Using Ubuntu 12.04 as router/firewall

by nimmis
Categories: ubuntu
Tags: No Tags
Comments: 1 Comment
Published on: December 2, 2011

You need to have a server with 2 network cards, 1 for WAN RED (external internet access) and 1 for NAT GREEN (internal access)

The article describes the following.

- Use a computer with 2 network cards and ubunu to protect you maskines
- DHCP assignment for local computers
- local DNS zone to name your local machine
- iptables with port routing to local maskines

Setting upp 2nd interface as local network 192.168.0.0

before changing, make a backup
`sudo cp /etc/network/interfaces /etc/network/interfaces.bak`

adding net for 2nd interface eth1

add the following information to /etc/network/interfaces

```
# Set up the internal wired network
#
# Don't forget to change eth1 to the proper name of the internal
# wired network interface if applicable.
#
auto eth1
iface eth1 inet static
    address 192.168.0.1
    network 192.168.0.0
    netmask 255.255.255.0
    broadcast 192.168.0.255
```

restart network with

```
sudo /etc/init.d/networking restart
```

Setup dhcp server for local network

```
sudo apt-get install dhcp3-server
```

inte the file /etc/dhcp/dhcpd.conf insert the following

```
authoritative;
option domain-name "mydomain";
option domain-name-servers 8.8.8.8, 8.8.4.4, 192.168.0.1;

default-lease-time 600;
max-lease-time 7200;

option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;

subnet 192.168.0.0 netmask 255.255.255.0 {
        range 192.168.0.32 192.168.0.128 ;
        option routers 192.168.0.1 ;
}
```

then edit /etc/default/isc-dhcp-server

```
INTERFACES="eth1"
```

then restart dhcp server

```
sudo service isc-dhcp-server restart
```

Setting up the firewall

Be sure that ufw is installed on the system

```
sudo apt-get install ufw
```

edit the file /etc/default/ufw and change the line

```
DEFAULT_FORWARD_POLICY="DROP"
```

so it reads

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

then we need to enable packet forward between the interfaces

edit the file /etc/ufw/sysctl.conf and remove the # infront of the line below so it reads

```
net/ipv4/ip_forward=1
```

One final file to change before we are upp and running

change the file /etc/ufw/before.rules add these line in the top before any commands

```
# nat rules
*nat
 OSTROUTING ACCEPT [0:0]

# Forward all packes through eth0
-A POSTROUTING -s 192.168.100.0/24 -o eth0 -j MASQUERADE

# WARNING, do not remove COMMIT line. This breaks the loading
COMMIT
```

Before starting the firewall, if you want to be able to access it with ssh you need to enable a rule accepting connections on port 22

```
ufw allow 22
```

Then start it up

```
ufw disable && sudo ufw enable
```

1 Comment

1. *John Thinstad* says:

   May 5, 2013 at 3:27 pm

   ufw allow 22 is a bit low level.
   ufw all list – gives list of installed applicatins ufw knows

ufw app update OpenSSH – opens the firewall for SSH
ufw app info OpenSSH – shows the port added (yes.. 22/tcp)