



PRICE DROP

\$23,140

[Iptables](#) → [Iptables](#) → Iptables MAC

MAC Address

ite • Last updated: December 27, 2005

ss can be filtered by using the
vices transmitting within your n
n for media access control add
ed to almost all-networking har
outers, mobile phones, wireles
[ess](#) at wikipedia for more infor
s how to block or deny access
ministration tool for IPv4 packe

Get Paid to Write

Learn step
how to w
earn a nic
No expe
need

Barefoot

Op

Linux Iptables comes with the MAC module. This module matches packets traveling through the firewall based on their MAC (Ethernet hardware) address. It offers good protection against malicious users who spoof or change their IP address. Remember that mac filtering only makes sense for packets coming

START

3 Easy Steps:

- 1) **Click** 'Start'
- 2) Download Extension
- 3) Get Custom Search Tool

**3 Easy Steps:**

- 1) **Click** 'Start'
- 2) **Download** Extension
- 3) **Get** Custom Search Tool

1. PREROUTING

2. FORWARD

3. INPUT



Examples: Access Restrictions Using MAC Address

Drop all connection coming from mac address 00:0F:EA:91:04:08 (add the following command to your firewall script):

```
/sbin/iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP
```

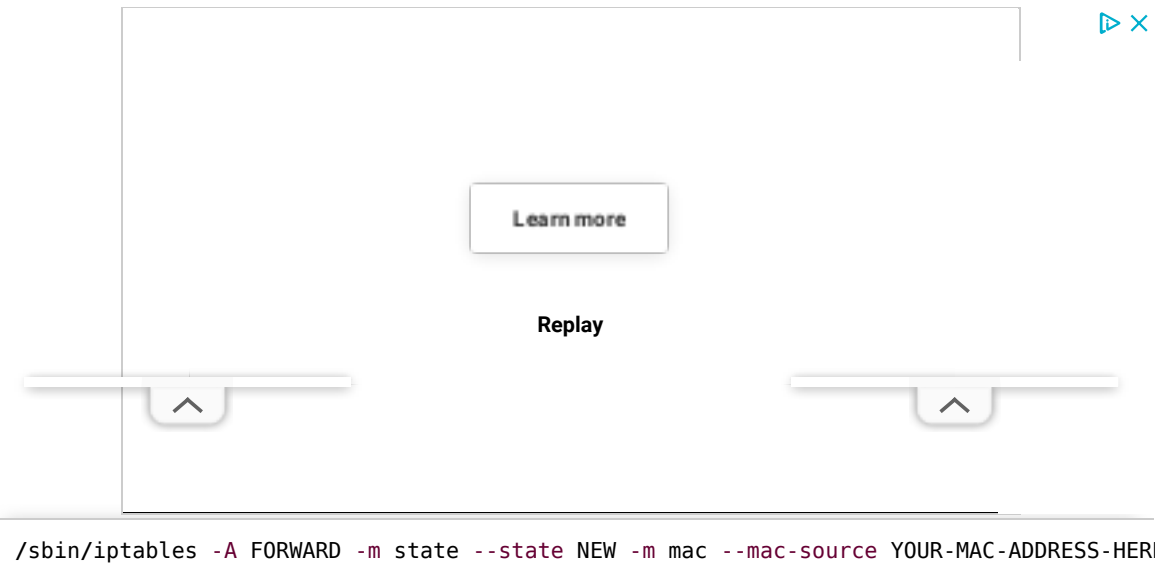
You can also use the interface name such as eth1:

```
/sbin/iptables -A INPUT -i eth1 -p tcp --destination-port 22 -m mac --mac-source 00:0F:00:00:00:00
```

You can also use FORWARD chain:

```
/sbin/iptables -A FORWARD -i ethX -m mac --mac-source YOUR-MAC-ADDRESS-HERE -j ACCEPT
```

You can also use NEW and other supported states as follows so that a known MAC address can be forwarded:

