**Configurações do Squid**

Posted in: 30/4/2012  
Updated : 02/04/2017

**Verificar se há erros no arquivo de configurações**

$ squid -k parse

**Apagar o cache de arquivos do squid**

$ sudo service squid stop

$ sudo su

# cd /var/spool/squid

# rm –f –R \*

# squid -z

$ squid start

$ squid –z

**Resetar o arquivo de log**

# echo >/var/log/squid/access.log

**Arquivo de log em Real Time**

$ sudo tail –f /var/log/squid3/access.log

**Verificar tamanho do cache**

$ sudo du -hs /var/spool/squid3

**Bloqueando sites e adicionando exceções no Squid**  
  
1º O bloqueio de domínios deve ser adicionado entre o penúltimo e último parágrafo de configuração

Exemplo:

http\_access allow manager localhost

http\_access deny manager

http\_access purge localhost

http\_access deny purge

http\_access deny Safe\_ports

http\_access deny CONNECT SSL\_ports  
  
**acl bloqueados url\_regex -i "/etc/squid/bloqueados"  
http\_access deny bloqueados**

acl redelocal src 192.168.10.0/24

http\_access allow localhost

http\_access allow redelocal

http\_access deny all

O arquivo de texto que contém os domínios que devem ser bloqueados estão localizados em /etc/squid/bloqueados  
Devemos criar uma política de acesso (acl) com um alias (bloqueados) depois a permissão HTTP\_acces allow (or deny) bloqueados.

Também há a possibilidade de usar **dstdomain** para bloquear domínios porém não é possível apontar para um arquivo txt ao contrário do **url\_regex**

**Exceções por MAC ou IP**  
  
1º) Criar uma **acl** do tipo **arp** e especificar o endereço MAC depois a permissão de execução ou não   
  
**acl macs arp “/etc/squid/macs”**

**http\_access allow macs**

2º) Devem ser implantadas acima das acls que bloqueiam

Exemplo:

http\_access allow manager localhost

http\_access deny manager

http\_access purge localhost

http\_access deny purge

http\_access deny Safe\_ports

http\_access deny CONNECT SSL\_ports

**acl macsallow arp 38:59:f9:09:f5:af**

**http\_access allow macsallow**  
**acl bloqueados url\_regex -i "/etc/squid/bloqueados"  
http\_access deny bloqueados**

acl redelocal src 192.168.10.0/24

http\_access allow localhost

http\_access allow redelocal

http\_access deny all  
  
Dica: Para muitos endereços MAC recomenda-se adicionar a uma arquivo de texto por exemplo em /etc/squid/macallow contudo a configuração da acl seria:

acl macsallow arp "/etc/squid/macsallow"  
http\_access allow macsallow

**Por IP**   
  
ao invés de **arp** usaríamos **src**  
  
acl ipsallow src "/etc/squid/ipsallow"

http\_access allow ipsallow  
  
Onde o arquivo que contém os IPs permitidos esta em /etc/squid/ipsallow

**Bloquear por IP**

acl ips src “/etc/squid/ips”  
http\_access deny ips

**Por palavras**

acl palavras **dstdom\_regex** “/etc/squid/palavras”  
http\_access deny palavras  
  
OBS: Caso o squid bloquei falsos positivos por exemplo a palavra copeve está bloqueada porém o cliente quer acessar a página copeve.cefetmg.br o squid irá bloquear faça uma exceção antes da acl que bloqueia as palavras.

**Redirecionar sites bloqueados**

acl barrar url\_regex [www.facebook.com](http://www.facebook.com/)

http\_access deny barrar

deny\_info [http://www.wikipedia.org](http://www.wikipedia.org/) barrar

**Verificar erros**  
$ squid -k parse

**Alguns tipos de ACLs**

dstdom\_regex - palavras

dstdomain ou url\_regex - domínios

arp - mac

src – ip

**Exemplo de arquivo de configuração**

http\_port 3128

visible\_hostname ubuntu

cache\_mem 64 MB

maximum\_object\_size\_in\_memory 64 KB

maximum\_object\_size 500 MB

minimum\_object\_size 0 KB

cache\_swap\_low 60

cache\_swap\_high 90

cache\_dir ufs /var/spool/squid 2048 16 256

cache\_access\_log /var/log/squid/access.log

refresh\_pattern ^ftp: 10 20% 2280

refresh\_pattern ^gopher: 10 0% 2280

refresh\_pattern . 10 20% 2280

acl all src 0.0.0.0/0.0.0.0

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 21 22 80 443 568 1025-65335

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 redelocal src 192.168.0.0/24

http\_access allow localhost

http\_access allow redelocal

http\_access deny all

**Controle de banda no squid**

Converter velocidade para bytes, exemplo:  
  
