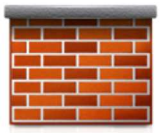
≡ Menu

- Home
- About
- Contact / Email us

nixCraft
Linux Tips, Hacks, Tutorials, And Ideas In Blog Format

Linux: 20 Iptables Examples For New SysAdmins

by Vivek Gite on December 13, 2011
in Iptables, Linux, Linux distribution, Linux Embedded devices, Linux laptop



Linux comes with a host based firewall called Netfilter. According to the official project site:

> netfilter is a set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack.

This Linux based firewall is controlled by the program called iptables to handles filtering for IPv4, and ip6tables handles filtering for IPv6. I strongly recommend that you first read our quick tutorial that explains how to configure a host-based firewall called Netfilter (iptables) under CentOS / RHEL / Fedora / Redhat Enterprise Linux. This post list most common iptables solutions required by a new Linux user to secure his or her Linux operating system from intruders.

IPTABLES Rules Example

- Most of the actions listed in this post are written with the assumption that they will be executed by the root user running the bash or any other modern shell. Do not type commands on remote system as it will disconnect your access.
- For demonstration purpose I've used RHEL 6.x, but the following command should work with any modern Linux distro.
- This is NOT a tutorial on how to set iptables. See tutorial here. It is a quick cheat sheet to common iptables commands.

#1: Displaying the Status of Your Firewall

Type the following command as root:

```
# iptables -L -n -v
```

Sample outputs:

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Above output indicates that the firewall is not active. The following sample shows an active firewall:

```
# iptables -L -n -v
```

Sample outputs:

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
  394 43586 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
   93 17292 ACCEPT     all  --  br0    *       0.0.0.0/0            0.0.0.0/0
    1   142 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  br0    br0     0.0.0.0/0            0.0.0.0/0
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
    0     0 TCPMSS     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x02 TCPMSS clamp to PMTU
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 wanin      all  --  vlan2  *       0.0.0.0/0            0.0.0.0/0
    0     0 wanout     all  --  *      vlan2   0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  br0    *       0.0.0.0/0            0.0.0.0/0
Chain OUTPUT (policy ACCEPT 425 packets, 113K bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain wanin (1 references)
 pkts bytes target     prot opt in     out     source               destination
Chain wanout (1 references)
 pkts bytes target     prot opt in     out     source               destination
```

Where,

- **-L** : List rules.
- **-v** : Display detailed information. This option makes the list command show the interface name, the rule options, and the TOS masks. The packet and byte counters are also listed, with the suffix 'K', 'M' or 'G' for 1000, 1,000,000 and 1,000,000,000 multipliers respectively.
- **-n** : Display IP address and port in numeric format. Do not use DNS to resolve names. This will speed up listing.

#1.1: To inspect firewall with line numbers, enter:

```
# iptables -n -L -v --line-numbers
```

Sample outputs:

```
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       all  --  0.0.0.0/0            0.0.0.0/0           state INVALID
2    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
2    DROP       all  --  0.0.0.0/0            0.0.0.0/0           state INVALID
3    TCPMSS     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x02 TCPMSS clamp to PMTU
```

```
4    ACCEPT     all  --  0.0.0.0/0           0.0.0.0/0           state RELATED,ESTABLISHED
5    wanin      all  --  0.0.0.0/0           0.0.0.0/0
6    wanout     all  --  0.0.0.0/0           0.0.0.0/0
7    ACCEPT     all  --  0.0.0.0/0           0.0.0.0/0
Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
Chain wanin (1 references)
num  target     prot opt source               destination
Chain wanout (1 references)
num  target     prot opt source               destination
```

You can use line numbers to delete or insert new rules into the firewall.

#1.2: To display INPUT or OUTPUT chain rules, enter:

```
# iptables -L INPUT -n -v
# iptables -L OUTPUT -n -v --line-numbers
```

#2: Stop / Start / Restart the Firewall

If you are using CentOS / RHEL / Fedora Linux, enter:

```
# service iptables stop
# service iptables start
# service iptables restart
```

You can use the iptables command itself to stop the firewall and delete all rules:

```
# iptables -F
# iptables -X
# iptables -t nat -F
# iptables -t nat -X
# iptables -t mangle -F
# iptables -t mangle -X
# iptables -P INPUT ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD ACCEPT
```

Where,

- **-F** : Deleting (flushing) all the rules.
- **-X** : Delete chain.
- **-t table_name** : Select table (called nat or mangle) and delete/flush rules.
- **-P** : Set the default policy (such as DROP, REJECT, or ACCEPT).

#3: Delete Firewall Rules

To display line number along with other information for existing rules, enter:

```
# iptables -L INPUT -n --line-numbers
# iptables -L OUTPUT -n --line-numbers
# iptables -L OUTPUT -n --line-numbers | less
# iptables -L OUTPUT -n --line-numbers | grep 202.54.1.1
```

You will get the list of IP. Look at the number on the left, then use number to delete it. For example delete line number 4, enter:

```
# iptables -D INPUT 4
```

OR find source IP 202.54.1.1 and delete from rule:

```
# iptables -D INPUT -s 202.54.1.1 -j DROP
```

Where,

- **-D** : Delete one or more rules from the selected chain

#4: Insert Firewall Rules

To insert one or more rules in the selected chain as the given rule number use the following syntax. First find out line numbers, enter:

```
# iptables -L INPUT -n --line-numbers
```

Sample outputs:

```
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       all  --  202.54.1.1          0.0.0.0/0
2    ACCEPT     all  --  0.0.0.0/0           0.0.0.0/0           state NEW,ESTABLISHED
```

To insert rule between 1 and 2, enter:

```
# iptables -I INPUT 2 -s 202.54.1.2 -j DROP
```

To view updated rules, enter:

```
# iptables -L INPUT -n --line-numbers
```

Sample outputs:

```
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       all  --  202.54.1.1          0.0.0.0/0
2    DROP       all  --  202.54.1.2          0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0           0.0.0.0/0           state NEW,ESTABLISHED
```

#5: Save Firewall Rules

To save firewall rules under CentOS / RHEL / Fedora Linux, enter:

```
# service iptables save
```

In this example, drop an IP and save firewall rules:

```
# iptables -A INPUT -s 202.5.4.1 -j DROP
# service iptables save
```

For all other distros use the iptables-save command:

```
# iptables-save > /root/my.active.firewall.rules
# cat /root/my.active.firewall.rules
```

#6: Restore Firewall Rules

To restore firewall rules form a file called /root/my.active.firewall.rules, enter:
```
# iptables-restore < /root/my.active.firewall.rules
```
To restore firewall rules under CentOS / RHEL / Fedora Linux, enter:
```
# service iptables restart
```

#7: Set the Default Firewall Policies

To drop all traffic:
```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
# iptables -L -v -n
#### you will not able to connect anywhere as all traffic is dropped ###
# ping cyberciti.biz
# wget http://www.kernel.org/pub/linux/kernel/v3.0/testing/linux-3.2-rc5.tar.bz2
```

#7.1: Only Block Incoming Traffic

To drop all incoming / forwarded packets, but allow outgoing traffic, enter:
```
# iptables -P INPUT DROP
# iptables -P FORWARD DROP
# iptables -P OUTPUT ACCEPT
# iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -L -v -n
### *** now ping and wget should work *** ###
# ping cyberciti.biz
# wget http://www.kernel.org/pub/linux/kernel/v3.0/testing/linux-3.2-rc5.tar.bz2
```

#8:Drop Private Network Address On Public Interface

IP spoofing is nothing but to stop the following IPv4 address ranges for private networks on your public interfaces. Packets with non-routable source addresses should be rejected using the following syntax:
```
# iptables -A INPUT -i eth1 -s 192.168.0.0/24 -j DROP
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

#8.1: IPv4 Address Ranges For Private Networks (make sure you block them on public interface)

- 10.0.0.0/8 -j (A)
- 172.16.0.0/12 (B)
- 192.168.0.0/16 (C)
- 224.0.0.0/4 (MULTICAST D)
- 240.0.0.0/5 (E)
- 127.0.0.0/8 (LOOPBACK)

#9: Blocking an IP Address (BLOCK IP)

To block an attackers ip address called 1.2.3.4, enter:
```
# iptables -A INPUT -s 1.2.3.4 -j DROP
# iptables -A INPUT -s 192.168.0.0/24 -j DROP
```

#10: Block Incoming Port Requests (BLOCK PORT)

To block all service requests on port 80, enter:
```
# iptables -A INPUT -p tcp --dport 80 -j DROP
# iptables -A INPUT -i eth1 -p tcp --dport 80 -j DROP
```

To block port 80 only for an ip address 1.2.3.4, enter:
```
# iptables -A INPUT -p tcp -s 1.2.3.4 --dport 80 -j DROP
# iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --dport 80 -j DROP
```

#11: Block Outgoing IP Address

To block outgoing traffic to a particular host or domain such as cyberciti.biz, enter:
```
# host -t a cyberciti.biz
```
Sample outputs:
```
cyberciti.biz has address 75.126.153.206
```

Note down its ip address and type the following to block all outgoing traffic to 75.126.153.206:
```
# iptables -A OUTPUT -d 75.126.153.206 -j DROP
```
You can use a subnet as follows:
```
# iptables -A OUTPUT -d 192.168.1.0/24 -j DROP
# iptables -A OUTPUT -o eth1 -d 192.168.1.0/24 -j DROP
```

#11.1: Example - Block Facebook.com Domain

First, find out all ip address of facebook.com, enter:
```
# host -t a www.facebook.com
```
Sample outputs:
```
www.facebook.com has address 69.171.228.40
```

Find CIDR for 69.171.228.40, enter:
```
# whois 69.171.228.40 | grep CIDR
```
Sample outputs:
```
CIDR:           69.171.224.0/19
```

To prevent outgoing access to www.facebook.com, enter:
```
# iptables -A OUTPUT -p tcp -d 69.171.224.0/19 -j DROP
```
You can also use domain name, enter:
```
# iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP
# iptables -A OUTPUT -p tcp -d facebook.com -j DROP
```

From the iptables man page:

> ... specifying any name to be resolved with a remote query such as DNS (e.g., facebook.com is a really bad idea), a network IP address (with /mask), or a plain IP address ...

#12: Log and Drop Packets

Type the following to log and block IP spoofing on public interface called eth1
```
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j LOG --log-prefix "IP_SPOOF A: "
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```
By default everything is logged to /var/log/messages file.
```
# tail -f /var/log/messages
# grep --color 'IP SPOOF' /var/log/messages
```

#13: Log and Drop Packets with Limited Number of Log Entries

The -m limit module can limit the number of log entries created per time. This is used to prevent flooding your log file. To log and drop spoofing per 5 minutes, in bursts of at most 7 entries .
```
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -m limit --limit 5/m --limit-burst 7 -j LOG --log-prefix "IP_SPOOF A: "
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

#14: Drop or Accept Traffic From Mac Address

Use the following syntax:
```
# iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP
## *only accept traffic for TCP port # 8080 from mac 00:0F:EA:91:04:07 * ##
# iptables -A INPUT -p tcp --destination-port 22 -m mac --mac-source 00:0F:EA:91:04:07 -j ACCEPT
```

#15: Block or Allow ICMP Ping Request

Type the following command to block ICMP ping requests:
```
# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
# iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j DROP
```
Ping responses can also be limited to certain networks or hosts:
```
# iptables -A INPUT -s 192.168.1.0/24 -p icmp --icmp-type echo-request -j ACCEPT
```
The following only accepts limited type of ICMP requests:
```
### ** assumed that default INPUT policy set to DROP ** ##############
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
iptables -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
## ** all our server to respond to pings ** ##
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

#16: Open Range of Ports

Use the following syntax to open a range of ports:
```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 7000:7010 -j ACCEPT
```

#17: Open Range of IP Addresses

Use the following syntax to open a range of IP address:
```
## only accept connection to tcp port 80 (Apache) if ip is between 192.168.1.100 and 192.168.1.200 ##
iptables -A INPUT -p tcp --destination-port 80 -m iprange --src-range 192.168.1.100-192.168.1.200 -j ACCEPT

## nat example ##
iptables -t nat -A POSTROUTING -j SNAT --to-source 192.168.1.20-192.168.1.25
```

#18: Established Connections and Restaring The Firewall

When you restart the iptables service it will drop established connections as it unload modules from the system under RHEL / Fedora / CentOS Linux. Edit, /etc/sysconfig /iptables-config and set IPTABLES_MODULES_UNLOAD as follows:
```
IPTABLES_MODULES_UNLOAD = no
```

#19: Help Iptables Flooding My Server Screen

Use the crit log level to send messages to a log file instead of console:
```
iptables -A INPUT -s 1.2.3.4 -p tcp --destination-port 80 -j LOG --log-level crit
```

#20: Block or Open Common Ports

The following shows syntax for opening and closing common TCP and UDP ports:

```
Replace ACCEPT with DROP to block port:
## open port ssh tcp port 22 ##
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 22 -j ACCEPT

## open cups (printing service) udp/tcp port 631 for LAN users ##
iptables -A INPUT -s 192.168.1.0/24 -p udp -m udp --dport 631 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -p tcp -m tcp --dport 631 -j ACCEPT

## allow time sync via NTP for lan users (open udp port 123) ##
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p udp --dport 123 -j ACCEPT

## open tcp port 25 (smtp) for all ##
iptables -A INPUT -m state --state NEW -p tcp --dport 25 -j ACCEPT

# open dns server ports for all ##
iptables -A INPUT -m state --state NEW -p udp --dport 53 -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 53 -j ACCEPT

## open http/https (Apache) server port to all ##
iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT

## open tcp port 110 (pop3) for all ##
iptables -A INPUT -m state --state NEW -p tcp --dport 110 -j ACCEPT

## open tcp port 143 (imap) for all ##
iptables -A INPUT -m state --state NEW -p tcp --dport 143 -j ACCEPT

## open access to Samba file server for lan users only ##
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 137 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 138 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 139 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 445 -j ACCEPT

## open access to proxy server for lan users only ##
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 3128 -j ACCEPT

## open access to mysql server for lan users only ##
iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
```

#21: Restrict the Number of Parallel Connections To a Server Per Client IP

You can use connlimit module to put such restrictions. To allow 3 ssh connections per client host, enter:

```
# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 3 -j REJECT
```

Set HTTP requests to 20:

```
# iptables -p tcp --syn --dport 80 -m connlimit --connlimit-above 20 --connlimit-mask 24 -j DROP
```

Where,

1. **--connlimit-above 3** : Match if the number of existing connections is above 3.
2. **--connlimit-mask 24** : Group hosts using the prefix length. For IPv4, this must be a number between (including) 0 and 32.

#22: HowTO: Use iptables Like a Pro

For more information about iptables, please see the manual page by typing man iptables from the command line:

```
$ man iptables
```

You can see the help using the following syntax too:

```
# iptables -h
```

To see help with specific commands and targets, enter:

```
# iptables -j DROP -h
```

#22.1: Testing Your Firewall

Find out if ports are open or not, enter:

```
# netstat -tulpn
```

Find out if tcp port 80 open or not, enter:

```
# netstat -tulpn | grep :80
```

If port 80 is not open, start the Apache, enter:

```
# service httpd start
```

Make sure iptables allowing access to the port 80:

```
# iptables -L INPUT -v -n | grep 80
```

Otherwise open port 80 using the iptables for all users:

```
# iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
# service iptables save
```

Use the telnet command to see if firewall allows to connect to port 80:

```
$ telnet www.cyberciti.biz 80
```

Sample outputs:

```
Trying 75.126.153.206...
Connected to www.cyberciti.biz.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

You can use nmap to probe your own server using the following syntax:

```
$ nmap -sS -p 80 www.cyberciti.biz
```

Sample outputs:

```
Starting Nmap 5.00 ( http://nmap.org ) at 2011-12-13 13:19 IST
Interesting ports on www.cyberciti.biz (75.126.153.206):
PORT   STATE SERVICE
```

```
80/tcp open  http
Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
```

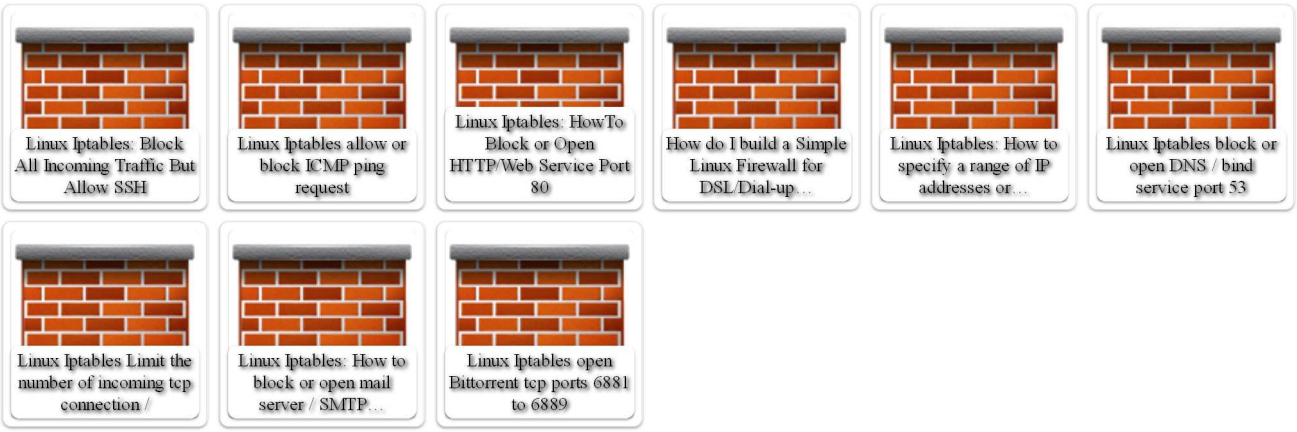
I also recommend you install and use sniffer such as tcpdupm and ngrep to test your firewall settings.

Conclusion:

This post only list basic rules for new Linux users. You can create and build more complex rules. This requires good understanding of TCP/IP, Linux kernel tuning via sysctl.conf, and good knowledge of your own setup. Stay tuned for next topics:

- Stateful packet inspection.
- Using connection tracking helpers.
- Network address translation.
- Layer 2 filtering.
- Firewall testing tools.
- Dealing with VPNs, DNS, Web, Proxy, and other protocols.

Related Posts:



Tagged as: /etc/sysconfig/iptables, /var/log/messages, Centos iptables rules examples, Debian iptables rules examples, enterprise linux, Fedora iptables rules examples, firewall iptables, iptables command, iptables rules example, iptables rules examples, kernel modules, linux distro, linux kernel, netfilter, RHEL iptables rules examples, Slackware iptables rules examples, Ubuntu iptables rules examples

{ 73 comments… add one }

- Happysysadm December 13, 2011, 10:10 am

  This is a nice breakdown of IPTABLES indeed! Thank you for taking the time for such a comprehensive explaination… I shall bookmark this!

