Contents

Depreciated,

- See Access Restrictions

Global Blacklisting per MAC

If you have a lot of DD-WRT routers, then denying of access for abusing users through the web interface of each router can be time consuming.

Here is a small firewall script to automatically download MAC-addresses of computers that should be denied access. The format of the file is Unix textfile one MAC address per line. The script assumes that you have a jffs partition. You can run it at startup by saving it as /jffs/etc/config/wifi_bl.wanup

```
#!/bin/sh
cd /jffs
rm wifi_blacklist.txt
#Please modify the script to download the blacklist file from your web server
wget http://www.myserver.com/wifi_blacklist.txt
module_exists=`lsmod | grep ipt_mac`
if [ -z "$module_exists" ] ; then
    insmod ipt_mac
fi
#Deleting the old table
old_mac=`iptables -L | egrep "..:..:..:..:..:.."  | sed "s/.*\(..:..:..:..:..:..\).*/\1/"`
for mac in $old_mac ; do
    iptables -D FORWARD -p tcp -m mac --mac-source $mac -j REJECT --reject-with tcp-reset
done
#Adding the table again
for mac in `cat /jffs/wifi_blacklist.txt` ; do
    iptables -I FORWARD -p tcp -m mac --mac-source $mac -j REJECT --reject-with tcp-reset
done
```

White Listing

If you want to create a white list to block access by default but allow certain traffic through, then you can use this script to do it. Remove any junk comment lines beginning with # to save nvram space. Discuss here.

```
# IP Tables White Listing script by phuzi0n -Tek @ http://www.dd-wrt.com/phpBB2/viewtopic.php?t=5
# This Wiki Page http://www.dd-wrt.comhttp://wiki.dd-wrt.com/wiki/index.php/Blocking_URLs/IPs#Whi
# Version 5. Please increment version number with subsequent modifications. GeeTek.

# Set up the chain
iptables -N wanout
iptables -I INPUT -i `nvram get lan_ifname` -j wanout
iptables -I FORWARD -i `nvram get lan_ifname` -j wanout
```

```
# Create whitelist 'function' script
WOUT="/tmp/wanout"
echo 'iptables -I wanout  -j ACCEPT' > $WOUT
chmod 777 $WOUT

# Exempt Machine MAC
# load xt_mac instead of ipt_mac on k2.6 builds
insmod ipt_mac
$WOUT '-m mac --mac-source 00:30:18:A9:A9:C6'

# Exempt Machine IP
$WOUT '-s 192.168.1.2'

# Allow everyone access to these sites  (DNS lookup only happens once when rule is inserted and s
$WOUT '-d www.google.com'
$WOUT '-d www.yahoo.com'
$WOUT '-d www.dd-wrt.com'

# Allow everyone access to these IP addresses/netmask
$WOUT '-d 74.125.67.100'
$WOUT '-d 74.125.127.100'
$WOUT '-d 74.125.45.100/24'
$WOUT '-d 209.131.36.158/29'

#Allow everyone access to specific destination ports
$WOUT '-p udp --dport 8000'

# Everything else gets blocked
iptables -A wanout -j REJECT --reject-with icmp-proto-unreachable

# IP Tables White Listing script by phuzi0n -Tek @ http://www.dd-wrt.com/phpBB2/viewtopic.php?t=5
# Version 1.1 for older chipsets and/or experimental firmware builds. Please freeze this version.
# URL for this Wiki Page http://www.dd-wrt.comhttp://wiki.dd-wrt.com/wiki/index.php/Blocking_URLs

# Set up the chain
iptables -N wanout
iptables -I FORWARD -i `nvram get lan_ifname` -j wanout

# Exempt Machine MAC
iptables -I wanout -m mac --mac-source 00:30:18:A9:A9:C6 -j ACCEPT

# Exempt Machine IP
iptables -I wanout -s 192.168.1.2 -j ACCEPT

# Allow everyone access to these sites (DNS lookup only happens once when rule is inserted and st
iptables -I wanout -d www.google.com -j ACCEPT
iptables -I wanout -d www.yahoo.com -j ACCEPT
iptables -I wanout -d www.dd-wrt.com -j ACCEPT

# Allow everyone access to these IP Addresses
iptables -I wanout -d 74.125.45.100 -j ACCEPT
iptables -I wanout -d 8.8.8.8 -j ACCEPT

# Allow everyone access to these IP Address ranges
iptables -A wanout -m iprange --dst-range 4.1.2.3-4.5.6.7 -j ACCEPT

# Allow everyone access to these Subnets
iptables -A wanout -d 7.0.0.0/8 -j ACCEPT

#Allow everyone access to specific destination ports
iptables -A wanout -i `nvram get lan_ifname` -p udp --dport 24500 -j ACCEPT
```

```
# Everything else gets blocked
iptables -A wanout -j REJECT --reject-with icmp-proto-unreachable

#modified script to work from (at least) build 21286. and decreasing required nvram space. (by ja
#IP Tables White Listing script by phuzi0n -Tek @ http://www.dd-wrt.com/phpBB2/viewtopic.php?t=56
#This Wiki Page http://www.dd-wrt.comhttp://wiki.dd-wrt.com/wiki/index.php/Blocking_URLs/IPs#Whit
#Version 6. Please increment version number with subsequent modifications. GeeTek.

#Set up the chain
iptables -N wanout
iptables -I INPUT -i `nvram get lan_ifname` -j wanout
iptables -I FORWARD -i `nvram get lan_ifname` -j wanout

#Create whitelist 'function' script
WOUT='iptables -I wanout  -j ACCEPT'
MAC='-m mac --mac-source'

# Exempt Machine MAC
$WOUT $MAC 00:30:18:A9:A9:C6

#Exempt Machine IP
$WOUT -s 192.168.1.2

#Allow everyone access to these sites  (DNS lookup only happens once when rule is inserted and st
$WOUT -d www.google.com
$WOUT -d www.yahoo.com
$WOUT -d www.dd-wrt.com

#Allow everyone access to these IP addresses/netmask
$WOUT -d 74.125.67.100
$WOUT -d 74.125.127.100
$WOUT -d 74.125.45.100/24
$WOUT -d 209.131.36.158/29

#Allow everyone access to specific destination ports
$WOUT -p udp --dport 8000

#Everything else gets blocked
iptables -A wanout -j REJECT --reject-with icmp-proto-unreachable
```

http://www.dd-wrt.comhttp://wiki.dd-wrt.com/wiki/index.php/Ad_blocking