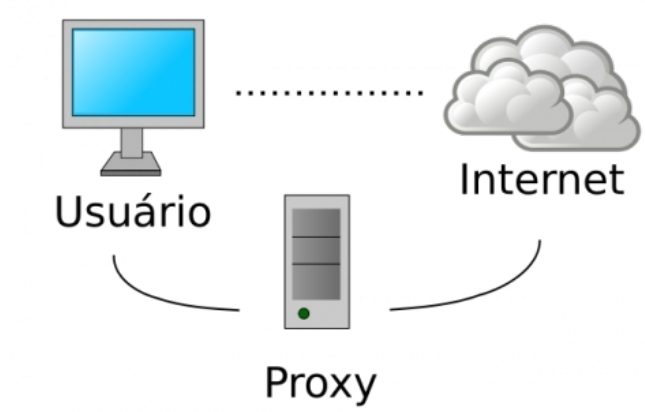
# Índice

# Definição de *Proxy*

O Proxy é um serviço de rede através do qual é possível estabelecer um alto nível de controle/filtro de tráfego/conteúdo e armazenamento em cache de navegação. Através de serviço, os administradores de rede podem contar com varias possibilidades, aumentando sua capacidade de adminsitração da rede, bem como aumentando a dinamica das regras e politicas implantadas nas organizações.

O Proxy atua como um intermediário entre o usuário e servidores de conteúdo, seja ele local ou remoto. Através dele, o administrador pode decidir, entre outras coisas, como, quando e o quê cada usuário o grupo de usuários pode acessar, bem como estabelecer regras baseadas em hardwares, protocolos, serviços e conteúdo.

Simplificando um pouco, o usuário deixa de ter contato direto com a internet e passa a contar com o Servidor Proxy para esse fim.




Muitas são as vantagens desse tipo de abordagem, entre elas: segurança – pois restringe o acesso externo à servidores internos; cache – mantém cópia dos conteúdos estáticos das páginas *web* diminuindo a carga em servidores *web*; compressão – comprime o conteúdo a ser transferido ao navegador do cliente; balanceamento de carga – distribui a carga entre dois ou mais servidores.

Neste tutorial, utilizaremos o Software Livre Squid-Cache para mostrar o que se pode fazer com um Servidor Proxy. É importante ressaltar que existem várias opções de softwares para isso, tanto proprietários como Softwares Livres, e que a opção pelo Squid é estritamente técnica e conceitual, e não envolve ideais mercadológicas.

# Utilizando o Software Squid

O Squid é uma ferramenta de *proxy* amplamente utilizada, possuindo as funcionalidades citadas no tópico anterior, atuando tanto como um *proxy* tradicional, quanto como um *proxy* reverso.

Sua instalação e configuração é relativamente simples, embora haja grande quantidade de parâmetros que podem ser ajustados em seu arquivo de configuração.

Assim como nos demais serviços que você já instalou até aqui, iremos configurar alguns dos parâmetros. Lembrando que para colocar o serviço em produção é recomendado analisar mais detalhadamente todos os parâmetros.

Os principais parâmetros são:

- **http_port** – Porta a ser utilizada pelo servidor;
- **icp_port** – Porta utilizada entre *proxies*;
- **cache_mem** – Quantidade de memória RAM utilizada pelo *proxy web*;
- **cache_dir** – Define os parâmetros de armazenamento do cache, tais como espaço em MB, diretórios de 1º e 2º nível;
- **access_log** – Local de armazenamento dos arquivos de log do acesso *web*;
- **cache_log** – Arquivo de log;
- **acl** – ACL (*Access Control List*), ou lista de controle de acesso, define o que poderá ou não ser acessado; e
- **http_access** – Regra de processamento da ACL.

# ACL - Access Control List

As listas de controle de acesso, denominadas de ACL (*Access Control List*) são regras de acesso utilizadas pelo *proxy*. Nelas podem ser definidos os critérios para controle que podem considerar parâmetros diversos tais como origem e destino, horário ou expressões regulares.

Para a implementação de uma política de acesso será necessária uma combinação de regras. No Squid as regras são analisadas da primeira até a última. Assim um acesso pode ser liberado assim que encontre uma regra na qual se encaixe. Por padrão é recomendada a inclusão de uma regra de negativa geral ao final de todas as ACL.

Ao criar as regras procure ser claro e objetivo, inclusive documentando-as através de comentários no próprio arquivo de configuração.

