

Controle de Internet com Squid

Passo 1 - Entrar como Root

apt-get install squid

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@henrique-linux:/# apt-get install squid
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os pacotes extra a seguir serão instalados:
  squid-common squid-langpack
Pacotes sugeridos:
  squidclient squid-cgi logcheck-database resolvconf winbind
Os NOVOS pacotes a seguir serão instalados:
  squid squid-common squid-langpack
0 pacotes atualizados, 3 pacotes novos instalados, 0 a serem removidos e 388 não
atualizados.
É preciso baixar 1.343kB de arquivos.
Depois desta operação, 8.372kB adicionais de espaço em disco serão usados.
Você quer continuar [S/n]?
```

Passo 2 - Entrar na pasta /etc/squid

Nessa pasta contem o arquivo squid.conf, que é o arquivo de configuração, mas ele vem todo comentado. Iremos renomear esse arquivo e criar um novo.

```
# mv squid.conf squid.conf-original
```

```
# nano squid.conf
```

Passo 3 - Começar a criar os blocos de configurações e parametrizações.

Primeiro bloco será o de autenticação, onde será tratado das funções de autenticação.

##Autenticação##

```
auth_param basic program /usr/lib/squid3/pam_auth
```

auth_param → parâmetro de autenticação

basic → autenticação básica

program → executável do squid que trata das autenticações, esse executável vem com squid

/usr/lib/squid3/pam_auth → caminho padrão que contem as contas do Linux

```
auth_param basic children 10
```

children 10 → Define quantos processos simultâneos podem ter no servidor. No caso foi parametrizado com 10 conexões simultâneas.

