Register   Login   **Contribute**   **Subscribe**   **RSS**

HowtoForge
LINUX TUTORIALS

Howtos   **Forums**   **Contribute**   **Subscribe**   **ISPConfig**   **FAQForge**   **News**

Options For This Howto

➡ Free Support
➡ Paid Support

Navigation

[+] Expand [-] Collapse

- Howtos
  - Linux
    - Android
    - CentOS
    - Debian
    - Fedora
    - Kernel
    - Mandriva
    - PCLinuxOS
    - SuSE
    - Ubuntu
  - Web Server
    - Apache
    - Cherokee
    - Lighttpd
    - nginx
  - Backup
  - Control Panels
    - ISPConfig
  - DNS
    - BIND
    - MyDNS
    - PowerDNS
    - djbdns
  - Desktop
  - Email
    - Anti-Spam/Virus
    - Postfix
  - FTP
  - High-Availability
  - Monitoring
  - MySQL
  - Programming
    - C/C++
    - PHP
  - Samba
  - Security
    - Anti-Spam/Virus
  - Storage
  - Virtualization
    - KVM
    - OpenVZ
    - VMware
    - VirtualBox
    - Xen
  - Other
  - FreeBSD

- ◻ Commercial
- ‣ Mini-Howtos
- ◻ Forums
- ‣ Contribute
- ◻ Subscription
- ◻ Login
- ◻ Site Map/RSS Feeds

User login

Username:

Password:

☐ Remember Me?

Log in

Create a new account
Request new password

Facebook

HowtoForg

Like   6,0

Who's online

There are currently 4 users
and 3307 guests online.

HowtoForge
Forums

SmartOS -node
howto

A proper way of
backing up your
email directory
...

Crons not
"in
Time" ...

Reset FTP Settings

Replace additional
PHP version

Postfix fake
emails

running from from
web site

Modsecurity Nxing
Ispconfig3 Debian7

IspConfig3 Nginx
Debian7 can be a

bug?

Postfix STARTTLS.

News

FLOSS Weekly 278: arkOS

Linux powers smart LED bulbs, crockpot, maker kit

How to check Internet speed from the command line on Linux

What The Intelligence Community Doesn't Get: Backdoor For 'The Good Guys' Is Always A Backdoor For The 'Bad Guys' As Well

Is the Steam Controller too bizarre for most gamers?

AMD RadeonSI Driver 2D Performance Is Getting Better

Firefox OS: The Return of Microsoft's Netscape Fears

Korora 20 Screenshot Tour

Zedge, for All Your Annoying Ringtones!

Violett, GhostControl Inc And More Linux Games New On Desura

more

Recent comments

LAMP support on Ubuntu
6 hours 4 min ago

Re: Hello Everyone.. sorry if
22 hours 20 min ago

NGiNX & PHP5
23 hours 2 min ago

Server replied: 554 5.7.1 <mobarak@xyz.com>: Relay
1 day 8 hours ago

Re: Re: Why not SSH?
2 days 2 hours ago

Error
2 days 5 hours ago

Doesn't Work
2 days 5 hours ago

tutorial
3 days 18 hours ago

Thanks for the post!. Helped
3 days 20 hours ago

Replace Windows
4 days 1 hour ago

Newsletter

Subscribe to

🇬🇧 **English** | 🇩🇪 Deutsch | Site Map/RSS Feeds | Advertise

Step-By-Step Configuration of NAT with iptables

Want to support HowtoForge? Become a subscriber!

g+1　7　　　　　**Like　Share** ‹ 34　　　　　**Tweet** ‹ 19

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

Step-By-Step Configuration of NAT with iptables | HowtoForge - Linux...

http://www.howtoforge.com/nat_iptables

```
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
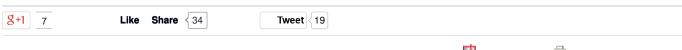
```
ping google.com
```

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.

Step-By-Step Configuration of NAT with iptables | HowtoForge - Linux...

http://www.howtoforge.com/nat_iptables

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.

g+1   7   Like   Share ‹34   Tweet ‹19

add comment | view as pdf | print: this | all page(s)

Related Tutorials

- Basic Iptables - Debian/RedHat

⚠️   *Please do not use the comment function to ask for help! If you need help, please use our forum. Comments will be published after administrator approval.*

NAT
Submitted by Abid (not registered) on Sun, 2012-09-02 03:53.

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

reply | view as pdf

IPTABLES NAT in fedora 13
Submitted by S.Babu (not registered) on Wed, 2012-04-11 05:34.

Dear Sir, its working excellent thank you very much

reply | view as pdf

No root directory found
Submitted by Anonymous (not registered) on Mon, 2011-11-14 09:23.

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..

reply | view as pdf

Howto fail.
Submitted by dAb (not registered) on Wed, 2010-05-12 14:30.

Howto FAIL.

reply | ⏷ view as pdf

Please be clear before you
Submitted by abhandari (not registered) on Tue, 2009-11-10 12:16.

Please be clear before you post anything?

reply | ⏷ view as pdf

Very Bad instructions
Submitted by Tim Martin (not registered) on Wed, 2009-03-18 05:23.

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

reply | ⏷ view as pdf

Re: Very Bad instructions - I agree
Submitted by psperez (not registered) on Sat, 2012-07-21 16:53.

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.

reply | ⏷ view as pdf

For the SuSE Distributions
Submitted by sharms (not registered) on Wed, 2009-02-04 21:03.

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.

reply | 🗋 view as pdf

Worst howto ever?

Submitted by Anonymous (not registered) on Thu, 2008-11-20 17:42.

Worst howto ever?

reply | 🗋 view as pdf

Re: Worst howto ever?

Submitted by Sharib (not registered) on Wed, 2010-11-10 07:43.

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

reply | 🗋 view as pdf

(i.e. 192.168.0.0/16,

Submitted by mynamewastaken (registered user) on Sun, 2007-02-04 03:52.

(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

reply | 🗋 view as pdf

IP addresses are seriously messed up in this

Submitted by tzs (registered user) on Fri, 2006-11-10 03:04.

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.

reply | 🗋 view as pdf

Re: IP addresses are seriously messed up in this
Submitted by mou5e (not registered) on Thu, 2010-12-02 10:07.

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.

reply | view as pdf

Re: Re: IP addresses are seriously messed up in this
Submitted by Anonymous (not registered) on Mon, 2010-12-20 00:40.

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!

reply | view as pdf

Re: Re: Re: IP addresses are seriously messed up in this
Submitted by Anonymous (not registered) on Sun, 2011-02-27 00:21.

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

reply | view as pdf

Re: Re: Re: Re: IP addresses are seriously messed up in this
Submitted by Anonymous (not registered) on Sun, 2011-03-06 15:02.

I would suggest 0.0.0.0/0 😃

reply | view as pdf

Linux as gateway
Submitted by rishi (not registered) on Tue, 2011-05-10 19:03.

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

reply | view as pdf

Re: Linux as gateway
Submitted by Anonymous (not registered) on Sun, 2011-09-04 00:19.

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

reply | view as pdf

Re: Re: Linux as gateway
Submitted by IRFroggy (not registered) on Wed, 2011-10-12 10:48.

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

reply | view as pdf