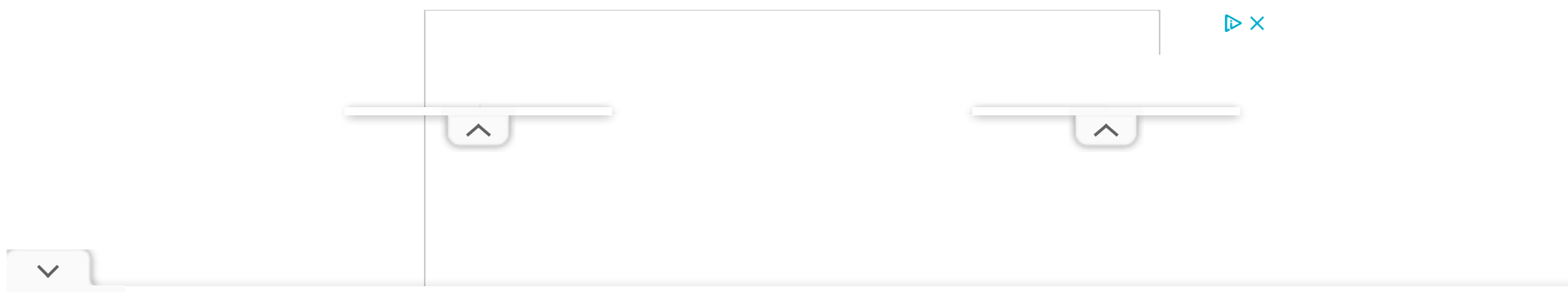


Use the following syntax:

```
/sbin/iptables -A INPUT -p tcp --dport PORT -m mac ! --mac-source MAC-ADDRESS-HERE-TO-SI
### Drop ssh access to all except our own MAC Address ###
/sbin/iptables -A INPUT -p tcp --dport 22 -m mac ! --mac-source YOUR-MAC-ADDRESS-HERE -
### Save rules ###
/sbin/service iptables save
```

The ! symbol means NOT. Your firewall will DROP packets destined to port 22 so long as they do NOT originate from your own computer with the desired MAC address.

Protecting MAC Address Spoofing From a Trusted Systems



kind of attacks use [VLANS](#) and/or static ARP entries.

See iptables man page for more information:

```
man 8 iptables
```

About the author: Vivek Gite is the founder of nixCraft, the oldest running blog about Linux and open source. He wrote more than 7k+ posts and helped numerous readers to master IT topics. Join the nixCraft community via [RSS Feed](#), [Email Newsletter](#) or follow on [Twitter](#).

🙄 Was this helpful? Please add [a comment to show your appreciation or feedback](#) ↓ Support the nixCraft with a [PayPal donation](#) if you use Adblock 🙏

🔍 To search, type & hit enter...

Related Posts

[Security Through Obscurity: MAC Address Filtering \(Layer 2...](#)



[How To Secure Mac OS X Computer \(Hardening Mac \)](#)



[FreeBSD: HowTo Change IP Address / Setup New IP Address For...](#)

[Linux Iptables block incoming access to selected or specific...](#)

[Linux Iptables Block Outgoing Access To Selected or Specific...](#)

[Google earth for Linux and MAC OS X released - A 3D...](#)

Start Now

3 Easy Steps:

- 1) **Click** 'Start Now'
- 2) Download Extension
- 3) Get Custom Search Tool

[Now run your windows applications, seamlessly on Mac OS X](#)



Category	List of Unix and Linux commands
Database Server	Backup MySQL server • MariaDB Galera cluster • MariaDB TLS/SSL • MariaDB replication • MySQL Server • MySQL remote access
Download managers	wget
Driver Management	Linux Nvidia driver • lsmod
Documentation	help • mandb • man • pinfo
Disk Management	df • dub • ncdu • pydf
File Management	cat • cp • less • mkdir • more • tree
Firewall	Alpine Awall • CentOS 8 • OpenSUSE • RHEL 8 • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 20.04 • Ubuntu 24.04
KVM Virtualization	CentOS/RHEL 7 • CentOS/RHEL 8 • Debian 9/10/11 • Ubuntu 20.04
Linux Desktop apps	Chrome • Chromium • GIMP • Skype • Spotify • VLC 3
LXD	Backups • CentOS/RHEL • Fedora • Mount dir • Ubuntu 20.04
Modern utilities	bat • exa
Network Management	Monitoring tools • Network services • RHEL static IP • Restart network interface • nmcli
Network Utilities	NetHogs • dig • nmap • ping
OpenVPN	CentOS 7 • CentOS 8 • Debian 10 • Debian 11 • Debian 8/9 • Ubuntu 18.04 • Ubuntu 20.04
Power Management	upower

Category	List of Unix and Linux commands
Shell builtins	compgen • echo • printf
System Management	reboot • shutdown
Terminal/ssh	sshpass • tty
Text processing	cut • rev
Text Editor	6 Text editors • Save and exit vim
User Environment	exit • who
User Information	groups • id • lastcomm • last • lid/libuser-lid • logname • members • users • whoami • w
User Management	/etc/group • /etc/passwd • /etc/shadow • chsh
Web Server	Apache • Let's Encrypt certificate • Lighttpd • Nginx Security • Nginx
WireGuard VPN	Alpine • Amazon Linux • CentOS 8 • Debian 10 • Firewall • Ubuntu 20.04 • qrencode

38 comments... [add one](#) ↓


Anonymous Jan 7, 2006 @ 8:58

Thanks!

