

## d-link DSL-504 and IPTables trouble

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/5203.html>

---

**From:** Jacob Reimann ([jacob@nipplenettrino.net](mailto:jacob@nipplenettrino.net))

**Date:** 07/20/02

From: Jacob Reimann <[jacob@nipplenettrino.net](mailto:jacob@nipplenettrino.net)>

Date: Fri, 19 Jul 2002 23:24:35 +0100

The situation :

I have a Bto Adsl connection plugged into a D-link DSL 504 router. The router ethernet interface – 192.168.0.1 plugs into eth0 – 192.168.0.2 of my firewall box – Mandrake 8.2 – iptables. eth1 has a 192.168.152.12.

I have a an iptables script (attached) which is working fine on my home firewall on a cable connection.

I have copied this script onto the dsl firewall box.

I have then set up port forwarding on the d-link to forward ports 22,25,80 and 443 to 192.168.152.2.

The problem is that twhen I try and connect to the external interface of the router on ports 25 or 22 (ppp1) 214.x.x.x , I get a connection timeout. When I however connect to to port 80, I get straight through to Apache on the Mandrake box.

I have been checking the firewall kernel logs, and can see the connection attempts on ports 25 etc being dropped by iptables.

My question is if I have these ports enabled on the firewall, why is it dropping connections to them.

I have done a nmap scan, and it reports all the ports above as filtered, but port 80 open .

I have been going round the bend, because of the fact that it works as it should on the cable connection.

What is a filtered port, and could there be some issue with using port forwarding with iptables ??

I hope I have made myself clear – any help or tips would be appreciated .

Good night

```
#!/bin/sh
#Generated by Firestarter 0.7.1, NETFILTER in use

IPT=`which iptables`
MPB=`which modprobe`
LSM=`which lsmod`

#Some distributions still load ipchains
$LSM | grep ipchains -q -s && rmmod ipchains

#Loading Requested Kernel Modules
if ! ( $LSM | /bin/grep ip_conntrack > /dev/null ); then
$MPB ip_conntrack
fi
if ! ( $LSM | /bin/grep ipt_REJECT > /dev/null ); then
$MPB ipt_REJECT
fi
if ! ( $LSM | /bin/grep ipt_REDIRECT > /dev/null ); then
$MPB ipt_REDIRECT
fi
if ! ( $LSM | /bin/grep ipt_TOS > /dev/null ); then
$MPB ipt_TOS
fi
if ! ( $LSM | /bin/grep ipt_MASQUERADE > /dev/null ); then
$MPB ipt_MASQUERADE
fi
if ! ( $LSM | /bin/grep ipt_MIRROR > /dev/null ); then
$MPB ipt_MIRROR
fi
if ! ( $LSM | /bin/grep ipt_LOG > /dev/null ); then
$MPB ipt_LOG
fi
if ! ( $LSM | /bin/grep iptable_mangle > /dev/null ); then
$MPB iptable_mangle
fi
if ! ( $LSM | /bin/grep iptable_nat > /dev/null ); then
$MPB iptable_nat
fi

IF=eth0
INIF=eth1
IP=`/sbin/ifconfig $IF | grep inet | cut -d : -f 2 | cut -d \ -f 1`
MASK=`/sbin/ifconfig $IF | grep Mas | cut -d : -f 4`
NET=$IP/$MASK
```

## comp.security.firewalls: d-link DSL-504 and IPTables trouble

```
INIP=`/sbin/ifconfig $INIF | grep inet | cut -d : -f 2 | cut -d \ -f 1`
INMASK=`/sbin/ifconfig $INIF | grep Mas | cut -d : -f 4`
INNET=$INIP/$INMASK
#Delete user made chains. Flush and zero the chains.
$IPT -F
$IPT -X
$IPT -Z

#Delete `nat' and `mangle' chains.
if ( $LSM | /bin/grep iptable_mangle > /dev/null ); then
$IPT -t mangle -F
fi
if ( $LSM | /bin/grep iptable_nat > /dev/null ); then
$IPT -t nat -F
fi

#Create a new log and drop (LD) convenience chain.
$IPT -N LD
$IPT -A LD -j LOG
$IPT -A LD -j DROP

# Add simple logging for "attack" packets
#iptables -N logit
#iptables -A logit -j LOG --log-level warning --log-prefix "logit: "
#iptables -A logit -j DROP

# Log, disallow NEW and INVALID incoming or forwarded packets from eth1.
#iptables -A INPUT -i eth1 -m state --state NEW,INVALID -j logit
#iptables -A FORWARD -i eth1 -m state --state NEW,INVALID -j logit

STOP=LD

TOSOFT=4

#Deny all traffic on these ports, without logging
if [ -e /etc/firestarter/do-not-log-ports ]
then
source /etc/firestarter/do-not-log-ports
fi

#Deny all traffic from these machines
source /etc/firestarter/deny-all

#Portforwarding rules
if [ -e /etc/firestarter/portfw ]
then
source /etc/firestarter/portfw
fi

#Allow all traffic from these machines
source /etc/firestarter/allow-all
```