  Reply Link
- logicos December 13, 2011, 11:56 am

  Try ferm, “for Easy Rule Making” .

  In file like “ferm.conf” :

  chain (INPUT OUTPUT FORWARD) policy DROP;
  chain INPUT proto tcp dport ssh ACCEPT;

  And next:
  ferm -i ferm.conf

  Source: http://ferm.foo-projects.org/

  Reply Link
- LeftMeAlone December 13, 2011, 1:58 pm

  Can any one tell me the difference between the DROP vs REJECT? Which one is recommended for my mail server?

  Reply Link
  - Worked December 13, 2011, 2:59 pm

    LeftMeAlone, “drop” does not send anything to the remote socket while “reject” sending the following message to the remote socket: (icmp destination port unrechable).

    Make clean… “drop” maybe the service does not exists. “reject” you can not access to the service.

    Reply Link
- Joeman1 December 13, 2011, 3:07 pm

  @LeftMeAlone

  DROP will silently drop a packet, not notifying the remote host of any problems, just won’t be available. This way, they will no know if the port is active and prohibited or just not used.

  REJECT will send an ICMP packet back to the remote host explaining (For the lack of better words) that the host is administratively denied.

  The former is preferred as a remote host will not be able to determine if the port is even up.

  The latter is not recommended unless software requires the ICMP message for what ever reason. Its not recommended because the remote host will know that the port is in use, but will not be able to connect to it. This way, they can still try to hack the port and get into the system,

Hope this helps!
Joe

Reply Link

- Prabal Mishra December 13, 2011, 3:36 pm

  thanks !

  help for Iptables……..

  Reply Link
- smilyface December 13, 2011, 4:11 pm

  Thankssss..

  Reply Link
- noone December 13, 2011, 7:28 pm

  how about you try
  host -t a http://www.facebook.com
  a few times, just to see how dns round-rbin works…

  Reply Link
- noone December 13, 2011, 7:37 pm

  also, you can try this

```
#!/bin/bash
# Clear any previous rules.
/sbin/iptables -F
# Default drop policy.
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT ACCEPT
# Allow anything over loopback and vpn.
/sbin/iptables -A INPUT -i lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
/sbin/iptables -A INPUT -i tun0 -j ACCEPT
/sbin/iptables -A OUTPUT -o tun0 -j ACCEPT
/sbin/iptables -A INPUT -p esp -j ACCEPT
/sbin/iptables -A OUTPUT -p esp -j ACCEPT
# Drop any tcp packet that does not start a connection with a syn flag.
/sbin/iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
# Drop any invalid packet that could not be identified.
/sbin/iptables -A INPUT -m state --state INVALID -j DROP
# Drop invalid packets.
/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags SYN,FIN SYN,FIN              -j DROP
/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST              -j DROP
/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,RST FIN,RST              -j DROP
/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags ACK,FIN FIN                  -j DROP
/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags ACK,URG URG                  -j DROP
# Reject broadcasts to 224.0.0.1
/sbin/iptables -A INPUT -s 224.0.0.0/4 -j DROP
/sbin/iptables -A INPUT -d 224.0.0.0/4 -j DROP
/sbin/iptables -A INPUT -s 240.0.0.0/5 -j DROP
# Blocked ports
/sbin/iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED,RELATED --dport 8010 -j DROP
# Allow TCP/UDP connections out. Keep state so conns out are allowed back in.
/sbin/iptables -A INPUT  -p tcp -m state --state ESTABLISHED     -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
/sbin/iptables -A INPUT  -p udp -m state --state ESTABLISHED     -j ACCEPT
/sbin/iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# Allow only ICMP echo requests (ping) in. Limit rate in. Uncomment if needed.
/sbin/iptables -A INPUT  -p icmp -m state --state NEW,ESTABLISHED --icmp-type echo-reply -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED --icmp-type echo-request -j ACCEPT
# or block ICMP allow only ping out
/sbin/iptables -A INPUT  -p icmp -m state --state NEW -j DROP
/sbin/iptables -A INPUT  -p icmp -m state --state ESTABLISHED -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# Allow ssh connections in.
#/sbin/iptables -A INPUT -p tcp -s 1.2.3.4 -m tcp --dport 22 -m state --state NEW,ESTABLISHED,RELATED -m limit --limit 2/m -j ACCEPT
# Drop everything that did not match above or drop and log it.
#/sbin/iptables -A INPUT   -j LOG --log-level 4 --log-prefix "IPTABLES_INPUT: "
/sbin/iptables -A INPUT   -j DROP
#/sbin/iptables -A FORWARD -j LOG --log-level 4 --log-prefix "IPTABLES_FORWARD: "
/sbin/iptables -A FORWARD -j DROP
#/sbin/iptables -A OUTPUT  -j LOG --log-level 4 --log-prefix "IPTABLES_OUTPUT: "
/sbin/iptables -A OUTPUT  -j ACCEPT
iptables-save > /dev/null 2>&1
```

  Reply Link
- Coolm@x December 13, 2011, 7:38 pm

  Nice examples, but missing one. Commonly searched rule is one for masquerade.

  Reply Link
- Roy December 13, 2011, 10:19 pm

  This is extremely useful, somekind of magic and quick recipe…
  (Of course now i can't send mail on my remote server (to strict rate limit …))

  Reply Link
- 3y3lop December 14, 2011, 3:00 am

  Nice examples & thanks.

  Reply Link
- Jani December 15, 2011, 9:00 am

  .. I'm anxiously awaiting similar translated to ip6tables. :-)

Reply Link

- Howard December 22, 2011, 3:24 am

  A most excellent presentation of iptables setup and use. Really Superior work. Thanks kindly.

  Reply Link
- Linus Gasser December 22, 2011, 7:32 pm

  Point 8:

  And for the private address ranges to block on public interfaces, you'll also want to block

  169.254/16 – zeroconf

  Reply Link
- Pieter December 23, 2011, 5:44 pm

  Nice post, thanks! In example #19 there is an error in the last line:

  ```
  ## open access to mysql server for lan users only ##
  iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
  ```

  Should probably be:

  ```
  ## open access to mysql server for lan users only ##
  iptables -I INPUT -p tcp -s 192.168.1.0/24 --dport 3306 -j ACCEPT
  ```

  Reply Link
  - shawn cao February 24, 2012, 4:33 am

    that is right.

    Reply Link
- Alejandro December 23, 2011, 11:15 pm

  Thanks for this post, I hope you don't mind if I translate this to spanish and post it on my blog, Mentioning the original source, of course.

  Regards

  Reply Link
- strangr December 24, 2011, 12:41 am

  Simple rules to share your connection to internet (interface IFNAME) with other hosts on your local LAN (NATTED_SUBNET).
  In other words how to do NAT and MASQEURADEing.

  ```
  IFNAME=ppp0
  NATTED_SUBNET=192.168.2.0/24

  # 1) load appropriate kernel module

  modprobe iptable_nat

  # 2) make sure IPv4 forwarding is enabled

  echo 1 > /proc/sys/net/ipv4/ip_forward

  # 3) the appropriate rules

  iptables -A POSTROUTING -t nat -o $IFNAME -s $NATTED_SUBNET -d 0/0 \
           -j MASQUERADE
  iptables -A FORWARD -t filter -o $IFNAME -s $NATTED_SUBNET -m state \
          --state NEW,ESTABLISHED,RELATED -j ACCEPT
  iptables -A FORWARD -t filter -i $IFNAME -d $NATTED_SUBNET -m state \
          --state ESTABLISHED,RELATED -j ACCEPT
  ```

  Reply Link
  - liRONux July 8, 2013, 12:50 pm

    THANKS for this.
    How about blocking a website while having those rules?

    Reply Link
- JD December 31, 2011, 2:27 am

  ## open access to mysql server for lan users only ##
  iptables -I INPUT -p tcp -s 192.168.1.0/24 –dport 3306 -j ACCEPT

  This should be like this:

  -s 192.168.1.0/24 -d 192.168.2.2 -i eth0 -p tcp -m state –state NEW -m tcp –dport 3306 -j ACCEPT

  a rule like this should go under RELATED,ESTABLISHED in the INPUT chain

  Reply Link
- JD December 31, 2011, 2:39 am

  For email servers, I have rate limiting rules in place for all service ports.

  In the INPUT chain I have the spam firewall ip(s), allowed via port 25.

  Then for the email ports, I impose a hit count of 10 in 60 seconds, smart phones, email clients do not poll every second. Anything more than this is dropped and they can continue on a rampage with no affect on the server(s). It took me a while to come up with the rate-limiting chains to work with the email server. Since the Watch Guard XCS devices needed to be exempt from the rules. They have rate-limits on incoming connections as well, a lot better than Barracuda.

  I always specify the source/destination interface, state then the port.

Reply Link

- MB January 3, 2012, 8:17 am

  How do i open the port 25 on a public ip (eg. 1.2.3.4) because it is close, I can only send email but can't receive email?
  But on my localhost it's open, when I test I able to send and receive only on 127.0.0.1. This is my rule

  iptables -A INPUT -p tcp -m tcp –dport 25 -j ACCEPT

  when i check netstat -tulpn | grep :25
  tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 2671/exim4
  tcp6 0 0 ::1:25 :::* LISTEN 2671/exim4

  Hope you can help me on this matter. I really confused on this one.

  Reply Link

- Badr Najah January 2, 2012, 6:55 pm

  Very useful.
  Thanks

  Reply Link

- dilip January 5, 2012, 7:36 am

  Wooooooooooowwwwww. thats coooool…
  very usefull link….

  Thanks yar….

  Reply Link

- nbasileu January 9, 2012, 10:19 am

  Rule #14

  ## *only accept traffic for TCP port # 8080 from mac 00:0F:EA:91:04:07 * ##
  # iptables -A INPUT -p tcp –destination-port 22 -m mac –mac-source 00:0F:EA:91:04:07 -j ACCEPT

  –destination-port 8080 not 22

  Anyway, this is a fu**** good website with fully nice articles.
  Very big thx dudes.

  Happy new year everyone.

  Reply Link

- Atul Modi March 11, 2012, 10:16 am

  Excellent Stuff Guys!!!

  Everyone is putting their part. Great to see this kind of community flourish further.

  I am thankful to the ppl who started this website.

  Reply Link

- Daniel Vieceli March 13, 2012, 2:38 pm

  Excellent thanks.

  Reply Link

- jm April 1, 2012, 3:48 am

  Good info and well written.Easy to understand for everyone… I will be back to learn more needed security rules.. Oh and yes I'm a human but I hate to say the definition of human is (MONSTER) don't believe me ? Look it up on the net ! Ha ha ha ha
  Thank you for this page….

  Reply Link

- rw1 April 5, 2012, 7:45 am

  thank you! for the information on how to delete a firewall rule! priceless! thanks!

  Reply Link

- Eli May 11, 2012, 12:19 am

  How can i use iptable rules to use multiple internet connections for the same bit torrent download?
  Actually, i have two broadband connections. I want to combine them. I am told to get load balancing hardware and i cant afford that. So, i did some experimenting.
  On first DSL modem, i set its IP to be 192.168.1.1
  On second modem, i set its IP to be 192.168.2.1
  Then in windows network adapter settings, i set Metric value of each adapter to 1. Thats about it. My bit torrent downloads/uploads use both my internet connections at the same time which gives effect of combined speed.
  Can i do something like that in Linux?
  Or, how can i combine two internet connections by using iptables? I dont want any hardware changes. All i have is two DSL modems and two network interface cards. Precise help would be greatly appreciated.

  Reply Link

- kolya May 13, 2012, 6:55 pm

  Hi, got a question to the author of the article. I have tried different kind of commands from the command line, edited the file /etc/sysconfig/iptables directly with following saving and restarting iptables/rebooting system. Nothing helps, my rules get overwritten by the system flushing my new rules or editing them. I tried to open ports (22,21 etc). The goal why I edit my firewall is to get connected to ftp server via FileZilla. Would you recommend me how to open ports? Tell me please if you need any system outputs or something. Cheers

  Reply Link

- nixCraft May 13, 2012, 8:35 pm

> *my rules get overwritten by the system flushing my new rules or editing them*

I think you got some sort of script or other firewall product running that is overwriting your rules. Check your cron job and you find the source for the same. If you need further assistance head over to the nixcraft Linux Support forum.

