Servidor Proxy

Prof. Dr. Márcio Andrey Teixeira
Instituto Federal de São Paulo – Campus Catanduva
Catanduva, SP
Membro Sênior do IEEE
marcio.andrey@ifsp.edu.br

Servidor Proxy

Instalação do squid

Para instalar o squid, execute o seguinte comando:

sudo apt-get install squid

O arquivo de configuração do squid está localizado em:
/etc/squid/squid.conf

Servidor Proxy

Controle de acesso - ACL

O squid controla o acesso as páginas da internet através das chamadas ACL (*Access Control List*)

As ACLs permitem especificar endereços de origem e destino, domínios, horários, portas ou métodos de conexão ao *proxy*, que serão utilizados para negar, permitir ou negar acessos.

Sintaxe de uma ACL:

acl [nome_da_acl] [tipo_da_acl] {argumentos}

Exemplos:

acl minharede src 192.168.10.1/24

httpd_access allow minharede

Servidor Proxy

Configuração Básica

Para que o squid funcione, as seguintes linhas devem ser inseridas/descomentada no do arquivo de configuração:

```
#Configuração por partes
#Parte I

# Squid normally listens to port 3128
http_port 3128

cache_mem 2000 MB

maximum_object_size_in_memory  8 MB
maximum_object_size 512 MB
minimum_object_size 0 KB

cache_dir ufs /var/spool/squid 10000 16 256
coredump_dir /var/spool/squid

cache_swap_low 90
cache_swap_high 93
```

```
#Rede Local
acl localnet src 192.168.10.0/24          #Rede LAN local

#Portas que utilizam o protocolo SSL
acl SSL_ports port 443

#Portas consideradas "seguras"
acl Safe_ports port 80                    # http
acl Safe_ports port 21                    # ftp
acl Safe_ports port 443                   # https
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
```

```
#Métodos que terão permissão
acl CONNECT method CONNECT
acl POST method POST
acl GET method GET

http_access allow POST
http_access allow GET
#---------------------

# Nega requisições para portas consideradas não seguras
http_access deny !Safe_ports

# Nega conexão para portas que utilizam o protocolo SSL e não são consideradas
seguras
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
```

```
#Permite conexão das redes previamente definidas
http_access allow localnet
http_access allow localhost

# Bloqueia o acesso para o restante.
http_access deny all
```

Uma vez tendo feito a configuração, é necessário criar a estrutura da cache. Para tanto, execute o comando:

squid -z

Obs: O comando acima é executado apenas quando for modificar a estrutura da cache.

Os comando utilizados para iniciar/reiniciar ou verificar o status do squid são: **sudo /etc/init.d/squid start | restart | status | stop**

Obs: A cada modificação existente no arquivo de configuração, o processo do squid deverá ser reiniciado.

Servidor Proxy

Bloqueando palavras por domínio

Uma forma fácil de bloquear sites no Squid é criar uma lista de palavras, um arquivo texto, onde você adiciona palavras e domínios que serão bloquados pelo squid.

Bloquear um determinado domínio, como por exemplo, “facebook.com”, não gera muitos problemas, mas deve-se tomar cuidado ao bloquear palavras específicas, pois o squid irá bloquear qualquer página que conter essa palavra em questão.

Se bloquear a palavra “sexo”, por exemplo, qualquer site ou artigo que conter a palavra sexo será bloqueado.

Ao bloquear por palavras, é necessário ser expecífico, bloqueando apenas “jargões” e expressões que normalmente se encontra no site que se quer bloquear.

Servidor Proxy

```
#
#Regras para bloqueios de sites
#
#############################################################################

acl bloqueados dstdom_regex -i "/etc/squid/Sites_bloqueados"
http_access deny bloqueados

#############################################################################
```

Servidor Proxy

Exemplos

```
acl bloqueados dstdomain www.globo.com
http_access deny bloqueados

acl proibidos dstdom_regex "/etc/squid/proibidos"
http_access deny proibidos
```

Servidor Proxy

Exemplos

acl palavras_bloqueadas url_regex -i "/etc/squid/palavras_bloqueadas.txt“

http_access deny palavras_bloqueadas

Servidor Proxy

Testando proibição de conteúdo:

1 - Dentro do diretório /etc/squid/ crie os seguintes arquivos:

Sites_bloqueados
Sites_liberados
Palavras_bloqueadas
Bloquear_downloads

Servidor Proxy

Testando proibição de conteúdo:

2 – Vamos utilizar as seguintes regras de acesso:

```
#Regras para bloqueios de sites
############################################################################
acl liberados dstdom_regex -i "/etc/squid/Sites_liberados"
http_access allow liberados

acl palavras url_regex -i "/etc/squid/Palavras_bloqueadas"
http_access deny palavras


acl bloqueados dstdom_regex -i "/etc/squid/Sites_bloqueados"
http_access deny bloqueados

acl block_downloads urlpath_regex -i "/etc/squid/Bloquear_downloads"
http_access deny block_downloads

############################################################################
```

Servidor Proxy

Testando proibição de conteúdo:

3 – Insira as palavras/domínios que se deseja bloquear/liberar e faça testes de acesso.

```
#Regras para bloqueios de sites
#############################################################################
acl liberados dstdom_regex -i "/etc/squid/Sites_liberados"
http_access allow liberados

acl palavras url_regex -i "/etc/squid/Palavras_bloqueadas"
http_access deny palavras


acl bloqueados dstdom_regex -i "/etc/squid/Sites_bloqueados"
http_access deny bloqueados

acl block_downloads urlpath_regex -i "/etc/squid/Bloquear_downloads"
http_access deny block_downloads

#############################################################################
```

Instalação do Sarg

Para instalar o SARG execute o seguinte comando:

sudo apt-get install sarg

Abra o arquivo de configuração em /etc/sarg/sarg.conf e configure as seguintes linhas:

Access_log //Local onde está o arquivo de log do squid

graph_font //Local onde está fonte utilizada para gerar o gráfico

output_dir //Local onde será publicado o arquivo html

Para gerar os relatórios, execute o comando: **sudo sarg –f /etc/sarg/sarg.conf**

Prof. Dr. Marcio Andrey Teixeira

marcio.andrey@ifsp.edu.br

http://marcioandrey.pro.br

Bibliografia

SILVA, G. M.. Segurança em sistemas Linux. 1. ed. Rio de Janeiro: Ciência Moderna, 2008. 240p.
THOMPSON, M. A.. Windows Server 2012: fundamentos. 1. ed. São Paulo: Érica, 2012. 232p.
VIANA, E. R. C.. Virtualização de servidores Linux para redes corporativas: guia prático. 1.
ed. Rio de Janeiro: Ciência Moderna, 2008. 342p.
6 - BIBLIOGRAFIA COMPLEMENTAR:
KUROSE, J. F.; ROSS, K. W.. Computer networking: a top-down approach. 6. ed. AddisonWesley, 2012. 864p.
SCHRODER, C.. Redes Linux: livro de receitas. 1. ed. Rio de Janeiro: Alta Books, 2006. 569p.