## comp.security.firewalls: d-link DSL-504 and IPtables trouble

```
#Allow a specific service to a specific machine
source /etc/firestarter/allow-service-machine

#Allow a specific service to everyone
source /etc/firestarter/allow-service-all

#Allow all traffic on the loopback interface
$IPT -t filter -A INPUT -i lo -s 0/0 -d 0/0 -j ACCEPT
$IPT -t filter -A OUTPUT -o lo -s 0/0 -d 0/0 -j ACCEPT

#Turn on source address verification in kernel
if [ -e /proc/sys/net/ipv4/conf/all/rp_filter ]; then
  for f in /proc/sys/net/ipv4/conf/*/rp_filter
  do
    echo 2 > $f
  done
fi

#Turn on syn cookies protection in kernel
if [ -e /proc/sys/net/ipv4/tcp_syncookies ]; then
  echo 1 > /proc/sys/net/ipv4/tcp_syncookies
fi

#ICMP Dead Error Messages protection
if [ -e /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses ]; then
  echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
fi

#ICMP Broadcasting protection
if [ -e /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts ]; then
  echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
fi

#Turn off dynamic TCP/IP address hacking
if [ -e /proc/sys/net/ipv4/ip_dynaddr ]; then
  echo 0 > /proc/sys/net/ipv4/ip_dynaddr
fi

#Doubling current limit for ip_contrack
if [ -e /proc/sys/net/ipv4/ip_contrack_max ]; then
  echo 16384 > /proc/sys/net/ipv4/ip_contrack_max
fi

#ICMP: Ping Requests
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type echo-request -j $STOP
#ICMP: Traceroute Requests
$IPT -t filter -A INPUT -p udp -s 0/0 -d $NET --dport 33434 -j $STOP
#ICMP: MS Traceroute Requests
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type destination-unreachable -j $STOP
#ICMP: Unreachable Requests
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type host-unreachable -j $STOP
```

## comp.security.firewalls: d-link DSL-504 and IPtables trouble

```
#ICMP: Timestamping Requests
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type timestamp-request -j $STOP
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type timestamp-reply -j $STOP
#ICMP: Address Masking
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type address-mask-request -j $STOP
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type address-mask-reply -j $STOP
#ICMP: Redirection Requests
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type redirect -j $STOP
#ICMP: Source Quench Requests
$IPT -t filter -A INPUT -p icmp -s 0/0 -d $NET --icmp-type source-quench -j $STOP
# ICMP vulnerabilty fix - 11/05/02 - JR
$IPT -A OUTPUT -m state -p icmp --state INVALID -j DROP
#FTP fix for masqed machines
#$MPB ip_nat_ftp

#Turn on IP forwarding
if [ -e /proc/sys/net/ipv4/ip_forward ]
then
echo 1 > /proc/sys/net/ipv4/ip_forward
fi

#Forward Int/Ext & Ext/Int Traffic before Masquerading
$IPT -t filter -A FORWARD -d 0/0 -s $INNET -o $IF -j ACCEPT
$IPT -t filter -A FORWARD -d $INNET -j ACCEPT
#Masquerade outgoing traffic
$IPT -t nat -A POSTROUTING -o $IF -j MASQUERADE

#Don't masq external interface traffic
$IPT -t nat -A POSTROUTING -s $NET -d 0/0 -j ACCEPT

#Allow traffic from internal network going anywhere
$IPT -t filter -A INPUT -s $INNET -d 0/0 -j ACCEPT
$IPT -t filter -A OUTPUT -s $INNET -d 0/0 -j ACCEPT
$IPT -t filter -A OUTPUT -p icmp -s $INNET -d 0/0 -j ACCEPT

#Setting default forwarding rule
$IPT -t filter -P FORWARD DROP

#Altering Type of Service (ToS) flags

#ToS: Server Applications
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 20:21 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 22 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 25 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 53 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 67 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 80 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 110 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 143 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 443 --set-tos $TOSOFT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 1812 --set-tos $TOSOFT
```

## comp.security.firewalls: d-link DSL-504 and IPtables trouble

```
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 1813 --set-tos $TOSOPT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 2401 --set-tos $TOSOPT
$IPT -t mangle -A OUTPUT -p tcp -j TOS --dport 8080 --set-tos $TOSOPT
```

### #Block nonroutable IPs

```
$IPT -t filter -A INPUT -s 1.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 2.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 7.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 23.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 27.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 31.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 41.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 45.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 60.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 68.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 69.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 70.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 71.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 80.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 88.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 90.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 91.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 92.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 100.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 111.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 112.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 127.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 127.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 128.66.0.0/16 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 172.16.0.0/12 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 192.168.0.0/16 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 197.0.0.0/16 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 201.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 220.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 222.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 240.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 242.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 244.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 251.0.0.0/8 -d $NET -i $IF -j $STOP
$IPT -t filter -A INPUT -s 254.0.0.0/8 -d $NET -i $IF -j $STOP
```

### #Block Back Orifice

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 31337 -m limit --limit 2/minute -j $STOP
$IPT -t filter -A INPUT -p udp -s 0/0 -d $NET --dport 31337 -m limit --limit 2/minute -j $STOP
```

```
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 31337 -m limit --limit 2/minute -j $STOP
$IPT -t filter -A OUTPUT -p udp -s $NET -d 0/0 --dport 31337 -m limit --limit 2/minute -j $STOP
```

### #Block Trinity v3

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 33270 -m limit --limit 2/minute -j $STOP
$IPT -t filter -A INPUT -p udp -s 0/0 -d $NET --dport 33270 -m limit --limit 2/minute -j $STOP
```

## comp.security.firewalls: d-link DSL-504 and IPtables trouble

```
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 33270 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A OUTPUT -p udp -s $NET -d 0/0 --dport 33270 -m limit --limit 2/minute -j $STOP
```

### #Block Subseven (1.7/1.9)

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 1234 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 6711 -m limit --limit 2/minute -j $STOP
```

```
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 1234 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 6711 -m limit --limit 2/minute -j $STOP
```

### #Block Stacheldraht

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 16660 --syn -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 60001 --syn -m limit --limit 2/minute -j $STOP
```

```
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 16660 --syn -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 60001 --syn -m limit --limit 2/minute -j $STOP
```

### #Block NetBus

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 12345:12346 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A INPUT -p udp -s 0/0 -d $NET --dport 12345:12346 -m limit --limit 2/minute -j $STOP
```

```
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 12345:12346 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A OUTPUT -p udp -s $NET -d 0/0 --dport 12345:12346 -m limit --limit 2/minute -j $STOP
```

### #Block Trin00

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 1524 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 27665 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A INPUT -p udp -s 0/0 -d $NET --dport 27444 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A INPUT -p udp -s 0/0 -d $NET --dport 31335 -m limit --limit 2/minute -j $STOP
```

```
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 1524 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A OUTPUT -p tcp -s $NET -d 0/0 --dport 27665 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A OUTPUT -p udp -s $NET -d 0/0 --dport 27444 -m limit --limit 2/minute -j $STOP  
$IPT -t filter -A OUTPUT -p udp -s $NET -d 0/0 --dport 31335 -m limit --limit 2/minute -j $STOP
```

### #Block Multicast

```
$IPT -t filter -A INPUT -s 224.0.0.0/8 -d 0/0 -j $STOP  
$IPT -t filter -A INPUT -s 0/0 -d 224.0.0.0/8 -j $STOP  
$IPT -t filter -A OUTPUT -s 224.0.0.0/8 -d 0/0 -j $STOP  
$IPT -t filter -A OUTPUT -s 0/0 -d 224.0.0.0/8 -j $STOP
```