Reply Link

- kolya May 14, 2012, 12:21 pm

thanks for your respond, as I am not a specialist I didn't any changes to my crontab yet, anyway I checked it, also /cron.d and everything connected to cron in /var/spool/…. Nothing about iptables or something. What I noticed there are several iptables files in /etc/sysconfig/: iptables.old written by system-config-firewall, iptables generated by iptables-save with some changes what I didn't entered.
Here is what I entered from wiki.centos.org/HowTos/Network/IPTables:

iptables -P INPUT ACCEPT
iptables -F
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp –dport 22 -j ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
iptables -L -v

Here is what I got in the iptables's file:

:INPUT DROP [1:40]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [526:43673]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state –state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp –dport 22 -j ACCEPT
COMMIT
Don't know why it changes, probably it is aplying kind of default settings, but analyzing this settings the port 22 should be open. Nmap says it is closed, telnet outputs connection refused. Was trying to set samba server with the same result due to my firewall. What to do?

Reply Link

- Sigma May 25, 2012, 6:53 am

Thanks a lot for this article, which is extremely easy to understand and follow for beginners as me!

Reply Link

- dima June 9, 2012, 10:38 am

Hi
Regarding the block #7.1: Only Block Incoming Traffic
The rule
iptables -A INPUT -m state –state NEW,ESTABLISHED -j ACCEPT
looks dubious to me
Why would you want to allow NEW connections?
In my view it should read
iptables -A INPUT -m state –state RELATED,ESTABLISHED -j ACCEPT

Reply Link

  - qubits4all February 2, 2013, 8:08 am

    I noticed this as well. The rule as given is not right. I've been using iptables for a couple of years now, and the INPUT rule here should read:
    iptables -A INPUT -m state –state ESTABLISHED,RELATED
    (actually the above order is equivalent), because one clearly wouldn't want to match the NEW state here. Doing so would open up the door to TCP connects (i.e., TCP SYN packets) to any listening TCP services, as well as to UDP datagrams.

    Cheers to the author(s) of nixCraft for a nice article & a useful collection of iptables rules. This has become one of my favorite Linux/Unix blogs, so please keep the articles coming.

    Reply Link

- BiBi June 21, 2012, 3:24 am

Thank you very much, this site is very useful. I love all of you.

Reply Link

- Juan July 14, 2012, 1:53 pm

Hi.
Excellent tutorial. My desire is to block social networking in my job, I did it with squid in transparent mode but skipped to enter https. I did the tests on a virtual pc and it worked fine. The issue is that I is working on the production server. This has two network cards, eth0 traffic where it enters the Internet and eth1 to connect to the network. For the case of Facebook do the following:

We block Facebook
iptables-A OUTPUT-p tcp-d 69.63.176.0/20-dport 443-j DROP
iptables-A OUTPUT-p tcp-d 66.220.144.0/20-dport 443-j DROP
iptables-A OUTPUT-p tcp-d 69.171.224.0/19-dport 443-j DROP
iptables-A OUTPUT-p tcp-d http://www.facebook.com-dport 443-j DROP
iptables-A OUTPUT-p tcp-d facebook.com-dport 443-j DROP

Any suggestions?.

Greetings.

Reply Link

- jaydatt August 30, 2012, 10:47 am

really helpful article

Reply Link

- Borislav Bozhanov September 11, 2012, 11:13 pm

Hi,

Here is how to BLOCK FACEBOOK with single line command and iptables:

for i in $(nslookup facebook.com|grep Address|grep -v "#53″|awk '{print $2}'); do iptables -I FORWARD -m tcp -p tcp -d $i/24 –dport 443 -j DROP; done

You can replace the website with any other secure (https) you want.

For http websites (non-secure) – use the following line, replacing yahoo.com with the desired domain name:
for i in $(nslookup yahoo.com|grep Address|grep -v "#53″|awk '{print $2}'); do iptables -I FORWARD -m tcp -p tcp -d $i/24 –dport 80 -j DROP; done

Don't forget to save your iptables configuration.

Regards,
Borislav Bozhanov

Reply Link

- Łukasz Bodziony September 13, 2012, 7:37 pm

Thank you!!!

Reply Link

- Gus September 29, 2012, 6:51 pm

Hello.
I'm working with virtual machines. and would like to make a firewall and rootin bash.

My question is this
I have several public ip — IP1 = (200.45.xx.xxx) IP2 (=200.xx), IP3 = ·

The issue is that one of them use to Wan IP1.

Now I want to direct traffic from outside to inside. But I also want to redirect the traffic that comes to public ip 2 (IP2 to the local machine in lan (192.168.1.2) and what comes to public ip 3 (IP3) to the local machine (192.168.1.3)

I can not find examples of how to redirect traffic coming to a specific public IP to a particular LAN private IP.
If you can ask to help me.

```
#!/bin/sh
## SCRIPT de IPTABLES
## Pello Xabier Altadill Izura
echo -n Aplicando Reglas de Firewall...
## Paramos el ipchains y quitamos el modulo
/etc/rc.d/init.d/firewall stop
rmmod ipchains
## Instalando modulos
modprobe ip_tables
modprobe ip_nat_ftp
modprobe ip_conntrack_ftp
## Variables
IPTABLES=iptables
EXTIF="eth1"
INTIF="eth0"
## En este caso,
## la tarjeta eth1 es la que va al ROUTER y la eth0 la de la LAN
## Primeras reglas
/sbin/iptables -P INPUT DROP
/sbin/iptables -F INPUT
/sbin/iptables -P OUTPUT ACCEPT
/sbin/iptables -F OUTPUT
/sbin/iptables -P FORWARD ACCEPT
/sbin/iptables -F FORWARD
/sbin/iptables -t nat -F
### En principio, si las reglas INPUT por defecto hacen DROP, no haria falta
### meter mas reglas, pero si temporalmente se pasa a ACCEPT no esta de mas.
## Todo lo que viene de cierta IP se deja pasar (administradores remotos…)
/sbin/iptables -A INPUT -i $EXTIF -s 203.175.34.0/24 -d 0.0.0.0/0 -j ACCEPT
## El localhost se deja
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
## Aceptar al exterior al 80 y al 443
# Permitir salida al 80
/sbin/iptables -A INPUT -i $EXTIF -p tcp --sport 80 -j ACCEPT
/sbin/iptables -A OUTPUT -o $EXTIF -p tcp --dport 80 -j ACCEPT
# Permitir salida al 443
/sbin/iptables -A INPUT -i $EXTIF -p tcp --sport 443 -j ACCEPT
/sbin/iptables -A OUTPUT -o $EXTIF -p tcp --dport 443 -j ACCEPT
## SALIDA SMTP - Para que el servidor se pueda conectar a otros MTA
# Permitir salida SMTP
/sbin/iptables -A INPUT -i $EXTIF -p tcp --sport 25 -j ACCEPT
/sbin/iptables -A OUTPUT -o $EXTIF -p tcp --dport 25 -j ACCEPT
## SALIDA FTP - Para que el servidor se pueda conectar a FTPs
/sbin/iptables -A INPUT -i $EXTIF -p tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT
/sbin/iptables -A OUTPUT -o $EXTIF -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT
# ftp activo
/sbin/iptables -A INPUT -i $EXTIF -p tcp --sport 20 -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A OUTPUT -o $EXTIF -p tcp --dport 20 -m state --state ESTABLISHED -j ACCEPT
# ftp pasivo
/sbin/iptables -A INPUT -i $EXTIF -p tcp --sport 1024:65535 --dport 1024:65535 -m state --state ESTABLISHED -j ACCEPT
/sbin/iptables -A OUTPUT -o $EXTIF -p tcp --sport 1024:65535 --dport 1024:65535 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Reply Link

- Rogier October 23, 2012, 5:48 am

Hi, I have two interfaces: eth0 (for internal network) and eth1 (WAN). The server does the routing to the clients with the following IPtables:

```
# Generated by iptables-save v1.4.12 on Fri Oct 19 21:14:26 2012
```

```
*nat
:PREROUTING ACCEPT [14:1149]
:INPUT ACCEPT [6:625]
:OUTPUT ACCEPT [4:313]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -o eth1 -j MASQUERADE
COMMIT
# Completed on Fri Oct 19 21:14:26 2012
# Generated by iptables-save v1.4.12 on Fri Oct 19 21:14:26 2012
*filter
:INPUT ACCEPT [505:53082]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [247:29622]
-A FORWARD -s 192.168.1.0/24 -i eth0 -o eth1 -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Fri Oct 19 21:14:26 2012
```

This works fine, however I have no other rules set up. Can anyone help me in deciding what rules I need? the server (who does the NAT) is also running a webserver on port 80, SSH server on 22. All other ports can may be blocked.. how can I achieve this?

Reply Link

- Jorge Robles October 24, 2012, 2:37 pm

  I use fwbuilder to create my rules, this interface “looks like” checkpoint’s fw1 client to edit rules. Very graphical, and good to work with.

  Reply Link

- sahil November 8, 2012, 10:14 am

  very nice and informative article
  it really helped to work for my VPS server

  Reply Link

- bussy November 9, 2012, 8:09 pm

  how i do give access ip ex 192.168.0.2 only for facebook .

  Reply Link

  - Sayajin December 19, 2012, 7:27 am

    fb_address=$(dig facebook.com +tcp +short);
    iptables -A OUTPUT -p tcp -s !192.168.0.2/32 -d $fb_address -j DROP;

    Reply Link

- bahathir November 25, 2012, 3:17 am

  For tip #2, it is advisable to run the -P chain ACCEPt first, before flushing it.
  Exampes
  # iptables -P INPUT ACCEPT
  # iptables -P OUTPUT ACCEPT
  # iptables -P FORWARD ACCEPT
  # iptables -F
  # iptables -t nat -F
  # iptables -X
  #iptables -t nat -X

  Why? If the current chain’s policy is DROP, and you are remotely accessing to the server via SSH, and the rule “-A INPUT -p tcp –dport 22 -j ACCEPT” is still opens the “-P INPUT DROP”. you may disconnected as soon as you flush *-F* the rules, and the default policy “-P INPUT DROP” kicks in. :) If you are working on the local console, it is fine.

  Thank you.

  Reply Link

  - qubits4all February 2, 2013, 8:34 am

    This is a valid point. Another way to avoid locking oneself out, which I have found very useful for testing firewall changes over an SSH session, is the iptables-apply command (incl. with the Ubuntu iptables package for e.g.). It functions essentially the same as the iptables command, but when applying a rule change it prompts w/ a timeout for a confirmation after making the change. If no response is received (in 30 secs. by default), then it rolls back the change (i.e., add, modify, delete or otherwise).

    Once rules have been tested, I save them with iptables-save, and load the stable configuration with an init.d script at system startup (and including support for a ‘restart’ command here, for a clean flush, delete & reapply rules cycle).

    Reply Link

- levi November 27, 2012, 4:24 am

  Could it be you are using iptables save after directly editing? This will overwrite your work. Do a restart to load your newly edited table.

  Reply Link

- KeepEnEmUp December 8, 2012, 2:32 am

  Great Thx for awesome site and for awesome reading,tutos.
  Respect And KeepUp dude!

  Reply Link

- rashid Iqbal December 13, 2012, 11:43 am

  from graphical user and groups If I add or delete any user I can’t see any reference log nor in messages or in /var/log/secure file,

  Kindly please advise on this that from GUI if we run/execute any command where does the log message will go.

  Reply Link

- Gangadhar February 27, 2013, 2:50 pm

thank you very much for such a wonderful explanation….. very clear and had nice experience with iptables…

Reply Link

- haidt March 10, 2013, 9:04 am

  Hi there,

  i have a problem, i have got a server and LAN network, and this's feature

  internet (eth0) server (eth1) clients -> 10.0.0.2
  -> 10.0.0.3
  now, i can config to iptables accept all client connect internet, but in this situation, i want to allow only one client (assume: 10.0.0.3), i try but not completed. pls help me :)

  Thanks

  Reply Link

- Manish Narnaware April 24, 2013, 5:33 am

  Thanks a lot.

  Reply Link

- Orange April 25, 2013, 11:08 pm

  Thank you very much. Coincidentally, I just discovered an hour ago that I need to use iptables to allow a tablet computer to talk through my laptop, using the same internet connection. And then I discovered that I can't remember any of it. I was using IP tables and IP nat 15 years ago, back when it was Darrin Reed's project (name???), but that was too long ago for my memory. This article will get me back on track fast.
  Thanks again.

  Reply Link

- Le Vu May 29, 2013, 8:23 am

  Module xt_connlimit was disabled. How to limit number of connection per IP, can you module limit and recent. Please help me. :)

  Reply Link

- abedatwa June 13, 2013, 7:08 am

  thank you

  Reply Link

- abedatwa June 13, 2013, 7:09 am

  thank you for you ivitation

  Reply Link

- Mark August 1, 2013, 1:33 pm

  Thank you for this example. I don't remember the command line off the top of my head and this gives me enough information to do what I need to do without having to read 30 man pages. If only proper support (support.oracle.com) would be so efficient.

  Reply Link

- paul August 3, 2013, 1:29 am

  Enjoyed and appreciated the article and the comments particularly from noone (13 December 2011). I've added some of the suggestions to my firewalls.

  The first lines in every INPUT are always

  -A INPUT -s 123.123.123.123/32 -j ACCEPT
