Sallustio

Configurazione Interfacce

“/etc/conf.d/net”

net

```
# This blank configuration will automatically use DHCP for any net.*
# scripts in /etc/init.d.  To create a more complete configuration,
# please review /etc/conf.d/net.example and save your configuration
# in /etc/conf.d/net (this file :]!).

ns_domain_lo="3di.it"
dns_domain_eth0="3di.it"
dns_domain_eth1="3di.it"
dns_domain_eth2="3di.it"
nis_domain_lo="3di.it"
nis_domain_eth0="3di.it"
nis_domain_eth1="3di.it"
nis_domain_eth2="3di.it"
ns_search_lo="3di.it bo.priv"
dns_search_eth0="3di.it bo.priv"
dns_search_eth1="3di.it bo.priv"
dns_search_eth2="3di.it bo.priv"
nis_search_lo="3di.it bo.priv"
nis_search_eth0="3di.it bo.priv"
nis_search_eth1="3di.it bo.priv"
nis_search_eth2="3di.it bo.priv"
domainname="3di.it"

dns_servers="10.17.61.33 10.17.61.56"

config_eth0="10.17.61.1 netmask 255.255.255.0 broadcast 10.17.61.255"

config_eth1="10.17.62.82 netmask 255.255.255.248 broadcast 10.17.61.199"

config_eth2="93.149.47.162 netmask 255.255.255.248 broadcast 93.149.47.167
93.149.47.163 netmask 255.255.255.248 broadcast 92.223.169.87
93.149.47.164 netmask 255.255.255.248 broadcast 92.223.169.87
93.149.47.165 netmask 255.255.255.248 broadcast 92.223.169.87
93.149.47.166 netmask 255.255.255.248 broadcast 92.223.169.87"
routes_eth2="default via 93.149.47.161"
```

Configurazione Firewall

firewall

```
#!/bin/bash

# i = interface
# n = net
# h = host

iLAN=eth0
iDMZ=eth1
iWAN=eth2
iLO=lo
nLAN=10.17.61.0/24
nDMZ=10.17.62.80/29
#nWAN=92.223.169.80/29
nWAN=93.149.47.160/29
nCH=37.235.56.141
ndw4=213.183.146.126
```

```
#h1 = dns1 = titano/vegezio
#h1DMZint=10.17.62.197
h1DMZint=10.17.62.85
#h1DMZext=81.208.26.197
#h1DMZext=92.223.169.85
h1DMZext=93.149.47.165
#h2 = dns3
#h2DMZint=10.17.62.198
h2DMZint=10.17.62.86
#h2DMZext=81.208.26.198
#h2DMZext=92.223.169.86
h2DMZext=93.149.47.166
#h3 = 3didemo
#h3DMZint=10.17.62.195
h3DMZint=10.17.62.83
#h3DMZext=81.208.26.195
#h3DMZext=92.223.169.83
h3DMZext=93.149.47.163
#h4 = xenit
#h4DMZint=10.17.62.196
h4DMZint=10.17.62.84
#h4DMZext=81.208.26.196
#h4DMZext=92.223.169.84
h4DMZext=93.149.47.164
#h sallustio
#hMEint=10.17.62.194
hMEint=10.17.62.82
#hMEext=81.208.26.194
#hMEext=92.223.169.82
hMEext=93.149.47.162


# NON UTILIZZATO
#ipWind=151.58.8.95

iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

iptables -F
iptables -t nat -F

iptables -F WAN
iptables -X WAN
iptables -N WAN

iptables -F LAN
iptables -X LAN
iptables -N LAN

iptables -F DMZ
iptables -X DMZ
iptables -N DMZ

iptables -F WANFORWARD
iptables -X WANFORWARD
iptables -N WANFORWARD

iptables -F LANFORWARD
iptables -X LANFORWARD
iptables -N LANFORWARD

iptables -F DMZFORWARD
iptables -X DMZFORWARD
iptables -N DMZFORWARD
```

```
iptables -F BLACKLIST
iptables -X BLACKLIST
iptables -N BLACKLIST

iptables -F MARTIANS
iptables -X MARTIANS
iptables -N MARTIANS

iptables -F LOGFORWARD
iptables -X LOGFORWARD
iptables -N LOGFORWARD


# WAN input rules
iptables -A WAN -j BLACKLIST
iptables -A WAN -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# LAN input rules