### #Block Packets with Stuffed Routing

```
$IPT -t filter -A INPUT -s 255.255.255.255 -j $STOP  
$IPT -t filter -A INPUT -d 0.0.0.0 -j $STOP  
$IPT -t filter -A OUTPUT -s 255.255.255.255 -j $STOP  
$IPT -t filter -A OUTPUT -d 0.0.0.0 -j $STOP
```

## comp.security.firewalls: d-link DSL-504 and IPtables trouble

### #Block Fragmented Packets

```
$IPT -t filter -A INPUT -f -m limit --limit 10/minute -j $STOP
```

### #DHCP

```
$IPT -t filter -A INPUT -p udp -s 0/0 -d 0/0 --dport 67:68 -i $IF -j ACCEPT
```

### #FTP

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 20 ! --syn -j ACCEPT
```

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 21 -j ACCEPT
```

### #SSH

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 22 -j ACCEPT
```

### #SMTP

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 25 -j ACCEPT
```

### #HTTP

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 80 -j ACCEPT
```

### #SSL HTTP

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 443 -j ACCEPT
```

### #IMAP

```
#$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 143 -j ACCEPT
```

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d $NET --dport 993 -j ACCEPT
```

### #Block SAMBA

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d 0/0 --dport 137:139 -i $IF -j $STOP
```

```
$IPT -t filter -A INPUT -p udp -s 0/0 -d 0/0 --dport 137:139 -i $IF -j $STOP
```

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d 0/0 --dport 445 -i $IF -j $STOP
```

```
$IPT -t filter -A INPUT -p udp -s 0/0 -d 0/0 --dport 445 -i $IF -j $STOP
```

### #IPSec / KLIPS

```
$IPT -t filter -A INPUT -p udp -s 0/0 -d 0/0 --dport 500 -j ACCEPT
```

```
$IPT -t filter -A INPUT -p 51 -s 0/0 -d 0/0 -j ACCEPT
```

### #Block NFS

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d 0/0 --dport 2049 -i $IF -j $STOP
```

```
$IPT -t filter -A INPUT -p udp -s 0/0 -d 0/0 --dport 2049 -i $IF -j $STOP
```

### #Block Xwindows

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d 0/0 --dport 6000:6015 -i $IF -j $STOP
```

```
$IPT -t filter -A INPUT -p udp -s 0/0 -d 0/0 --dport 6000:6015 -i $IF -j $STOP
```

### #block squid

```
$IPT -t filter -A INPUT -p tcp -s 0/0 -d 0/0 --dport 3128 -i $IF -j $STOP
```

### #Allow ICMP Output

```
$IPT -A OUTPUT -p icmp -s $NET -d 0/0 -j ACCEPT
```

## comp.security.firewalls: d-link DSL-504 and IPtables trouble

#Open ports for inbound established connections

#SSH fix

```
$IPT -A INPUT -p tcp --sport 22 --dport 513:65535 ! --syn -m state --state RELATED -j ACCEPT
```

#FTP Data fix

```
$IPT -A INPUT -p tcp --sport 20 --dport 1023:65535 ! --syn -m state --state RELATED -j ACCEPT
```

```
$IPT -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
```

```
$IPT -A INPUT -p udp -s 0/0 -d $NET --dport 1023:65535 -j ACCEPT
```

```
$IPT -A INPUT -p tcp -s 0/0 -d $NET --dport 1023:65535 -j ACCEPT #ftp fix
```

#Open ports for outbound established connections

```
$IPT -A OUTPUT -p tcp -s $NET -d 0/0 --dport 1023:65535 -j ACCEPT
```

```
$IPT -A OUTPUT -p udp -s $NET -d 0/0 --dport 1023:65535 -j ACCEPT
```

#Deny everything not let through earlier

```
$IPT -A INPUT -j $STOP
```

---

- *Next message:* [mhicaoidh: "Re: ZA "Plus" Trialware"](#)
- *Previous message:* [Duane Arnold: "Re: BlackIce Issue"](#)
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)