[reply](#) [link](#)

addresses. thanks in advance

[reply](#) [link](#)

 **nixcraft** • Aug 15, 2006 @ 15:23

You can setup default policy to drop all packets and allow selected incoming packets from MAC based ip filtering.

Set default INPUT to deny all

Setting default filter policy

iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

iptables -A INPUT -m mac --mac-source

00:0F:EA:91:04:08 -j ACCEPT

HTH

[reply](#) [link](#)

Vladimir • Jan 28, 2015 @ 9:39

Would this work? As everyone is asking for ACL of MAC addresses.

```
iptables -A INPUT -m mac --mac-source  
00:0F:EA:91:04:08 -j ACCEPT  
00:0F:EA:91:AA:BB -j ACCEPT  
..  
..
```

[reply](#) [link](#)

Michael Egan • Nov 15, 2006 @ 0:40

Does anybody know if this works on Suse 10.0? I need to filter a few MACs.

[reply](#) [link](#)

rick • Mar 23, 2007 @ 22:46

Is there a way to get the MAC address of an attacker via iptable logging? All of the log levels that I've tried give me my server's MAC address. I'd love to get the MAC of the person I'm blocking so I can block on their MAC in case they try using a pro

ex: -A RH-Firewall-1-INPUT -s ATTACKER_IP_HERE -j LOG --log-level 4 --log-prefix "DROP ATTACKER: "

DST=MY_SERVER_IP LEN=48 TOS=0x00 PREC=0x00 TTL=114 ID=50714 DF
PROTO=TCP SPT=39616 DPT=80 WINDOW=65535 RES=0x00 SYN URGP=0

[reply](#) [link](#)

irfan • Oct 3, 2007 @ 15:18

hello i am using iptables

now i need that only those mac id can accept all other droped who can i do this

[reply](#) [link](#)

Catalin • Nov 13, 2007 @ 18:30

Hello. I have a problem when i try to log with iptables. iptables v1.3.8: Unknown
arg `LOG'

what should i do ?

[reply](#) [link](#)

zee • Nov 19, 2007 @ 14:50

please i want to ban everyone of using my shell which is port 22 but keep their

Lilian • Nov 28, 2007 @ 5:57

to ZEE

Allow an ip or network group to conect via SSH

/etc/host.allow

SSHD:192.168.0.4 or something like this 192.168.0.

Deny all conection on SSH

/etc/host.deny


SSHD:ALL

I think it will help you

[reply](#) [link](#)

Orvalho J  **isto** • May 7, 2008 @ 2:32

Great!

 You are good ones

Shawn • May 12, 2008 @ 20:26


Is there a way to use this in conjunction with the source IP. So that you can enforce a MAC address to only be allowed through if it is using a specific IP address?

—

Thanks

Shawn

[reply](#) [link](#)

 **nixCraft** • May 12, 2008 @ 20:33

Sure, you can use -s IP-address option. Verify source IP 192.168.1.200 along with MAC 00:0F:EA:91:04:08 and if both matched drop it:

```
iptables -A INPUT -p tcp -s 192.168.1.200 -m mac --mac-source  
00:0F:EA:91:04:08 -j DROP
```

[reply](#) [link](#)

Luis • Jul 8, 2008 @ 16:07

0B:62:9D:6D:1A:34

I made ping suceful but when I try ftp ore telnet it refuse the conection...

[reply](#) [link](#)

coop • Mar 26, 2009 @ 13:46

Hello

I wanna config a router with iptables for my WLAN. my problem, there is a database (mysql) there are all mac adresses, whitch have access...

is there a way to marry iptables with mysql??

best & THX coop

[reply](#) [link](#)

 **nixCraft** • Mar 26, 2009 @ 16:07

I don't think so.. you need to take help of perl or python and send those IPs using system or exec or " call to iptables.

[reply](#) [link](#)



Here is a script i use to write my iptables.

```
#!/usr/bin/perl

use DBI;

$sql_user      = "dhcpd";
$sql_password  = "*****";
$sql_database  = "dhcpd";
$sql_hostname  = "localhost";
$sql_port      = "3306";

$dsn          = "DBI:mysql:database=$sql_database;host=$sql_hostname";
print "-----n";
print "      Building iptables config from mysql      n";
print "-----n";
print "Getting information from mysql database      ";
$dbh = DBI->connect($dsn, $sql_user, $sql_password);
$getmac = $dbh->prepare("select mac from trusted order by ip");
$getip = $dbh->prepare("select ip from trusted order by ip");
$getmac->execute;
```

```
print "Creating temp file...";
#print `rm iptables.conf.temp`;
open (CONFIGFILE, '>>iptables.conf.temp');
print "Donen";
print "Start writing configfile...n-----

$count      = 0;

while ( @getmac = $getmac->fetchrow_array, @getip = $getip->fetch
    @mac[$count] = @getmac;
    @ip[$count] = @getip;
    $count++;
}

$dbh->disconnect;
$count = 0;

foreach (@mac) {
    print CONFIGFILE "iptables -A INPUT -p tcp -s @ip[$count] -m i
    " . " ";
    $count++;
}
```

```
close (CONFIGFILE);  
print "-----nDone.n";  
print `mv iptables.conf.temp iptables.conf`;  
sleep(1);  
#print `echo "do something here :)"`
```

I also made one for dhcpd so unknown mac's logging on my wireless will be in a different subnet.

[reply](#) [link](#)

 **nixCraft** • Apr 6, 2009 @ 14:19

Thanks for sharing perl script.

[reply](#) [link](#)

Atheya • Nov 2, 2009 @ 0:50

How do I execute this Perl script?

[reply](#) [link](#)

 **Zohaib Hussain** • Feb 22, 2010 @ 6:22

m facing the prb of mac spoofing but some of users whom i blocked by my server they user mac address changer different softwares and by this software they detect any Online Active user mac address and just change the IP Address and use internet and when i try to block that mac address by iptables but i cant block that mac address because its mine online active users mac and who users blocked the connection of my LAN they do these things and use mac address changing software and get solid and valid legal mac address by network scanning. what i do i m much confused

[reply](#) [link](#)

Robert • Mar 24, 2010 @ 17:02

Zohaib,

Sorry to say this but using Mac address filtering to control access to your network is like using a locked screen door to control access to your house. It keeps the generally honest out but doesn't stop those who's motives are less than pure. It's a good general backup to the main security, but it is not a main security measure in and off itself. We use passwords and Mac filtering. Mac Address filtering makes it harder to use a stolen or hacked password.

[reply](#) [link](#)



if you have a proxy server then use password authentication
better if you have a managed switch
statically fix the ip address and MAC for every switch port
that way the only way to access the network is to use a certain IP address with
the Original MAC address of the NIC while plugged to the correct switch port
and i don't think that there is any way around this

check also VLAN

[reply](#) [link](#)

Tawfiq • May 12, 2010 @ 4:35

is it possible to put the info in a separate file and call it from your main firewall
script?

lets say, there is a file called /root/scripts/ip-mac-list

where u have the info written as,

```
[code] 192.168.0.1 00:13:xx:xx:xx:xx
```

```
[/code]
```

[reply](#) [link](#)

raj • Jun 17, 2010 @ 10:59

I do not want to block TCP or UDP Traffic at all.

Thanks

[reply](#) [link](#)

Andy • Apr 8, 2011 @ 18:59

Can I use this tutorial to create a MAC filter between a wireless network switch and the core? I need access to the network resources so I can't use a router. What would you suggest?

[reply](#) [link](#)

Madhab • Jun 6, 2011 @ 14:28

Hi,

I wanna block internet some computer PC with mac address which rule can do it

[reply](#) [link](#)

Jim • Aug 26, 2011 @ 21:41

Dert • Oct 22, 2011 @ 1:07

Jim, i think no because i haven't found in man special mac-adress diapason system support (like for IP-adresses)

[reply](#) [link](#)

Willy • Oct 3, 2012 @ 9:04

Hi,

someone knows why that command:

```
iptables -A INPUT -i eth0 -p tcp --dport 1234 -m mac --mac-source  
XX:XX:XX:XX:XX -j ACCEPT
```

works properly in a pc with iptables 1.4.4 and it give me this error:

iptables: No chain/target/match by that name.

on a pc with iptables 1.4.12.1

—

Willy

Hai,

Can anyone let me know how to block all the mac addresses except two mac addresses in the linux server..

