## On this page



# Step-By-Step Configuration of NAT with iptables

This tutorial shows how to set up network-address-translation (NAT) on a Linux system with iptables rules so that the system can act as a gateway and provide internet access to multiple hosts on a local network using a single public IP address. This is achieved by rewriting the source and/or destination addresses of IP packets as they pass through the NAT system.

## Requirements:

CPU - PII or more
OS - Any Linux distribution
Software - Iptables
Network Interface Cards: 2

**Here is my considerations:**

Replace xx.xx.xx.xx with your WAN IP

Replace yy.yy.yy.yy with your LAN IP

(i.e. 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8 as suggested by Mr. tzs)

WAN = eth0 with public IP xx.xx.xx.xx
LAN = eth1 with private IP yy.yy.yy.yy/ 255.255.0.0

## Step by Step Procedure

**Step #1.** Add 2 Network cards to the Linux box

**Step #2.** Verify the Network cards, Wether they installed properly or not

```
ls /etc/sysconfig/network-scripts/ifcfg-eth* | wc -l
```

( The output should be "2")

**Step #3.** Configure eth0 for Internet with a Public ( IP External network or Internet)

```
cat /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=eth0
BOOTPROTO=none
BROADCAST=xx.xx.xx.255     # Optional Entry
HWADDR=00:50:BA:88:72:D4     # Optional Entry
IPADDR=xx.xx.xx.xx
NETMASK=255.255.255.0     # Provided by the ISP
NETWORK=xx.xx.xx.0        # Optional
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
IPV6INIT=no
PEERDNS=yes
GATEWAY=xx.xx.xx.1     # Provided by the ISP
```

**Step #4.** Configure eth1 for LAN with a Private IP (Internal private network)

```
cat /etc/sysconfig/network-scripts/ifcfg-eth1
```

```
BOOTPROTO=none
PEERDNS=yes
HWADDR=00:50:8B:CF:9C:05     # Optional
TYPE=Ethernet
IPV6INIT=no
DEVICE=eth1
NETMASK=255.255.0.0         # Specify based on your requirement
BROADCAST=""
IPADDR=192.168.2.1         # Gateway of the LAN
NETWORK=192.168.0.0         # Optional
```

```
USERCTL=no
ONBOOT=yes
```

**Step #5.** Host Configuration (Optional)

```
cat /etc/hosts
```

```
    127.0.0.1       nat localhost.localdomain   localhost
```

**Step #6.** Gateway Configuration

```
cat /etc/sysconfig/network
```

```
    NETWORKING=yes
    HOSTNAME=nat
    GATEWAY=xx.xx.xx.1    # Internet Gateway, provided by the
ISP
```

**Step #7.** DNS Configuration

```
cat /etc/resolv.conf
```

```
    nameserver 203.145.184.13      # Primary DNS Server
provided by the ISP
    nameserver 202.56.250.5        # Secondary DNS Server
provided by the ISP
```

**Step #8.** NAT configuration with IP Tables

# Delete and flush. Default table is "filter". Others like "nat" must be explicitly stated.

```
iptables --flush            # Flush all the rules in filter and nat tables
```

```
iptables --table nat --flush
```

```
iptables --delete-chain
```

# Delete all chains that are not in default filter and nat table

```
iptables --table nat --delete-chain
```

# Set up IP FORWARDing and Masquerading

```
iptables --table nat --append POSTROUTING --out-interface eth0 -j
MASQUERADE
```

```
iptables --append FORWARD --in-interface eth1 -j ACCEPT
```

# Enables packet forwarding by kernel

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

#Apply the configuration

```
service iptables restart
```

**Step #9.** Testing

# Ping the Gateway of the network from client system

```
ping 192.168.2.1
```

Try it on your client systems

```
ping google.com
```

## Configuring PCs on the network (Clients)

- All PC's on the private office network should set their "gateway" to be the local private network IP address of the Linux gateway computer.
- The DNS should be set to that of the ISP on the internet.

Windows '95, 2000, XP, Configuration:

- Select "Start" + Settings" + "Control Panel"
- Select the "Network" icon
- Select the tab "Configuration" and double click the component "TCP/IP" for the ethernet card. (NOT the TCP/IP -> Dial-Up Adapter)
- Select the tabs:

o "Gateway": Use the internal network IP address of the Linux box. (192.168.2.1)
o "DNS Configuration": Use the IP addresses of the ISP Domain Name Servers. (Actual internet IP address)
o "IP Address": The IP address (192.168.XXX.XXX - static) and netmask (typically 255.255.0.0 for a small local office network) of the PC can also be set here.

## 23 Comment(s)

### Add comment

Name * Email *

p

Submit comment

I'm not a robot reCAPTCHA Privacy - Terms

### Comments

**From:** Reply

1. The example is using 190.1.0.0/16 for private IP addresses. This is bad. That block is real live addresses, allocated to ISPs in Latin America and the Carribean. Private IP addresses should be choosen from one of the following blocks:
192.168.0.0/16
172.16.0.0/12
10.0.0.0/8
2. The example uses 190.1.7.1 as the address of the gateway on the LAN in step #4, but pings it at 190.1.6.1 in step #9.

**From:** mou5e Reply

Are you sure what are you talking about?
It is called NAT because the inside addresses are Translated into the outside address. For example my home inside NAT is 70.80.90.0/24.

**From:** Reply

(i.e. 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8 as suggested by Mr. tzs)
Unless you are doing some subnetting here, I would suggest keeping those internal addresses at their defaults which are:
192.168.1.0/24, ie mask 255.255.255.0 for a class c address.
172.16.0.0/16 mask 255.255.0.0 for class b
10.0.0.0/8 255.0.0.0 for class a

**From:** Anonymous Reply

Worst howto ever?

