'interfaccia web di Zeroshell (SYSTEM → Setup → Network) in questo modo:



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

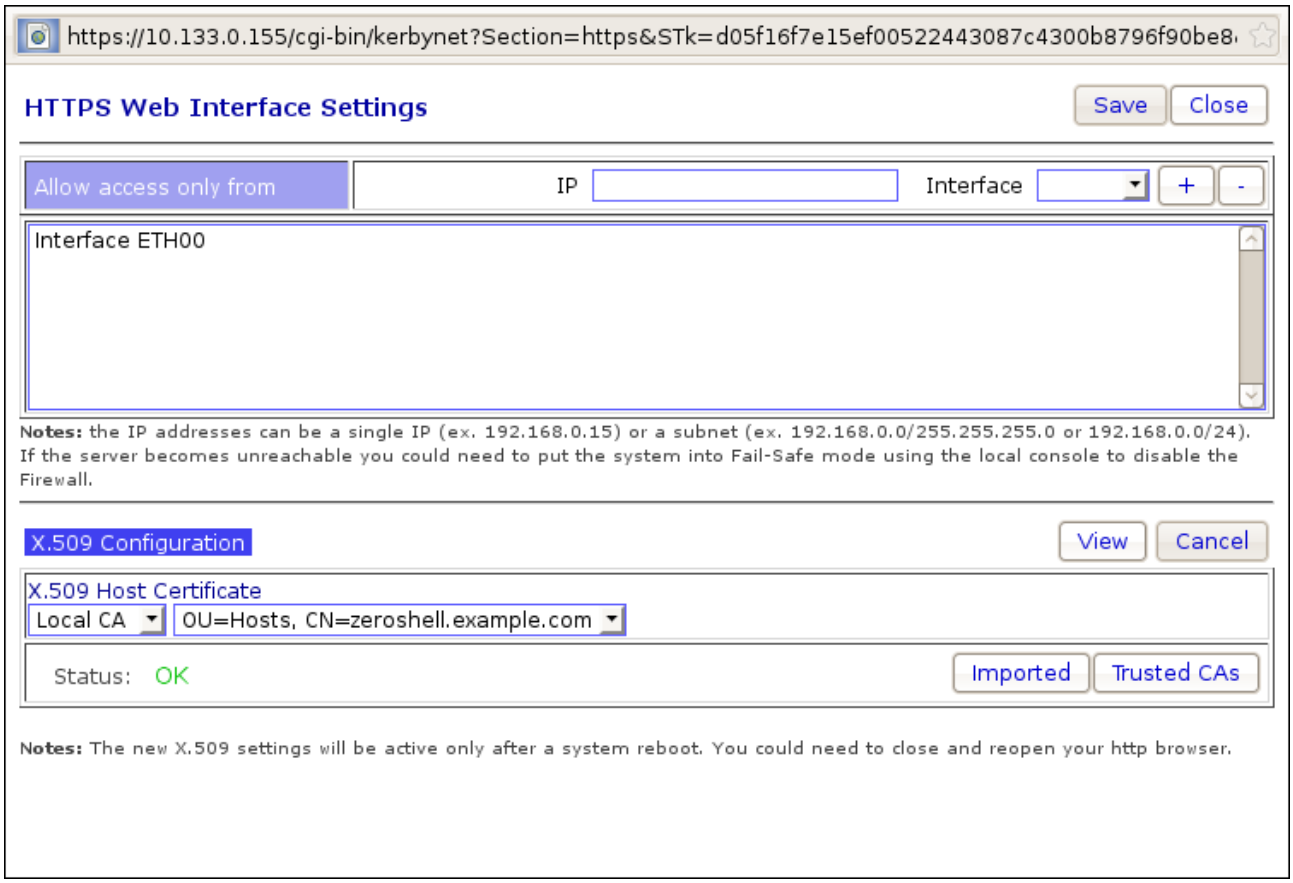
#
#
 # fa il nat tra ip xxx.xxx.xxx.115 e ip 192.168.0.115 per le connessioni dall'esterno verso
 # porta 80
iptables -t nat -A PREROUTING -p tcp -i ETH02 -d xxx.xxx.xxx.115 --dport 80 -j DNAT --to-destination 192.168.0.115
 # fa uscire il server http 192.168.0.115 come xxx.xxx.xxx.115
iptables -t nat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

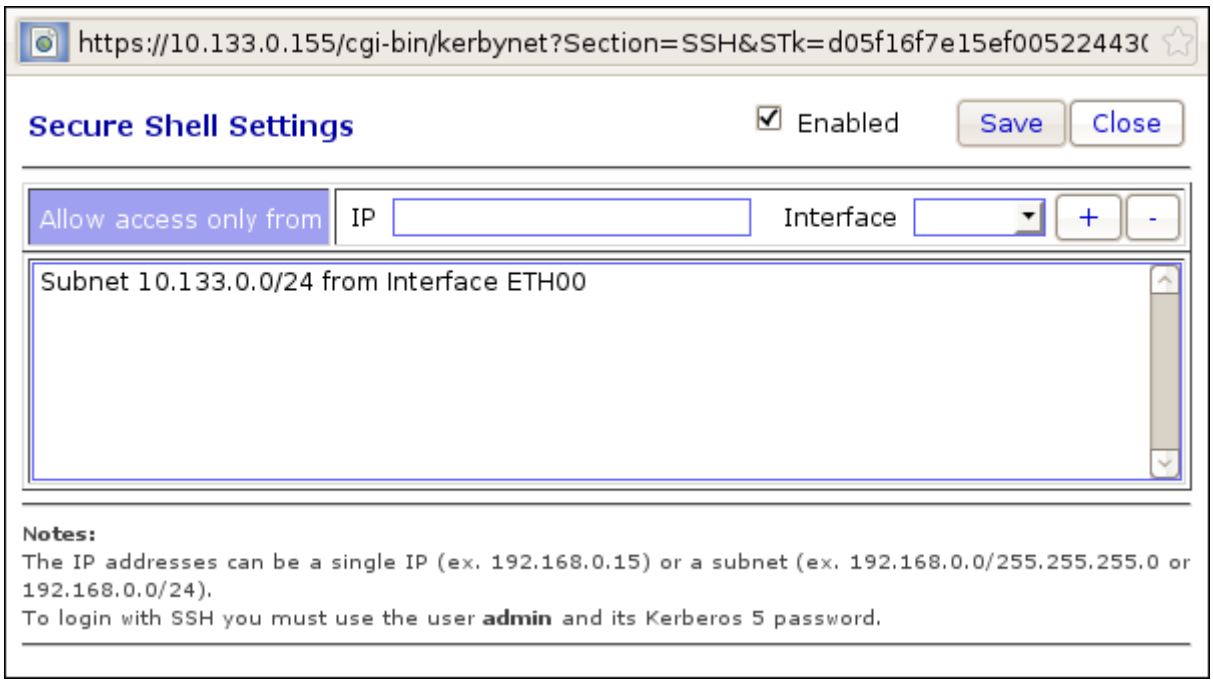
ROUTING

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.





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