[reply](#) [link](#)

Tom Boland • Jun 24, 2013 @ 17:19

Warning on trying to use `-mac-source` when on a VM instance: It may not work.

For instance, in Hyper-V , the VM host machine's IP address for the switch is what will **always** show as the source mac address, rather than the true mac address.

It may also be true for VMware, depending on configuration of the switch on the host.

[reply](#) [link](#)

John • Nov 26, 2014 @ 19:04

Thanks for this post. I don't really see this anywhere else in the IPTables documentation, though I could be missing it

If one fails (maybe just forgets) to implement a prohibition on source routing (i.e. on a new install), it would be possible to source route (or partially source route) even an non-route-able packet to a destination in a LAN, ostensibly from the IPTables protected host, and then to respond to that opened pinhole (related connection) in the IPTables firewall. I presently see rogue hosts, which are NOT DNS servers, sending unsolicited DNS responses (UDP/TCP port 53) to various hosts on my LAN (as well as faux ICMP responses) to try to open that pinhole to respond to. The ploy is almost as prevalent as MITM attacks, though, since it's really difficult to detect good MITM attacks, how many MITM attacks can really be identified?

[reply](#) [link](#)

maresh deshmkh • Dec 2, 2014 @ 5:59

by using the above commands i'm getting the following error..

iptables v1.4.12:ether

can any1 help pls?

[reply](#) [link](#)

Helipil0t • Oct 26, 2015 @ 19:29

```
iptables -I FORWARD -m mac --mac-source XX:XX:XX:XX:XX:01 -j ACCEPT
sudo iptables -A FORWARD -j DROP
```

Which give me the following table:

Chain FORWARD (policy ACCEPT 322 packets, 181K bytes)

num	pkts	bytes	target	prot	opt	in	out	source
1	342	21034	ACCEPT	0	--	*	*	0.0.0.0/0
2	490	28916	DROP	0	--	*	*	0.0.0.0/0

This SHOULD allow the mac address full access.. But all packets are still being dropped. The client has no access to the internet. Can anyone help me out.

What am I doing wrong? This is on DD-WRT. Thanks

[reply](#) [link](#)

devoarabawy@gmail.com • Aug 4, 2016 @ 9:32

```
[root@localhost ~]# iptables -A INPUT -i enp0s25 -p tcp --destination-port 22 -m
mac --mac-source 14-58-D0-B7-2C-A7 -j ACCEPT
iptables v1.4.21: ether
Try `iptables -h' or 'iptables --help' for more information.
```

Wrong format: 14-58-D0-B7-2C-A7

Need to be in 14:58:D0:B7:2C:A7

[reply](#) [link](#)

JOEL AGUSTIN SANCHEZ BALTAZAR • Jan 17, 2017 @ 2:50

This works only in a LAN enviroment or in a internet public webserver?

[reply](#) [link](#)

Mani • Feb 21, 2017 @ 3:00

i want to write a rule in IPtable so that i can any single MAC address to telnet on port 2333. any suggestions??

[reply](#) [link](#)

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *



Name

Email

Website

Post Comment



Use HTML `<pre>...</pre>` for code samples. Your comment will appear only after approval by the site admin.



Next post: [GTK+ fundamentals, Part 1: Why use GTK+?](#)

Previous post: [How To Monitor Bandwidth With iptables](#)

FEATURED ARTICLES

- 1 [30 Cool Open Source Software I Discovered in 2013](#)
- 2 [30 Handy Bash Shell Aliases For Linux / Unix / Mac OS X](#)
- 3 [Top 32 Nmap Command Examples For Linux Sys/Network Admins](#)
- 4 [25 PHP Security Best Practices For Linux Sys Admins](#)
- 5 [30 Linux System Monitoring Tools Every SysAdmin Should Know](#)
- 6 [40 Linux Server Hardening Security Tips](#)
- 7 [Linux: 25 Iptables Netfilter Firewall Examples For New SysAdmins](#)
- 8 [Top 20 OpenSSH Server Best Security Practices](#)
- 9 [Top 25 Nginx Web Server Best Security Practices](#)
- ✓ 10 [My 10 UNIX Command Line Mistakes](#)

[Linux shell scripting tutorial](#)[RSS/Feed](#)[About nixCraft](#)

©2002-2023 nixCraft • [Privacy](#) • [ToS](#) • [Contact/Email](#) • Corporate patron [Linode & Cloudflare](#)