```
auth_param basic realm Autentique-se para acessar a Internet
```

realm → Tela de autenticação para o usuário

auth_param basic credentialsttl 4 hours

credentialsttl → Tempo de vida de autenticação enquanto o browser estiver aberta

auth_param basic casesensitive off

casesensitive off → desligar o case sensitive, aceitar qualquer coisa entre maiúscula e minúscula

Controle de Acesso (ACL)

Bloco de controle de acessos

acl all src all

Define tudo no universo acl

acl localhost src 127.0.0.1/32

ACL Padrões.

Meus Controles de Acesso###

Minhas regras.

acl usuarios proxy_auth REQUIRED

ACL para autenticação de nome usuários.

REQUIRED → obriga a um usuário digitar uma autenticação

acl negados url_regex sexy playboy sexo xxx ultrasurf

Não quer que passe pelo proxy. Coloca as palavras negadas

acl liberados url_regex libsexy computador sexoesaude

Exceções no proxy

acl downloads urlpath_regex \.avi\$ \.rmvb\$ \.mp3\$ \.avi? \.rmvb? \.mp3?

Capturar nomes de arquivos na URL

HTTP_ACCESS

Controle de acessos com as ACLs que foram criadas.

Iremos informar o que deve acontecer com as ACLs e devemos colocar em ordem

http_access allow liberados

http_access deny negados

http_access deny downloads

http_access allow usuarios

###

http_access allow localhost

http_access deny all

Nega tudo para o todo tipo de ip.

Configurações gerais

http_port 3128

Define a porta de saída

cache_mem 256 MB

Quanto de memória RAM a ser utilizado para o proxy

maximum_object_size_in_memory 4 MB

Tamanho máximo por arquivo de objeto individual na memória RAM.

cache_dir ufs /var/spool/squid3 3000 16 256

ufs → tipo de arquivo unix

/var/spool/squid3 → local

3000 16 256 → Tamanho em Megabyte do cache, 16 subdiretórios, e 256 subdiretórios

access_log /var/log/squid3/access.log squid

Log de acesso do Proxy

cache_mgr email@email.com

visible_hostname kelton-linux

nome da máquina

error_directory /usr/share/squid3/errors/pt-br

Páginas com as mensagens de erro do squid

SALVE O ARQUIVO

Passo 4 - Reinicie o serviço com alguns dos comando abaixo

/etc/init.d/squid3 restart ou **service squid3 restart**

Passo 5 - Log do squid

Local que está o log de acesso, **tail -f /var/log/squid3/access.log**

Passo 6 - Criação de um usuário

useradd -s /bin/false -d /dev/null usuarioteste

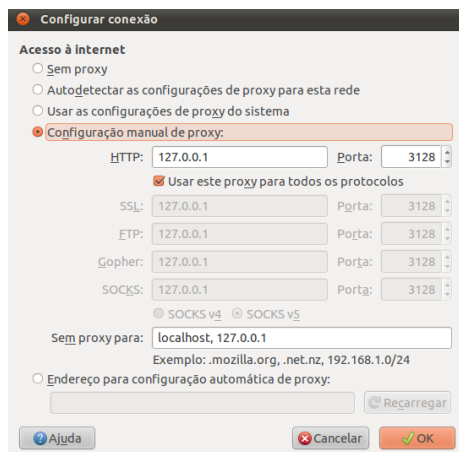
-s /bin/false → não irá logar no Linux, somente testar o squid

-d /dev/null → Não cria diretório home

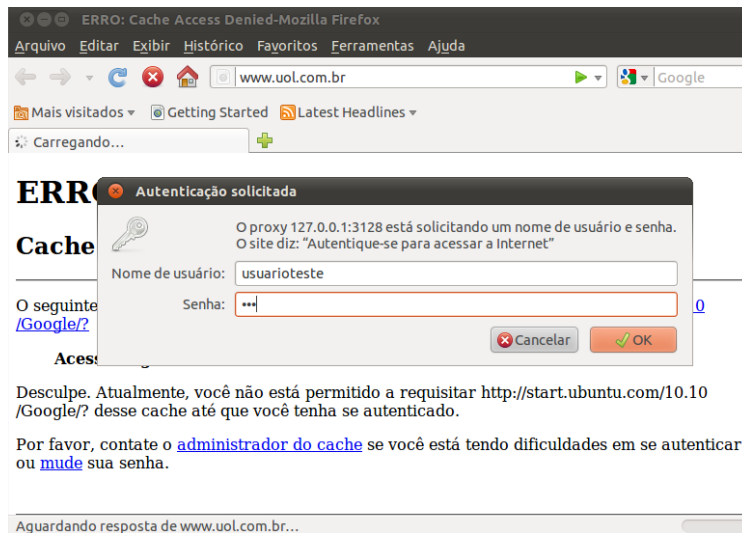
passwd usuarioteste

Passo 7 - TESTAR O PROXY

Entrar no navegador e colocar o endereço do servidor e a porta



Em seguida irá aparecer a tela de login, isso significa que funcionou o proxy.



sudo chmod u+s /usr/lib/squid3/pam_auth (para autorizar os usuários)

Passo 8 - Para verificar o log do squid:

Esse comando irá mostrar o log do proxy.

`tail -f /var/log/squid3/access.log`

Alternativa de verificação de log:

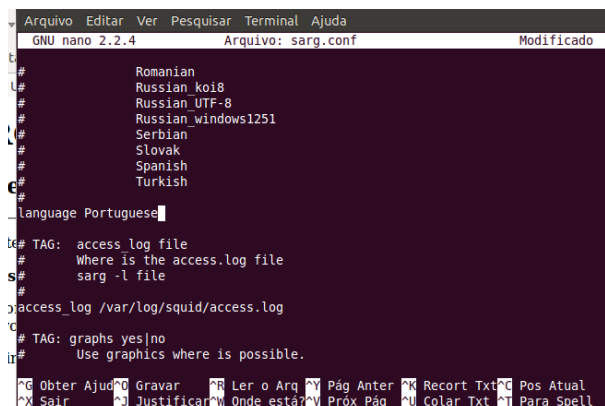
Para verificar o log através de um software de monitoramento, recomenda-se a utilização do aplicativo SARG

`apt-get install sarg`

Entrar no arquivo de configuração do SARG

`/etc/sarg`

`nano sarg.conf`



Trocar a linguagem para desejada

Se atentar ao access_log verificar se é o mesmo caminho do seu squid normalmente o caminho é squid3

E deve ser alterado o diretório WEB de saída dos log.

Linha 144

output_dir /var/www/sarg

colocar /var/www/sarg, que será o diretório padrão. Se não tiver esse diretório deverá ser criado:

Salvar o arquivo e criar o diretório.

mkdir -p /var/www/sarg

Passo 9 - Em seguida instalar o servidor WEB caso não tenha sido instalado

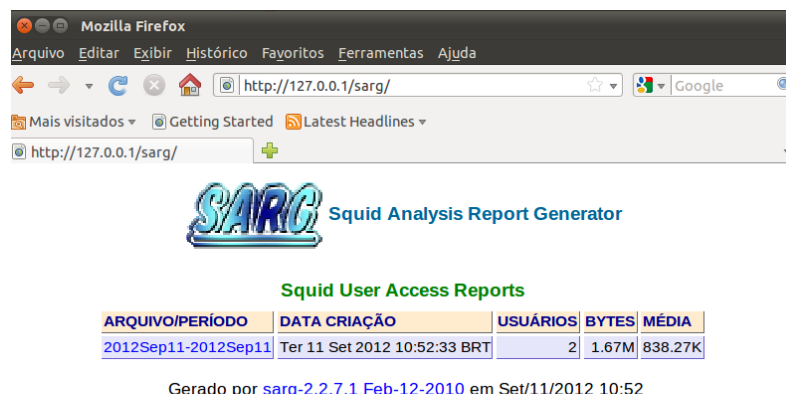
apt-get install apache2

Entrar no diretório do SARG e verificar se tem algum arquivo

ls /var/www/sarg → não deve ter nada, pois não rodou nada ainda.

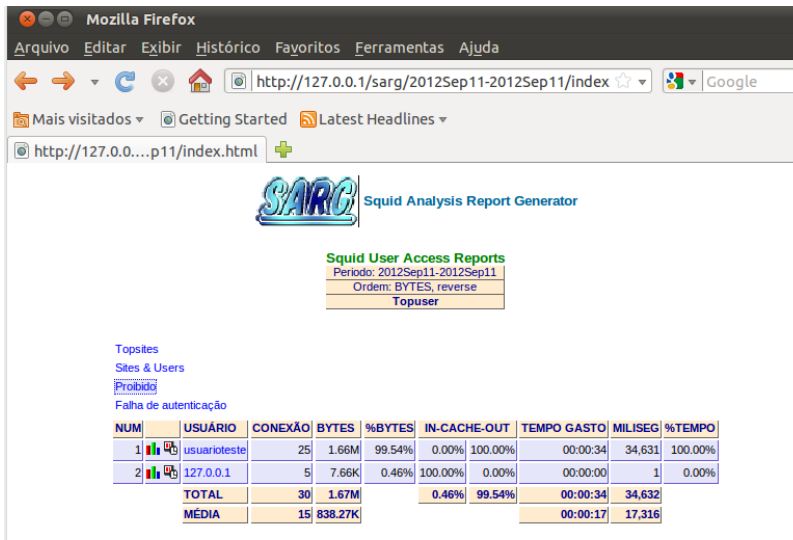
Digitar sarg para roda o programa

Em seguida no browser digitar 127.0.0.1/sarg



ARQUIVO/PERIODO	DATA CRIAÇÃO	USUÁRIOS	BYTES	MÉDIA
2012Sep11-2012Sep11	Ter 11 Set 2012 10:52:33 BRT	2	1.67M	838.27K

Gerado por [sarg-2.2.7.1 Feb-12-2010](#) em Set/11/2012 10:52



##Autenticação##

```
auth_param basic program /usr/lib/squid3/pam_auth
auth_param basic children 10
auth_param basic realm Autentique-se para acessar a Internet
auth_param basic credentialsttl 4 hours
auth_param basic casesensitive off
```

Controle de Acesso (ACL)

```
#acl all src all
#acl localhost src 127.0.0.1/32
```

Meus Controles de Acesso###

```
#acl usuarios proxy_auth REQUIRED
#acl negados url_regex sexy playboy sexo xxx ultrasurf
#acl liberados url_regex libsexy computador sexoesaude
#acl downloads urlpath_regex \.avi$ \.rmvb$ \.mp3$ \.avi? \.rmvb? \.mp3?
```

HTTP_ACCESS

```
#http_access allow liberados
#http_access deny negados
#http_access deny downloads
#http_access allow usuarios
###
#http_access allow localhost
#http_access deny all
http_access allow all
```

Configurações gerais

```
http_port 3128
cache_mem 256 MB
maximum_object_size_in_memory 4 MB
cache_dir ufs /var/spool/squid3 3000 16 256
access_log /var/log/squid3/access.log squid
cache_mgr email@email.com
visible_hostname Kelton-linux
error_directory /usr/share/squid3/errors/pt-br
```