**From:** Sharib Reply

Hi All,
I tried and it is working fine till Step 7..
After that you can follow
http://www.howtoforge.com/internet-connection-sharing-masquerading-on-linux
The MASQUERADE steps explained over here works fine till the system is not restarted.
Best Regards,
Sharib Tasneem
SAP BASIS Consultant

**From:** sharms Reply

It should be noted that /etc/sysconfig exists on SuSE / Novell systems, if you are a Ubuntu server user this will not exist. The equivalent file is /etc/network/interfaces, but the syntax differs.

**From:** Tim Martin Reply

Step 8 is completely useless--don't try this at home kids...or at work for that matter.

"iptables --table nat --flush"
This will remove all chains from your current running netfilter table (firewall rules)...you just dropped your pants.

"iptables --delete-chain"
This will remove all chains from your current running nat table

"iptables --delete-chain"
No need to do this after a flush! There are no chains in your current running netfilter table because you already flushed it.

"iptables --table nat --delete-chain"
No need to do this after a flush! There are no chains in your current running nat table because you already flushed it.

"iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE"
This will enable nat in your current running nat table until we get down to the restart below.

"iptables --append FORWARD --in-interface eth1 -j ACCEPT"
This is useless because forwarding is accepted because you flushed your netfilter table

"echo 1 > /proc/sys/net/ipv4/ip_forward"
This will turn on routing. To bad next time you boot, it will not be enabled. Use sysctl!!!!

"service iptables restart"
I love this one. This command will un-do every "iptable" command above. Now NAT is no longer running. When the iptables service is restarted, it reads the saved config and anything was in "current running" is gone. Instead, use iptables-save!

Congratulations, you have a router with no NAT. But don't worry, it will no longer be a router after you reboot it. It will go back to the way it was before you started...thankfully

Tim Martin, RHCE

**From:** psperez Reply

I'd like to discuss some configuration instructions that I can't get working. You seem to have a handle on this tech.
Please email me, rather not post configs here on this site.

**From:** abhandari Reply

Please be clear before you post anything?

**From:** dAb Reply

Howto FAIL.

**From:** Anonymous Reply

Either you bought the 70.80.90.0/24 adress space or your inside NAT addressing is bad, because any connection attempt to 70.80.90.15 or similar in that network will never leave your home network, even though this may be real public adress used somewhere out there in the Internet. Always use private adresses inside the NATed network!

**From:** Anonymous Reply

Yeah I use 66.102.0.0/16... what could possible go wrong:P
#ping google.com

PING google.com (66.102.7.99)

I am sure that won't be a problem

**From:** Anonymous Reply

I would suggest 0.0.0.0/0

**From:** rishi Reply

http://reddragon-linux.blogspot.com/2011/05/linux-internet-gateway-server-setup.html

**From:** Anonymous Reply

buddy, you copied parts of this inept article and posted it on your blog???

**From:** IRFroggy Reply

Then linux users want to know why companies are still running Microsoft. This how to will make me run back.

**From:** Anonymous Reply

My server is loged in with root but msg showing no root folder/directory found. it is login with home .. why its hapen??? any one help me.. and how to masquerade to other internet user with that firewall..??? I m not a linux engineer but i have responsibilty to solve that.... please help me..

**From:** S.Babu Reply

Dear Sir, its working excellent thank you very much

**From:** Abid Reply

Complete steps at the following link http://www.ittechguru.net/?p=21

**From:** Praveen Reply

its not working for me i am tryed in DSL Linux server internet where shared from server to client but rules is not working what can i do ? how to block ? my client xp machine where bypassed ...:(

**From:** XenServer 6.2 Reply

Hi, I will give an relevant update for users that need it on XenServer 6.2 (newest at this time) so, I tried and tried and made it work :)

1. for eg. OVH gaves you server with one NIC (eth1) so this is first problem if you aren't

using your own server. The answer to this is creating new external network with VLAN (i used 1024) on ETH1 (NIC1) and give this new network an IP in your XenCenter (Networking), for me 10.20.30.1 / 24 - why not :)

2. go to console of the serwer and check your interfaces i have (I won't write all):

eth1 - external network (OVH - with my static IP) - will call it EXT1

xapi0 - external network for internal use (our 10.20.30.0/24 network) - will call it INT1

xenbr1 - network bridge for vSwitch - all networks

you can check all information via ifconfig command

3. system changes

a. Edit file */etc/sysctl.conf*

**nano /etc/sysctl.conf**

b. Uncomment the following line to enable packet forwarding for IPv4 and other stuff

```
net.ipv4.ip_forward = 1
net.ipv4.conf.default.proxy_arp = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.xenbr0.send_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
kernel.sysrq = 1
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
kernel.msgmnb = 65536
kernel.msgmax = 65536
kernel.shmmax = 4294967295
kernel.shmall = 268435456
vm.dirty_ratio = 5
kernel.printk = 4 4 1 4
```

4. creating NAT

$IPTABLES -t nat -A POSTROUTING -s $INT1/255.255.255.0 -j MASQUERADE

$IPTABLES -I RH-Firewall-1-INPUT -s $INT1/24 -j ACCEPT

PS. i made a bash script and added it to my starting scripts or you can use add it to /etc/sysconfig/iptables

5. testing

from my VM - ping google.com - OK

VM cofig:

IP - 10.20.30.50 (static)

gateway - 10.20.30.1

nameserver - 10.20.30.1

I could use command lokkit but in my case there is no MASQUERADE there, that ISP makes it hard as allways !!!

http://support.citrix.com/article/CTX123930

I hope it hepled someone more :)

**From:** tim Reply

nice. easy. works. thanks.

**From:** MR.Princess Reply

i can't configuration DNS y ?





**Tutorial Info**

Author: ganesh35
Tags: kernel, linux

**Share This Page**