

Servidor de Cache e Firewall com Squid, Dhcp-Server e Firewall na Cubieboard 2 com Cubian

Nesse artigo você aprenderá a instalar e configurar servidor de cache com [squid](#), dhcpd-server e firewall iptables.

Utilizaremos o sistema operacional Cubian para Cubieboard 2.

Material utilizado

Adaptador de rede USB 2.0



[Onde encontrar o adaptador de rede USB 2.0.](#)

Download da Imagem para SD:

<http://dl.cubieboard.org/software/a20-cubieboard/cubian/Cubian-base-r4-arm-a20.img.7z>

Instalação:

```
root@Cubian:~# sudo su
```

```
root@Cubian:~# apt-get install squid
```

```
root@Cubian:~# cd /etc/squid/
```

```
root@Cubian:~# mkdir cache
```

```
root@Cubian:~# chmod 777 cache
```

```
root@Cubian:~# mv squid.conf squid.conf.original
```

```
root@Cubian:~# touch bloqueados
```

```
root@Cubian:~# vim bloqueados
```

```
#Conteúdo bloqueado
```

```
google.com
```

```
google.com.br
```

```
playboy.com
```

```
playboy.com.br
```



```
root@Cubian:~# vim squid.conf
```

```
#Conteúdo do 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 /etc/squid/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
access_log /var/log/squid/access.log squid
```

```
root@Cubian:~# /etc/init.d/squid restart
```

#Configurando Firewall

```
root@Cubian:~# touch firewall
root@Cubian:~# chmod +x firewall
root@Cubian:~# vim firewall
```

#Conteúdo do Firewall

```
#!/bin/sh
set -e
```

Definindo 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
```

#Iniciando Firewall

```
root@Cubian:~# /etc/init.d/firewall
```

#Firewall na Inicialização

```
root@Cubian:~# vim /etc/rc.local
```

Insira a seguinte linha abaixo:

```
root@Cubian:~# /etc/init.d/firewall
```

#Configurando DHCP Server

Configurando interface Eth1 para o DHCPD

```
root@Cubian:~# vim /etc/network/interfaces
```

#Conteúdo das interfaces

```
auto eth1  
iface eth1 inet static  
address 192.168.0.254  
netmask 255.255.255.0
```

```
root@Cubian:~# apt-get install isc-dhcp-server
```

```
root@Cubian:~# cd /etc/default
```

```
root@Cubian:~# vim isc-dhcp-server
```

#Conteúdo do isc-dhcp-server

```
# Defaults for isc-dhcp-server initscript  
# sourced by /etc/init.d/isc-dhcp-server  
# installed at /etc/default/isc-dhcp-server by the maintainer scripts
```

```
#
```

```
# This is a POSIX shell fragment
```

```
#
```

```
# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
```

```
DHCPD_CONF=/etc/dhcp/dhcpd.conf
```

```
# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
```

```
DHCPD_PID=/var/run/dhcpd.pid
```



```
# Additional options to start dhcpd with.  
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead  
#OPTIONS=""  
  
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?  
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".  
INTERFACES="eth1"  
root@Cubian:~# cd /etc/dhcpd/  
  
root@Cubian:~# vim dhcpd.conf  
  
#Conteúdo do dhcpd.conf  
ddns-update-style none;  
default-lease-time 600;  
max-lease-time 7200;  
authoritative;  
  
subnet 192.168.0.0 netmask 255.255.255.0 {  
  range 192.168.0.100 192.168.0.199;  
  option routers 192.168.0.254;  
  option domain-name-servers 8.8.8.8,8.8.4;  
  option broadcast-address 192.168.0.255;  
}
```

Configuração dos clientes:

Windows

Em um cliente Windows, deverá ser ativada a opção "Obter automaticamente um endereço IP", nas propriedades TCP/IP da interface de rede. Em uma rede caseira, com acesso à Internet via modem ADSL ou cabo, esta opção deverá, a princípio, já estar ativada.

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

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:

Subnet mask:

Default gateway:

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel