

Squid 3

#Recomendo escrever tudo na mão, sem copiar e colar.

Instalação

wget <http://www.squid-cache.org/Versions/v3/3.5/squid-3.5.27.tar.gz>

```
tar -zxvf squid-3.5.27.tar.gz
```

```
./configure --prefix=/usr --sysconfdir=/etc/squid --localstatedir=/var --enable-auth --enable-auth-basic --enable-auth-basic --enable-auth-ntlm --enable-external-acl-helpers="wbinfo_group" --enable-icmp --enable-cache-digests --enable-poll --enable-esi --enable-kill-parent-hack --enable-follow-x-forwarded-for --enable-stacktraces --enable-truncate --enable-heap-replacement --disable-ident-lookups --with-logdir=/var/log/squid --with-pidfile=/var/run/squid/squid.pid --with-swapdir=/var/cache/squid --with-default-user=squid
```

```
make && make install
```

Ajustando permissões

```
chown -R squid. /var/log/squid
chown -R squid. /var/run/squid
chown -R squid. /var/cache/squid
chmod 750 /var/log/squid
chmod 750 /var/run/squid
chmod 750 /var/cache/squid
```

Configuração

Servidor Proxy/ Cache – Squid Basico

```
cd /etc/squid/
```

```
// Fazer uma copia Backup
```

```
cp squid.conf squid.conf.old
```

```
vim squid.conf
```

adicione as seguintes linhas responsavel por adicionar as redes conectadas

```
acl rede01 src 192.168.10.0/24
```

```
acl rede02 src 192.168.20.0/24
```

```
http_access allow rede01
```

```
http_access allow rede02
```

```
#Configurando o Cache
```

```
#descomente a line 68 ou pesquise no vim por /cache_dir ufs
```

```
# o numero 400 é quantidade de mg armazenado para o Proxy Cache, 16 a quantidade de  
pastas e 256 as subpastas
```

```
cache_dir ufs /usr/local/squid/var/cache/squid 400 16 256
```

```
#Adicionar linha para definir tamanho maximo do arquivo armazenado no Proxy
```

```
maximum_object_size 20496 KB # Tamanho maximo do arquivo
```

```
visible_hostname servidorSquid
```

```
#Criar a estrutura de cache
```

```
squid -z
```

Criando scrip para inicializacao /etc/init.d/squid

```
#!/bin/bash
```

```
#  
  
# squid    Bring up/down  
  
#  
# config:   /etc/squid/squid.conf  
  
#  
# chkconfig: - 90 20  
  
# description: Activates/Deactivates all squid services configured to \  
#              start at boot time.  
  
#  
### BEGIN INIT INFO  
# Provides: squid  
# Required-Start: $network $syslog  
# Required-Stop: $network $syslog  
# Short-Description: start and stop squid daemon  
# Description: proxy squid cache  
### END INIT INFO  
  
USER_SQUID='squid'  
PIDDIR='/var/run/squid'  
PIDFILE=${PIDDIR}/squid.pid  
  
if [[ ! -d ${PIDDIR} ]]; then
```

```
mkdir ${PIDDIR}

chown -R ${USER_SQUID}. ${PIDDIR}

chmod 750 ${PIDDIR}

fi

squid_pid() {

    echo $(ps aux | grep '(squid-1)' | grep -v grep | awk '{ print $2 }')

}

start() {

    ulimit -n 32768

    echo -n "Starting Squid: "

    [[ -n $(squid_pid) ]] && { echo "Squid is already running. PID: $(squid_pid)"; return 1 ; }

    su - $USER_SQUID -s /bin/bash -c 'squid'

    [[ -n $(squid_pid) ]] && { echo "Squid is started. PID: $(squid_pid)"; return 0 ; }

}

stop() {

    echo -n "Stopping Squid: "

    [[ -z $(squid_pid) ]] && { echo "Squid is not running."; return 0 ; }

    su - $USER_SQUID -s /bin/bash -c 'squid -k shutdown'

    echo -n "Wait shutdown"

    until [[ -z $(squid_pid) ]]; do

        echo -n "."; sleep 2

    done

}
```

```
done

echo " Squid is down"; return 0;

}

check(){

    echo -n "Checking configuration: "

    su - $USER_SQUID -s /bin/bash -c 'squid -k check'

    [[ $? -eq 0 ]] && { echo "OK"; return 0 ; } || return 1

}

squidReload(){

    echo "Reload Squid configurations: "

    check && su - $USER_SQUID -s /bin/bash -c 'squid -k reconfigure'

}

squidKill(){

    [[ -z $(squid_pid) ]] && { echo "Squid is not running."; return 1 ; }

    echo "Kill Squid PID: $(squid_pid)"

    kill -9 $(squid_pid)

    rm -r ${PIDFILE}

    [[ -z $(squid_pid) ]] && { echo "Squid died."; return 0 ; }

}

case "$1" in
```

```
start)  start;;

stop)   stop;;

restart) $0 stop && $0 start;;

check)  check;;

reload)  squidReload;;

kill)   squidKill;;

*)      echo "Usage: [start|stop|restart|check|reload|kill]";;

esac
```

Adicionando Squid na inicialização do SO

```
cd /etc/init.d/

chmod +x squid

chkconfig squid on
```

Criar Log Rotate /etc/logrotate.d/squid

```
/var/log/squid/*.log {

    daily

    rotate 31

    compress

    notifempty

    missingok

    nocreate

    sharedscripts

    postrotate

        /sbin/squid -k rotate 2>/dev/null
```

```
    sleep 1  
endscript  
}
```

iniciar squid

/etc/init.d/squid start

#Regras de Iptables

Ativando o Encaminhamento (ip_forward)

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

Rotas e Mascaramento de Pacotes

iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

Proxy Transparent

vim /etc/squid/squid.conf

#line 63

http_port 3128 intercept

#Reload Squid

/etc/init.d/squid reload

#Squid não pode ficar interceptando dados de conexões https.

iptables -A FORWARD -s 192.168.20.0/24 -p tcp --dport 443 -j ACCEPT

iptables -A FORWARD -s 192.168.10.0/24 -p tcp --dport 443 -j ACCEPT

Tudo que vira da rede 192.168.20.0/24 e 192.168.10.0/24 na porta 80 vai ser redirecionado para o porta do "SQUID" 3128

iptables -t nat -A PREROUTING -s 192.168.20.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3128

iptables -t nat -A PREROUTING -s 192.168.10.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3128

#Controle de Acessos para site

mkdir /etc/squid/regras

#Dentro desta pasta, posso criar arquivo que ira conter minha lista de negacao e aceitacao de sites.

#Meu arquivo de sites bloqueados

vim /etc/squid/regras/sites_bloqueados.txt

#Voce pode adicionar qualquer nome que quiser bloquear neste arquivo

#Torna a regra valida no squid.conf

vim /etc/squid/squid.conf

line 55 adicione a linha

acl bloqueados url_regex -i "/etc/squid/regras/sites_bloqueados.txt"


```
#Agora aplicar em qual rede a regra
vim /etc/squid/squid.conf
# Na linha 58 incremente
http_access allow rede01 !bloqueados
```

```
# Na linha 59 incremente
http_access allow rede02 !bloqueados
```

```
#Reload Squid
/etc/init.d/squid reload
```

```
#Tambem pode bloquear por dominios
```

```
vim /etc/squid/regras/dominio
```

```
#Adicionar a linha
acl dominios dstdomain -i "/etc/squid/regras/dominios"
```

```
# Na linha 58 incremente para adicionar bloqueio por dominios
http_access allow rede01 !bloqueados !dominios
```

```
# Na linha 59 incremente
http_access allow rede02 !bloqueados !dominios
```

```
Criar Script de Firewall
vim /etc/init.d/firewall.sh
```

```
#!/bin/bash          #Indicar qual o shell vem abaixo
```

```
case "$1" in
```

start)

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

```
iptables -A FORWARD -s 192.168.10.0/24 -p tcp --dport 443 -j ACCEPT
```

```
iptables -A FORWARD -s 192.168.20.0/24 -p tcp --dport 443 -j ACCEPT
```

```
iptables -t nat -A PREROUTING -s 192.168.10.0/24 -p tcp --dport 80 -j REDIRECT -  
-to-port 3128
```

```
iptables -t nat -A PREROUTING -s 192.168.10.0/24 -p udp --dport 80 -j REDIRECT  
--to-port 3128
```

```
iptables -t nat -A PREROUTING -s 192.168.20.0/24 -p tcp --dport 80 -j REDIRECT -  
-to-port 3128
```

```
iptables -t nat -A PREROUTING -s 192.168.20.0/24 -p udp --dport 80 -j REDIRECT  
--to-port 3128
```

```
iptables -t nat -A POSTROUTING -o enp0s3
```

```
-j MASQUERADE
```

```
iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT
```

::

stop)

```
iptables -F
```

```
iptables -X
```

```
iptables -t nat -F
```

```
iptables -t nat -X
```

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

```
iptables -t nat -A POSTROUTING -o eth0 -j
```

MASQUERADE

::

*)

```
echo "Parametro Invalido"
```

::

esac

```
#Dar permissao para o arquivo  
chmod +x /etc/init.d/firewall.sh
```

```
#Iniciar o firewall
```

```
/etc/init.d/firewall.sh start
```

```
#Configurando a quantidade de download que sera aceita
```

```
vim /etc/squid/squid.conf  
#Adicione a seguinte linha  
reply_body_max_size 10 MB rede01  
reply_body_max_size 5 MB rede02
```

Parei em 00:18:00.

Referencias Bibliograficas

<<http://www.crop11.com.br/wiki/instalando-proxy-squid-no-centos-7/>> Acessado em 29 de Out. 2017