Uma ACL é composta de duas partes: uma diretiva especificando o tipo de controle e outra com a regra de acesso. O tipo de controle pode ser baseado no endereço de origem ou destino, no domínio de origem ou de destino. Já a regra de acesso especifica o tipo de controle, podendo ser por protocolo, porta, método de acesso ((GET) Método do protocolo HTTP utilizado para obter dados a partir de um recurso específico por meio de pares de objeto-valor em uma requisição HTTP. ou POSTMétodo do protocolo HTTP para manipulação de requisições na qual os dados estão inseridos na mensagem de solicitação.), tipo de navegador, horário, conteúdo MIME (*Multipurpose Internet Mail Extensions), que* é uma extensão de protocolo originalmente de e-mail, e depois adotada em servidores *web* na transmissão de diferentes tipos de dados, tais como áudio, vídeo, executáveis etc. e limite de conexões.

Assim uma regra que permita o acesso HTTP (*Hypertext Transfer Protocol)* protocolo para transferência de hipertexto utilizado em sistemas *web* aos dispositivos da rede 192.168.10.0/255.255.255.0, seria:

**acl rede src 192.168.10.0/255.255.255.0**

**http_access allow rede**

Enquanto que uma regra que bloqueie o acesso a arquivos MP3 seria:

**acl mp3 url_regex –i.*\.mp3$**

**http_access deny mp3**

# Tipos de ACL

**src:** Utilizada para especificar um determinado host ou rede de origem.

**Ex: acl rede_local src 192.168.1.0/255.255.255.0**

**dst**: Utilizada para especificar um determinado host ou rede de destino.

**Ex: acl rede_local dst 192.168.1.0/255.255.255.0**

**dstdomain**: Utilizado para especificar um determinado domínio de destino.

**Ex: acl hotmail dstdomain .hotmail.com**

**port**: Porta usada pelo site.acl rede_local

**Ex: acl Safe_ports port 80**

**url_regex:** Procura por expressão em toda a URL

**Ex: acl palavras_proibidas url_regex -i "/etc/squid/palavras_proibidas"**

**dstdomain_regex:** Procura por expressão no domínio.

**Ex: acl sites_proibidos dstdomain_regex -i "/etc/squid/sites_proibidos"**

**Time:** Hora e dia da semana. Especifica um determinado horário

**Ex: acl horario_comercial time MTWHF 08:00-18:00**

*OBS: Nesse tipo de ACL, “time”, usa-se letras indicando os dias da semana, conforme tabela abaixo:*

| | |
|---|---|
| S | domingo |
| M | segunda-feira |
| T | terça-feira |
| W | quarta-feira |
| H | quinta-feira |
| F | sexta-feira |
| A | sábado |

# Instalação do Servidor - Repositório

Instale o pacote relativo ao serviço Squid:

**# apt-get install squid3**

Verifique se o serviço Squid está em funcionamento:

**# service squid3 status**

# Instalação a Partir do Código-Fonte

Alternativamente, caso deseje instalar o Squid a partir do código fonte, execute os passos a seguir:

**# cd /tmp**

**# wget http://www.squid-cache.org/Versions/v3/3.5/squid-3.5.13.tar.gz**

**# tar –xzvf squid-3.5.13.tar.gz**

**# groupadd squid**

**# useradd –g squid –s /dev/null squid**

**# cd squid-3.5.13**

**# ./configure**

**# make**

**# make install**

Teste o funcionamento do serviço Squid:

**# service squid3 status**

# Configuração Básica

As configurações do serviço de *proxy* Squid estão localizadas no arquivo */etc/squid3.conf*.

O Squid possui numerosos recursos que podem ser ativados e ajustados por meio de seu arquivo de configuração. Contudo, ressalta-se que o símbolo cerquilha, **“#”**, quando utilizado no arquivo, indica que a linha não influenciará na configuração, pois se trata de linhas de balizamento, ou, comentários.

Vejamos a configuração do arquivo */etc/squid3/squid.conf*:

Edite o arquivo squid.conf utilizando o editor de sua preferência. Nesse exemplo utilizaremos o editor NANO, presente em a maioria dos Sistemas Operacionais Linux.

**# nano /etc/squid3/squid.conf**

**# Porta cliente**

http_port 3128

**# Porta proxies**

icp_port 3130

visible_hostname cache.rede.teste

**# Cache**

cache_mem 512 MB

cache_swap_low 75

cache_swap_high 97

maximum_object_size 900 MB

minimum_object_size 0 KB

maximum_object_size_in_memory 32 KB

**# Logs**

cache_dir ufs /var/spool/squid3 1024 64 256

cache_access_log /var/log/squid/access.log

cache_log /var/log/squid/cache.log

cache_store_log none

logfile_rotate 10

**# ACL**

acl all src all

acl manager proto cache_object

acl localhost src 127.0.0.1/32

acl to_localhost dst 127.0.0.0/8 0.0.0.0/32

acl SSL_ports port 443 563

acl Safe_ports port 80

acl Safe_ports port 21

acl Safe_ports port 443 563

acl Safe_ports port 70

acl Safe_ports port 210

acl Safe_ports port 1025-65535

acl Safe_ports port 280

acl Safe_ports port 488

acl Safe_ports port 591

acl Safe_ports port 777

acl CONNECT method manager

**# Cache manager**

http_access allow manager localhost

http_access deny manager

**# Acesso Defaults**

http_access deny !Safe_ports

http_access deny CONNECT !SSL_ports

**# Regras de acesso**

acl rede src 192.168.10.0/255.255.255.0

http_access allow rede

http_access deny all

Pause momentaneamente o servidor Squid para a criação do diretório onde será armazenado o *cache*:

# **service squid3 stop**

Crie diretórios de troca ausentes e outras estruturas cache_dir ausentes. O parametro “-z” faz a leitura no arquivo squid.conf e cria todos arquivos de cache citados, porém, ausentes no servidor.

**# mkdir /usr/local**

**# squid –z**

Verifique se foram criados os diretórios para cache em */var/spool/squid3*. Caso não tenham sido criados, verifique se a diretiva *cache_dir* foi corretamente digitada no arquivo de configuração.

# Implementando autenticação de usuários no Squid

O Squid permite implementar restrição de acesso por usuários logados, podendo interagir com diversos outros serviços/métodos de autenticação, como:

- LDAP - Lightweight Directory Access Protocol
- NCSA - Arquivo com usuário e senha no formato do NCSA
- MSNT - Domínio Windows NT
- PAM - Módulos PAM do Unix
- SMB - Servidor SMB (Windows ou Samba)

É importante frisar que o Squid não gerencia a autenticação de usuários quando ativo em modo transparente

## Criação de usuários com o aplicativo htpasswd

Crie o arquivo (vazio) que será usado para armazenar as senhas, usando o comando "touch".

# **touch /etc/squid/squid_passwd**

O próximo passo é cadastrar os logins usando o htpasswd, especificando o arquivo que acabou de criar e o login que será cadastrado, como em:

# **htpasswd /etc/squid/squid_passwd “usuário”**

## Configuração da autenticação no arquivo squid.conf

Para configurar a autenticação dos usuários, é necessário inserir alguns blocos de parâmetros, os quais serão utilizados na autenticação.

Está linha indica o nome do servidor, o qual aparecerá na tela de login
***auth_param basic realm Squid***

O "/usr/lib/squid/ncsa_auth" é a localização da biblioteca responsável pela autenticação;
O "/etc/squid/squid_passwd" indica a localização do arquivo de senhas que criamos
***auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd***

As linhas a seguir mostram a criação da ACL “autenticados” e o tratamento dado a ela.
**acl autenticados proxy_auth REQUIRED**
**http_access allow autenticados**

Caso a autenticação seja exigida para apenas alguns sites, pode-se utilizar a seguinte sintaxe.
**# acl usuarios proxy_auth REQUIRED /etc/squid3/sitios-autenticados**

# Configuração de Navegadores

Na sua rede, de modo geral, você pode bloquear no *firewall* o acesso de todos os computadores à internet, exceto os que o façam por meio do *proxy*.

Desse modo é necessário que os navegadores de todos os computadores de sua rede interna sejam configurados para acessar o *proxy*.

Acesse a VM2 (cliente) e configure o navegador para utilizar o *proxy* seguindo os passos indicados. No navegador Mozilla Firefox, a configuração dá-se por meio do menu “ferramentas” e “opções”. Selecionando o menu “geral” e clicando no botão “proxy”. Na janela “Servidores proxy”, marque “Usar servidores proxy” e “Utilizar o mesmo proxy em todos os protocolos”. Digite o IP e porta do *proxy*.

Abra o navegador da VM2 e acesse uma página na internet. Em seguida, avalie o conteúdo dos diretórios de cache.

# Configuração de Proxy Transparente

É possível que agora você esteja se perguntando: “Será que para utilizar *proxy* vou ter de configurar todos os navegadores de todos os computadores da rede?”

A resposta a essa indagação é: não necessariamente. Você pode preferir utilizar um *proxy* transparente. O qual não requer configurações nos computadores dos usuários, pois, como o nome já diz, é transparente para ele.

O *proxy* transparente elimina ainda outro problema, que é quando o usuário leva o computador para outra rede, por exemplo para casa. Chegando lá a configuração de *proxy* no navegador pode impedi-lo de acessar as páginas que deseja.

Como eu faço para criar um *proxy* transparente?

Será necessário incluir duas regras no *Iptables*. São elas:

**# iptables –I PREROUTING –t nat –p tcp –s 192.168.10.0/24 –dport 80 –j REDIRECT –to-port 3128**

**# iptables –t nat –I POSTROUTING –s 192.168.10.0/24 –j MASQUERADE**

Verifique a criação das regras com o comando:

**# iptables -L**

Após incluir essas duas regras, remova as configurações de *proxy* do navegador e teste novamente o acesso à internet.