Cubietruck: Como configurar servidor de cache com Squid

Nesse artigo você irá aprender a instalar e configurar servidor de cache com squid.

Material Utilizado: Cubietruck (Onde encontrar)

Utilizaremos o sistema operacional Fedora 20 imagem NAND para esse procedimento.

DOWNLOAD NAND
http://dl.cubieboard.org/software/a20-cubietruck/fedora/ct-fedora20-lxde/ (LXDE Desktop)
http://dl.cubieboard.org/software/a20-cubietruck/fedora/ct-fedora20-minimal/ (No Desktop)

Instalação:

1. **Download da imagem gzip**
2. **Descompactar a imagem**
3. **Flash a imagem para Cubietruck com livesuit/phoenixsuit**

Desabilitando Selinux:

 # This file controls the state of SELinux on the system.
 # SELINUX= can take one of these three values:
 # enforcing – SELinux security policy is enforced.
 # permissive – SELinux prints warnings instead of enforcing.
 # disabled – No SELinux policy is loaded.
SELINUX=disabled
 # SELINUXTYPE= can take one of these two values:
 # targeted – Targeted processes are protected,
 # minimum – Modification of targeted policy. Only selected processes are protected.
 # mls – Multi Level Security protection.
SELINUXTYPE=targeted

Desabilitando Firewall:
systemctl stop firewalld.service
systemctl disable firewall.service

#Criando firewall

touch /etc/init.d/firewall
chmod 755 /etc/rc.d/rc.local
vi firewall

#!/bin/sh
set -e

 # Definido variáveis
#redeinterna='192.168.0.254/24'

 # Definindo interface
#internet='eth0'
#redeinterna='eth1'

 # Política padrão

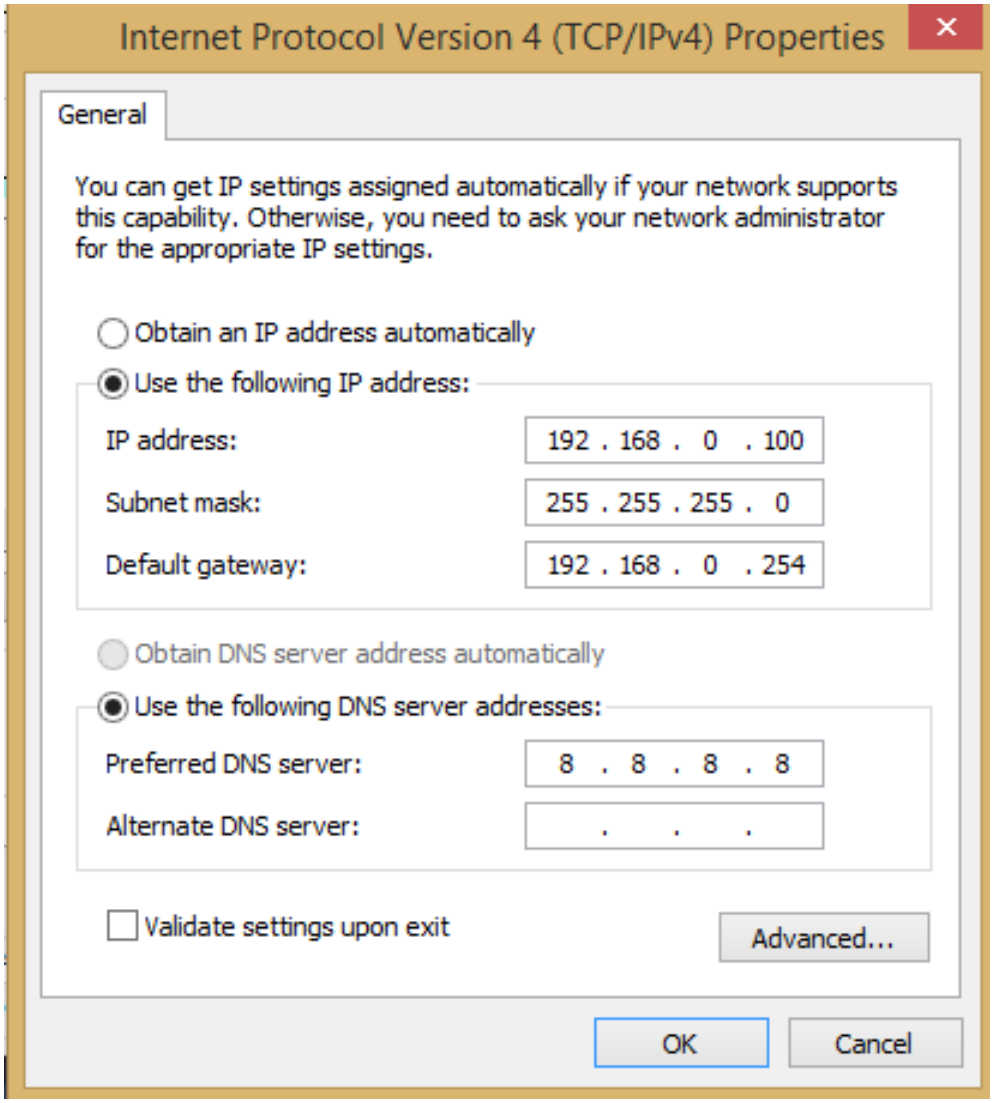
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

 # Limpando regras anteriores

iptables -t nat -F
iptables -t mangle -F
iptables -F
iptables -X

```
# Habilitando repasse entre as interfaces
echo 1 >/proc/sys/net/ipv4/ip_forward

# Proteção contra ICMP Broadcasting
echo “1” > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

# Proteções diversas contra portscanners, ping of death, ataques DoS, etc.
modprobe ip_nat_ftp
modprobe ip_conntrack_ftp

#Squid
iptables -t nat -A POSTROUTING -s 192.168.0.254/24 -o eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -i eth1 -p tcp –dport 80 -j REDIRECT –to-port 3128

touch /etc/rc.d/rc.local
chmod 755 /etc/rc.d/rc.local

vi rc.local

#!/usr/bin/bash
/etc/init.d/firewall

systemctl enable squid.services

yum -y install squid

cd /
mkdir cache
chmod 777 /cache

cd /etc/squid/
touch bloqueados
rm squid.conf
vi squid.conf

#Squid.conf
http_port 3128 transparent
visible_hostname cubietruck

cache_mem 128 MB
maximum_object_size_in_memory 128 KB
maximum_object_size 512 MB
minimum_object_size 0 KB
cache_swap_low 90
cache_swap_high 95
```

```
cache_dir ufs /cache 512 16 256
cache_access_log /var/log/squid/access.log
refresh_pattern ^ftp: 15 20% 2280
refresh_pattern ^gopher: 15 0% 2280
refresh_pattern . 15 20% 2280

acl all src all
#acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl Safe_ports port 901 # SWAT
acl purge method PURGE
acl CONNECT method CONNECT

http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

acl bloqueados dstdom_regex “/etc/squid/bloqueados”
http_access deny bloqueados

acl redelocal src 192.168.0.0/24
http_access allow localhost
http_access allow redelocal
http_access deny all

#Inicializando Squid
systemctl enable squid.service
systemctl start squid.service
```


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: . . .
Validate settings upon exit
Advanced...
OK
Cancel