iptables -A LAN -j ACCEPT

# DMZ input rules
iptables -A DMZ -j ACCEPT

# WAN forward list
iptables -A WANFORWARD -j BLACKLIST
iptables -A WANFORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A WANFORWARD -p tcp -d 10.17.61.33 --dport 636 -j ACCEPT
iptables -A WANFORWARD -p udp -d 10.17.61.33 --dport 636 -j ACCEPT
iptables -A WANFORWARD -p tcp -d 10.17.61.2 --dport 636 -j ACCEPT
iptables -A WANFORWARD -p udp -d 10.17.61.2 --dport 636 -j ACCEPT
#VPascali
iptables -A WANFORWARD -p tcp -d 10.17.61.2 -s $nCH --dport 389 -j ACCEPT
iptables -A WANFORWARD -p tcp -d 10.17.61.2 -s $ndw4 --dport 389 -j ACCEPT
iptables -A WANFORWARD -p tcp -d 10.17.61.2 -s 151.236.7.237 --dport 389 -j ACCEPT #LDAP FTP
iptables -A WANFORWARD -p tcp -d 10.17.61.33 --dport 389 -j ACCEPT
iptables -A WANFORWARD -p udp -d 10.17.61.33 --dport 389 -j ACCEPT
iptables -A WANFORWARD -p tcp -d 10.17.61.2 --dport 389 -j ACCEPT
iptables -A WANFORWARD -p udp -d 10.17.61.2 --dport 389 -j ACCEPT
iptables -A WANFORWARD -p tcp -d $h1DMZint -m multiport --dports 22,53,80,443,554 -j ACCEPT
iptables -A WANFORWARD -p tcp -d $h3DMZint -m multiport --dports 80,443 -j ACCEPT
iptables -A WANFORWARD -p tcp -d $h4DMZint -m multiport --dports 80,443 -j ACCEPT
#iptables -A WANFORWARD -p tcp -d $h2DMZint -m multiport --dports 25,53,80,443,465,993,2221
-j ACCEPT
iptables -A WANFORWARD -p tcp -d $h2DMZint -m multiport --dports 53,80,443,2221 -j ACCEPT
iptables -A WANFORWARD -p tcp -d $h2DMZint -s $nCH --dport 636 -j ACCEPT
iptables -A WANFORWARD -p tcp -d $h2DMZint -s $ndw4 --dport 636 -j ACCEPT
iptables -A WANFORWARD -p udp -d $h1DMZint --dport 53 -j ACCEPT
iptables -A WANFORWARD -p udp -d $h2DMZint --dport 53 -j ACCEPT
iptables -A WANFORWARD -p udp -d 10.17.61.52 --dport 1194 -j ACCEPT
iptables -A WANFORWARD -p udp -d 10.17.61.52 --dport 1194 -j ACCEPT
iptables -A WANFORWARD -p tcp -d 10.17.61.30 --dport 2525 -j ACCEPT # Laco Sharepoint Demo
iptables -A WANFORWARD -p udp -d 10.17.61.30 --dport 2525 -j ACCEPT # Laco Sharepoint Demo
#iptables -A WANFORWARD -p tcp -d 10.17.61.98 --dport 1521 -j ACCEPT # Laco Oracle
#iptables -A WANFORWARD -p udp -d 10.17.61.98 --dport 1521 -j ACCEPT # Laco Oracle
#iptables -A WANFORWARD -p tcp -d 10.17.61.181 --dport 3389 -j ACCEPT #
alberimonumentali.3di.it
#iptables -A WANFORWARD -p udp -d 10.17.61.181 --dport 3389 -j ACCEPT #
alberimonumentali.3di.it
#iptables -A WANFORWARD -p tcp -d 10.17.61.97 --dport 3389 -j ACCEPT # IRVV Odolini
#iptables -A WANFORWARD -p udp -d 10.17.61.97 --dport 3389 -j ACCEPT # IRVV Odolini
#iptables -A WANFORWARD -p tcp -d 10.17.61.62 --dport 3306 -j ACCEPT # mySQL Millennium
(fcavola)
#iptables -A WANFORWARD -p udp -d 10.17.61.62 --dport 3306 -j ACCEPT # mySQL Millennium
(fcavola)
```

```
iptables -A WANFORWARD -p tcp -d 10.17.61.62 --dport 22 -j ACCEPT # ssh Millennium (fcavola)
iptables -A WANFORWARD -p udp -d 10.17.61.62 --dport 22 -j ACCEPT # ssh Millennium (fcavola)
iptables -A WANFORWARD -p tcp -d 10.17.61.63 --dport 22 -j ACCEPT # ssh Magento (fcavola)
iptables -A WANFORWARD -p udp -d 10.17.61.63 --dport 22 -j ACCEPT # ssh Magento (fcavola)
iptables -A WANFORWARD -p tcp -d 10.17.61.61 --dport 22 -j ACCEPT # ssh VipMaster (svanetti)
iptables -A WANFORWARD -p udp -d 10.17.61.61 --dport 22 -j ACCEPT # ssh VipMaster (svanetti)
iptables -A WANFORWARD -p tcp -s $nCH -d 10.17.61.61 --dport 25 -j ACCEPT # Mail Server IT
#iptables -A WANFORWARD -p tcp -d 10.17.61.24 --dport 80 -j ACCEPT # forward FTSWS-temp per
rtirabassi
iptables -A WANFORWARD -p tcp -d 10.17.61.68 --dport 80 -j ACCEPT # forward ZoneMinder
iptables -A WANFORWARD -p tcp -d 10.17.61.68 --dport 22 -j ACCEPT # forward ZoneMinder
iptables -A WANFORWARD -p tcp -d 10.17.61.46 --dport 1521 -j ACCEPT #temp oracle-precise
dbms
iptables -A WANFORWARD -p tcp -d 10.17.61.17 --dport 1521 -j ACCEPT #temp regventest
iptables -A WANFORWARD -p tcp -d 10.17.61.8  --dport 22 -j ACCEPT # ssh gitlab
iptables -A WANFORWARD -p tcp -d 10.17.61.50  --dport 22 -j ACCEPT # ssh per supporto
easyredmine
iptables -A WANFORWARD -p tcp -d 10.17.61.192  --dport 22 -j ACCEPT # ssh Regesta
#VPN Albania
iptables -A WANFORWARD -p tcp -d 10.17.61.68 --dport 500 -j ACCEPT # forward VITO
iptables -A WANFORWARD -p tcp -d 10.17.61.68 --dport 4500 -j ACCEPT # forward VITO
iptables -A WANFORWARD -p tcp -d 10.17.61.68 --dport 1701 -j ACCEPT # forward VITO


# LAN forward list
iptables -A LANFORWARD -o $iWAN -j MARTIANS
iptables -A LANFORWARD -j ACCEPT

# DMZ forward list
iptables -A DMZFORWARD -o $iWAN -j MARTIANS
iptables -A DMZFORWARD -s $h1DMZint -j ACCEPT
iptables -A DMZFORWARD -s $h2DMZint -j ACCEPT
iptables -A DMZFORWARD -s $h3DMZint -j ACCEPT
iptables -A DMZFORWARD -s $h4DMZint -j ACCEPT

# PREROUTING rules
iptables -t nat -A PREROUTING -i $iLAN -s $nLAN -d $h1DMZext -j DNAT --to-destination
$h1DMZint
iptables -t nat -A PREROUTING -i $iLAN -s $nLAN -d $h2DMZext -j DNAT --to-destination
$h2DMZint
iptables -t nat -A PREROUTING -i $iLAN -s $nLAN -d $h3DMZext -j DNAT --to-destination
$h3DMZint
iptables -t nat -A PREROUTING -i $iLAN -s $nLAN -d $h4DMZext -j DNAT --to-destination
$h4DMZint
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $h1DMZext --dport 25 -j DNAT --to
10.17.61.61:25 # Mail Server IT su container LXC dedicato mail-it.bo.priv
iptables -t nat -A PREROUTING -i $iWAN -d $h1DMZext -j DNAT --to-destination $h1DMZint
iptables -t nat -A PREROUTING -i $iWAN -d $h2DMZext -j DNAT --to-destination $h2DMZint
iptables -t nat -A PREROUTING -i $iWAN -d $h3DMZext -j DNAT --to-destination $h3DMZint
iptables -t nat -A PREROUTING -i $iWAN -d $h4DMZext -j DNAT --to-destination $h4DMZint
#iptables -t nat -A PREROUTING -i $Wan -p tcp --dport 13389 -j DNAT --to 192.168.1.100:3389
# shape-cm enav-da-modificare
iptables -t nat -A PREROUTING -p tcp -d $hMEext --dport 2525 -j DNAT --to 10.17.61.30 # Laco
Sharepoint Demo
iptables -t nat -A PREROUTING -p udp -d $hMEext --dport 2525 -j DNAT --to 10.17.61.30 # Laco
Sharepoint Demo
#iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 1521 -j DNAT --to
10.17.61.98 # Laco Oracle ----NEW
#iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 1521 -j DNAT --to
10.17.61.98 # Laco Oracle ----NEW
#iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 13389 -j DNAT --to
10.17.61.181:3389 # alberimonumentali
#iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 13389 -j DNAT --to
10.17.61.181:3389 # alberimonumentali
#iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 13389 -j DNAT --to
```

```
10.17.61.97:3389 # IRVV Odolini
#iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 13389 -j DNAT --to
10.17.61.97:3389 # IRVV Odolini
#iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 13306 -j DNAT --to
10.17.61.62:3306 # mySQL Millennium (fcavola)
#iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 13306 -j DNAT --to
10.17.61.62:3306 # mySQL Millennium (fcavola)
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 33022 -j DNAT --to
10.17.61.62:22 # ssh Millennium (fcavola)
iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 33022 -j DNAT --to
10.17.61.62:22 # ssh Millennium (fcavola)
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 33023 -j DNAT --to
10.17.61.63:22 # ssh Magento (fcavola)
iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 33023 -j DNAT --to
10.17.61.63:22 # ssh Magento (fcavola)
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 33024 -j DNAT --to
10.17.61.61:22 # ssh VipMaster (svanetti)
iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 33024 -j DNAT --to
10.17.61.61:22 # ssh VipMaster (svanetti)
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 20000 -j DNAT --to
10.17.61.50:22 # ssh Per suppoerto easyredmine
iptables -t nat -A PREROUTING -p tcp -s 188.9.83.251 -d $hMEext --dport 20001 -j DNAT --to
10.17.61.192:22 # ssh Regesta
iptables -t nat -A PREROUTING -p tcp -s 195.78.211.98 -d $hMEext --dport 20001 -j DNAT --to
10.17.61.192:22 # ssh Regesta
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 10636 -j DNAT --to
10.17.61.33:636
iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 10636 -j DNAT --to
10.17.61.33:636
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 20636 -j DNAT --to
10.17.61.2:636
iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 20636 -j DNAT --to
10.17.61.2:636
#VPascali
iptables -t nat -A PREROUTING -p tcp -s 37.235.56.141 -i $iWAN -d $hMEext --dport 60389 -j
DNAT --to 10.17.61.33:389
iptables -t nat -A PREROUTING -p udp -s 37.235.56.141 -i $iWAN -d $hMEext --dport 60389 -j
DNAT --to 10.17.61.33:389
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 60389 -j DNAT --to
10.17.61.33:389
iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 60389 -j DNAT --to
10.17.61.33:389
iptables -t nat -A PREROUTING -p tcp -s 213.183.146.126 -i $iWAN -d $hMEext --dport 20389 -j
DNAT --to 10.17.61.33:389
iptables -t nat -A PREROUTING -p udp -s 213.183.146.126 -i $iWAN -d $hMEext --dport 20389 -j
DNAT --to 10.17.61.33:389
iptables -t nat -A PREROUTING -p udp -s 151.236.7.237 -i $iWAN -d $hMEext --dport 20389 -j
DNAT --to 10.17.61.33:389 #LDAP FTP
iptables -t nat -A PREROUTING -p tcp -s 151.236.7.237 -i $iWAN -d $hMEext --dport 20389 -j
DNAT --to 10.17.61.33:389 #LDAP FTP
iptables -t nat -A PREROUTING -p tcp -s 213.183.146.126 -i $iWAN -d $hMEext --dport 30389 -j
DNAT --to 10.17.61.2:389
iptables -t nat -A PREROUTING -p udp -s 213.183.146.126 -i $iWAN -d $hMEext --dport 30389 -j
DNAT --to 10.17.61.2:389
iptables -t nat -A PREROUTING -p tcp -s 213.183.146.83 -i $iWAN -d $hMEext --dport 60389 -j
DNAT --to 10.17.61.2:389
iptables -t nat -A PREROUTING -p udp -s 213.183.146.83 -i $iWAN -d $hMEext --dport 60389 -j
DNAT --to 10.17.61.2:389
iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 1194 -j DNAT --to
10.17.61.52
iptables -t nat -A PREROUTING -p udp -i $iWAN -d $hMEext --dport 1194 -j DNAT --to
10.17.61.52
#iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 10880 -j DNAT --to
10.17.61.24:80 # nat FTSWS-temp per rtirabassi
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 10880 -j DNAT --to
```

```
10.17.61.68:80 # nat ZoneMinder
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 10882 -j DNAT --to
10.17.61.68:22 # nat ZoneMinder
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 11521 -j DNAT --to
10.17.61.46:1521 #temp oracle-precise dbms
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 21521 -j DNAT --to
10.17.61.17:1521 #temp oracle regventest
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 5521 -j DNAT --to-
destination 10.17.61.8:22 # git.3di.it => gitlab.bo.priv
#VPN ALBANIA
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 500 -j DNAT --to
10.17.61.68:500 # nat VITO
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 4500 -j DNAT --to
10.17.61.68:4500 # nat VITO
iptables -t nat -A PREROUTING -p tcp -i $iWAN -d $hMEext --dport 1701 -j DNAT --to
10.17.61.68:1701 # nat VITO

# POSTROUTING rules

#iptables -t nat -A POSTROUTING -p udp -o $iLAN -s $nLAN -d 10.17.61.181 --dport 13389 -j
SNAT --to-source $hMEext # alberimonumentali.3di.it
iptables -t nat -A POSTROUTING -p udp -o $iLAN -s $nLAN -d 10.17.61.30 --dport 2525 -j SNAT
--to-source $hMEext # Laco Sharepoint Demo
iptables -t nat -A POSTROUTING -p tcp -o $iWAN -s 10.17.61.61 --dport 25 -j SNAT --to-source
$h4DMZext # Mail Server IT
#iptables -t nat -A POSTROUTING -p tcp -o $iWAN -s 10.17.61.8  -j MASQUERADE
iptables -t nat -A POSTROUTING -o $iLAN -d $nLAN -s $h1DMZint -j SNAT --to-source $h1DMZext
iptables -t nat -A POSTROUTING -o $iLAN -d $nLAN -s $h2DMZint -j SNAT --to-source $h2DMZext
iptables -t nat -A POSTROUTING -o $iLAN -d $nLAN -s $h3DMZint -j SNAT --to-source $h3DMZext
iptables -t nat -A POSTROUTING -o $iLAN -d $nLAN -s $h4DMZint -j SNAT --to-source $h4DMZext
iptables -t nat -A POSTROUTING -o $iWAN -s $h1DMZint -j SNAT --to-source $h1DMZext
iptables -t nat -A POSTROUTING -o $iWAN -s $h2DMZint -j SNAT --to-source $h2DMZext
iptables -t nat -A POSTROUTING -o $iWAN -s $h3DMZint -j SNAT --to-source $h3DMZext
iptables -t nat -A POSTROUTING -o $iWAN -s $h4DMZint -j SNAT --to-source $h4DMZext
#iptables -t nat -A POSTROUTING -o $iWAN -s $nLAN -j MASQUERADE
iptables -t nat -A POSTROUTING -o $iWAN -s $nLAN -j SNAT --to-source $hMEext
#iptables -t nat -A POSTROUTING -o $iDMZ -s $nLAN -j MASQUERADE
iptables -t nat -A POSTROUTING -o $iDMZ -s $nLAN -j SNAT --to-source $hMEint

# loopback!
iptables -A INPUT -i $iLO -j ACCEPT

# block unauthorized!!!
dirname=`dirname $0`
for i in `cat ${dirname}/ip_blacklist`; do
    iptables -A BLACKLIST -p tcp -s $i -j REJECT --reject-with=tcp-reset
    iptables -A BLACKLIST -s $i -j REJECT
done

# martians won't flee!!
dirname=`dirname $0`
for i in `cat ${dirname}/ip_martians`; do
        iptables -A MARTIANS -d $i -j DROP
done


# logging (LOGFORWARD)
# log pacchetti INVALID in LOGFORWARD
iptables -A LOGFORWARD -m conntrack --ctstate INVALID -j LOG --log-level 6 --log-
prefix="firewall: INVALID - "
# log ssh
iptables -A LOGFORWARD -m conntrack --ctstate NEW -p tcp -d $h2DMZint --dport 22 -j LOG --
log-level 6 --log-prefix="firewall: CVS - "
# log vpn
iptables -A LOGFORWARD -m conntrack --ctstate NEW -p tcp -d 10.17.61.52 --dport 1194 -j LOG
```

```
--log-level 6 --log-prefix="firewall: VPN - "
iptables -A LOGFORWARD -m conntrack --ctstate NEW -p udp -d 10.17.61.52 --dport 1194 -j LOG
--log-level 6 --log-prefix="firewall: VPN - "
# log sharepoint
iptables -A LOGFORWARD -m conntrack --ctstate NEW -p tcp -d 10.17.61.30 --dport 2525 -j LOG
--log-level 6 --log-prefix="firewall: SHAREPOINT -"
iptables -A LOGFORWARD -m conntrack --ctstate NEW -p udp -d 10.17.61.30 --dport 2525 -j LOG
--log-level 6 --log-prefix="firewall: SHAREPOINT -"
# log oracle
#iptables -A LOGFORWARD -m conntrack --ctstate NEW -p tcp -d 10.17.61.98 --dport 1521 -j LOG
--log-level 6 --log-prefix="firewall: ORACLE -"
#iptables -A LOGFORWARD -m conntrack --ctstate NEW -p udp -d 10.17.61.98 --dport 1521 -j LOG
--log-level 6 --log-prefix="firewall: ORACLE -"
iptables -A LOGFORWARD -m conntrack --ctstate NEW -p tcp -d 10.17.61.8 --dport 22 -j LOG --
log-level 6 --log-prefix="firewall: GIT -"
# chains
iptables -A INPUT -i $iWAN -j WAN
iptables -A INPUT -i $iLAN -j LAN
iptables -A INPUT -i $iDMZ -j DMZ
iptables -A FORWARD -j LOGFORWARD
iptables -A FORWARD -i $iWAN -j WANFORWARD
iptables -A FORWARD -i $iLAN -s $nLAN -j LANFORWARD
iptables -A FORWARD -i $iDMZ -j DMZFORWARD

# Chiude tutto il resto
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
```