  -A INPUT -s 124.124.124.124/32 -j ACCEPT

  123 & 124 represent my external IPs including home and office backup connections.

  These entries ensure that whatever errors I make in IPTables I can never lock myself out of my remote servers.

  Best regards to all,

  Paul.

  Reply Link

- John August 21, 2013, 2:40 am

  In 7.1, the example provided does not block all incoming traffic like it claims. If you don't add more parameters, the rule will apply to both directions.

  The example rule:

  iptables -I INPUT -m state –state NEW,ESTABLISHED -j ACCEPT

  This would not only allow for NEW outgoing requests but also NEW incoming requests. The DROP policy for the INPUT chain can't do it's job to block incoming connections since it is applied after the rule which allows both NEW incoming and outgoing connections.

  Reply Link

- sophea October 30, 2013, 8:53 am

  I have problem when i add by manually (ex: #iptables -A INPUT -s 192.168.0.1 -p tcp –dport 53 -j ACCEP) but when i restart iptables by service iptables restart it not work because :

  1- when i view in /etc/sysconfig/iptables the IP address will be 192.168.0.1/32 but my land /24
  2- problem when i start or stop by system-config-firewall

  Can u help me pls?

  Reply Link

- Mohammad February 27, 2014, 3:38 pm

  Hi, I have a question. Could we log packets which are dropped because of forwarding queue is filled (e.g in congestion time)? How do I perform this work?
  Regards Mohammad.

  Reply Link
- juan-vargas May 26, 2014, 12:49 am

  Hi there. Greetings from Mexico. Nice examples. Very usefull all of them. But, can I bypass traffic in the port-80 once my iptables-policies are: -P INPUT DROP, -P OUTPUT DROP, -P FORWARD DROP?

  thank you all in advance.

  Reply Link
- Anumod August 4, 2014, 12:47 pm

  How to disable sending back TCP Reset to clients or how to increase TCP reset timeout in iptable.
  (I am using a raw socket as server and able to receive tcp client SYN request, but before sending SYNACK, tcp reset packet is going from server)

  Reply Link
- John August 9, 2014, 1:20 am

  Hi Guys,

  New to IP Tables, need a little advice – I have a guest wifi network setup, how do I block port 25 outgoing for an ip range?

  Thanks, John Tankard

  Reply Link
- Darko Vrsic October 15, 2014, 9:30 am

  Very nice!

  Thank you!

  Reply Link
- Bas October 15, 2014, 5:52 pm

  Nice breakdown on iptables!

  However, I prefer (& recommend) to use a firewall manager (command-line / config file based tool) like shorewall:

  http://shorewall.net/

  Reply Link
- Ron Barak December 1, 2014, 4:43 pm

  Useful page.
  Here'XXX errXXX I found
  #18: Established Connections and >>>Restaring<<< The Firewall

  Reply Link
- Ron Barak December 1, 2014, 4:44 pm

  Useful page.
  Here's errtum I found
  #18: Established Connections and >>>Restaring<<< The Firewall

  Reply Link
- Ramesh Das April 6, 2015, 7:32 pm

  iptables -p tcp –syn –dport 80 -m connlimit –connlimit-above 20 –connlimit-mask 24 -j DROP

  I tried above but its not taking through so if am not wrong then it should be as below.

  iptables -A INPUT -p tcp –syn –dport 80 -m connlimit –connlimit-above 20 –connlimit-mask 24 -j DROP

  Reply Link

Leave a Comment

Name *

Email *

Website

Comment

Submit

Next post: Linux / UNIX Desktop Fun: Let it Snow On Your Desktop

Previous post: Download CentOS 6.1 CD / DVD ISO

To search, type and hit e

Featured Articles:

- 30 Cool Open Source Software I Discovered in 2013
- 30 Handy Bash Shell Aliases For Linux / Unix / Mac OS X
- Top 30 Nmap Command Examples For Sys/Network Admins
- 25 PHP Security Best Practices For Sys Admins
- 20 Linux System Monitoring Tools Every SysAdmin Should Know
- 20 Linux Server Hardening Security Tips
- Linux: 20 Iptables Examples For New SysAdmins
- Top 20 OpenSSH Server Best Security Practices
- Top 20 Nginx WebServer Best Security Practices
- 20 Examples: Make Sure Unix / Linux Configuration Files Are Free From Syntax Errors
- 15 Greatest Open Source Terminal Applications Of 2012
- My 10 UNIX Command Line Mistakes
- Top 10 Open Source Web-Based Project Management Software
- Top 5 Email Client For Linux, Mac OS X, and Windows Users
- The Novice Guide To Buying A Linux Laptop

Linux/Unix Howtos & Tutorials

- How To Join Several Partition Together To Form a Single Larger One On a Linux Using mhddfs
- How To Find My Public IP Address From Command Line On a Linux
- Linux and Unix Test Disk I/O Performance With dd Command
- How To: Ubuntu Linux Firewall Open Port Command
- FreeBSD Add a User To Wheel Group Command
- How To Run Cronjob Script On The Last Day Of a Month
- How To: Temporarily Clear Bash Environment Variables on a Linux and Unix-like System
- Debian 8 and Ubuntu 14.04 LTS Install Suhosin PHP Extension To Protect Your Server
- How To Find the WiFi Password on Mac OS X
- How to update Debian or Ubuntu Linux containers (lxc) VM
- Bash: Find out the exit codes of all piped commands
- How To Find Out FreeBSD Version and Patch Level Number
- How To Setup a LAMP Server on Debian Linux 8 (Jessie)
- Linux/Unix: How To Extract and Decompress a .bz2/.tbz2 File
- Debian/Ubuntu Linux: Restrict an SSH user session to a specific directory by setting chrooted jail
- SSH ProxyCommand example: Going through one host to reach another server
- Linux exit from lxc-console keyboard shortcut
- How to run sudo command without a password on a Linux or Unix
- How To Patch and Protect Linux Server Against the VENOM Vulnerability # CVE-2015-3456
- How To CentOS / RHEL 7 Install Gnome Desktop Using Yum