600 KB/8 = 75kbps \* 1024 = 76800 bytes  
  
Agora é só fazer a distribuição por exemplo distribuir metade de 600Kbs = 38400 bytes

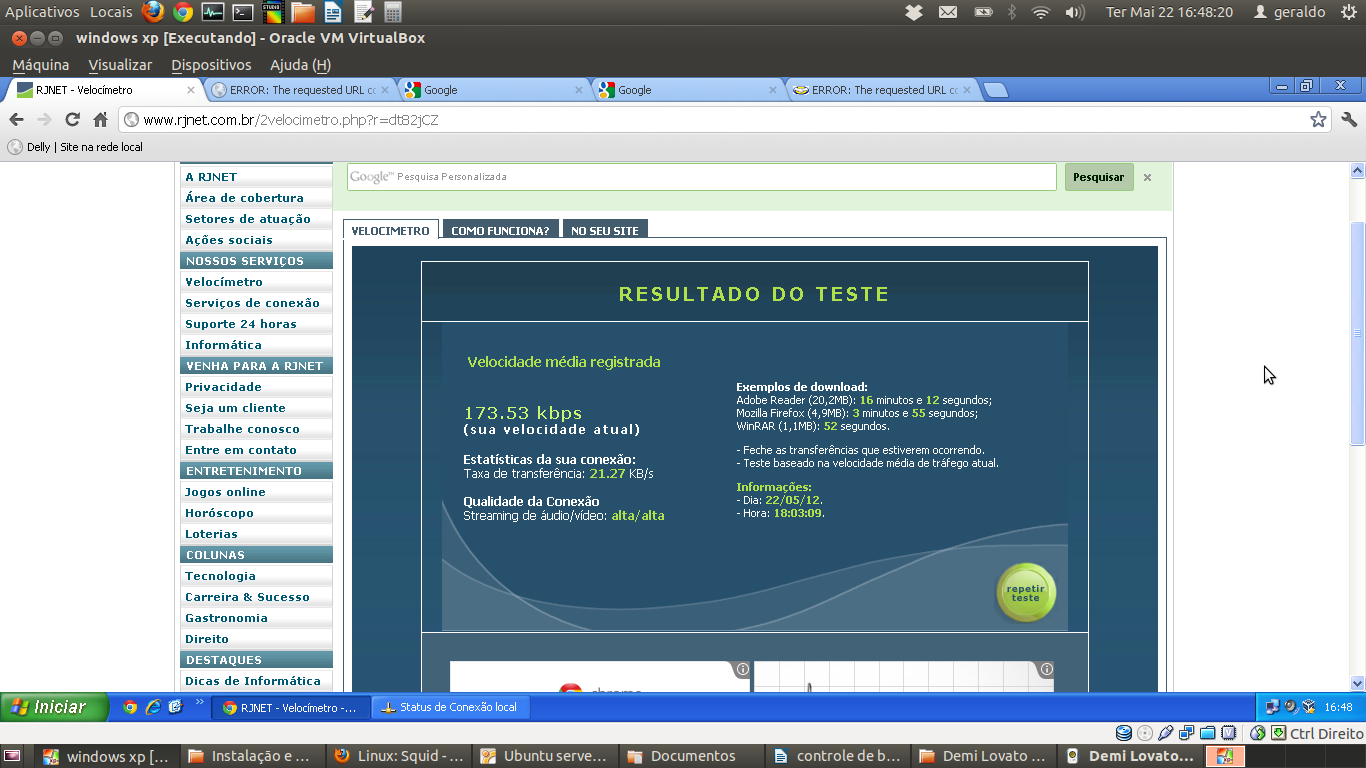
adicionar as regras no último paragrafo de configuração entre a primeira a o segunda linha

acl redelocal src 172.16.0.0/16

**delay\_pools 1  
delay\_class 1 2  
delay\_parameters 1 38400/38400 19200/19200  
delay\_access allow 1 redelocal**

http\_access allow localhost  
http\_access allow redelocal  
http\_access deny all

38400/38400 19200/19200 – referente a banda que o squid pode utilizar e por último a banda na qual irá fazer a distribuição entre os clientes.  
  
Lembre-se de utilizar o comando $ squid ou squid -k parse para verificar se há erros no arquivos de configuração.



Configuração mais avançada, exceção via MAC

acl redelocal src 172.16.0.0/16

acl macs arp "/etc/squid/macs"

delay\_pools 2

delay\_class 1 2

delay\_class 2 2

delay\_parameters 1 -1/-1 -1/-1

delay\_parameters 2 38400/38400 19200/19200

delay\_access 1 allow macs

delay\_access 2 allow redelocal

http\_access allow localhost

http\_access allow redelocal

http\_access deny all

-1/-1 – Sem limites