Squid Proxy

Departamento de Engenharia Informática
Instituto Politécnico de Leiria

Leonel Santos, Miguel Frade - 2014

Squid Proxy

- É um web *proxy* com ou sem *web cache.*
- Analisa o tráfego até à camada de aplicação.
- Permite filtrar os acessos web com base em várias regras.
- Permite autenticação de utilizadores.
- Pode operar em modo transparente e em modo *reverse.*

Instalação e gestão

- Instalação:
  - `sudo apt-get update`
  - `sudo apt-get install squid3`
- Gestão
  - `sudo service squid3 start|stop|reload|status`
  - Verificar sintaxe das configurações:
    - `sudo squid3 -k check`

Configuração

- Ficheiro de configuração:
  - `/etc/squid3/squid.conf`
- Utiliza ACLs para definir o tipo de tráfego permitido ou negado.
- A ordem de aplicação das regras interessa (idêntico ao *iptables*).
- É possível também definir regras por omissão.
- Algumas *tags*:
  - auth (autenticação de utilizadores)
  - acl (definição das listas de controlo de acessos)
  - http_access (definições de acesso HTTP)
  - network (definições de rede)
  - logs (definições relacionadas com *logs*)

Exercício 1

- Instale o serviço *Squid*
- Verifique em que porto está à escuta.
- Abra o *browser* e configure manualmente o seu *proxy*.
- Teste a navegação no site do IPLeiria.
- Conseguiu abrir o site pretendido?
- Se não conseguiu, qual será a justificação?

Network options

- A *tag* `http_port` permite definir o IP, porto e modo de operação.
- Sintaxe:
  - `http_port <porto> [opções] #3128 por omissão`
  - `http_port <nome_máquina:porto> [opções]`
  - `http_port <ip:porto> [opções]`

Access controls

- Nesta secção poderemos definir e personalizar as listas de controlo de acesso e aplicá-las ao sentido de saída ou entrada na nossa rede.
- A *tag* `acl` permite definir uma lista de controlo de acesso e suas regras.
- A *tag* `http_access` permite negar ou aceitar tráfego com base em `acl` definidas.
- A *tag* `http_reply_access` permite aceitar respostas aos pedidos dos clientes.

Tag ACL

- Esta *tag* permite definir e agrupar um conjunto de regras.
- Sintaxe:
  - `acl <nome_acl> <tipo_acl> <argumento|ficheiro>`
- Tipos de `acl`:
  - src
  - dst
  - dstdomain
  - dstdom_regex
  - time
  - url_regex
  - port
  - proxy_auth
  - rep_mime_type

Tag http_access

- Esta tag permite negar e/ou aceitar tráfego dos clientes com base nas `acl` previamente definidas.
- Sintaxe:
  - `http_access allow|deny [!]<nome_acl> …`

    Nota: o [!] permite-nos fazer a negação do tráfego definido pela `acl` indicada
  - Exemplo:

```
acl my_url dstdomain .badurl.com  # define domínio
http_access deny my_url           # aplica negando
```

Tag http_reply_access

- Esta *tag* permite negar e/ou aceitar tráfego de resposta aos pedido anteriores dos clientes com base em `acl` previamente definidas. Esta é complementar ao `http_access`.
- Sintaxe:
  - `http_reply_access allow|deny [!] <nome_acl> …`

    Nota: o [!] permite-nos fazer a negação do tráfego definido pela `acl` indicada
  - Exemplo:

```
acl Blockimg rep_mime_type image/png
http_reply_access deny Blockimg
```

Exercício 2

- Faça uma cópia de segurança

```
sudo mv /etc/squid3/squid.conf /etc/squid3/squid.conf.backup
```

- Crie um ficheiro vazio

```
sudo touch

sudo mv /etc/squid3/squid.conf
```

  - Edite o ficheiro e escreva:

```
http_port 3128                  # porto pré-definido, tb podia ser o 8080
acl my_net src 192.168.0.0/16   # acl para definir a rede local
http_access allow my_net        # permitir a rede local
http_access deny all            # política por omissão explícita
```

- Reconfigure: `sudo squid3 -k check && sudo service squid3 reload`
- Configure o seu navegador e teste a ligação

Error Page options

- A *tag* `error_diretory` permite definir a localização das páginas de erro.
- Sintaxe:

```
error_diretory <caminho_diretoria>
```

  - Exemplo:

```
error_directory
/usr/share/squid3/errors/Portuguese
```

Logfile options

- A tag access_log permite definir a localização do ficheiro de logs relativos aos vários acessos.
- Sintaxe:

```
access_log <filepath> [<logformat name> [acl acl …]]
```

  - Exemplo:

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

Exercício 3

- Altere as configurações do *Squid* por forma a que o mesmo:
  - fique à escuta no porto 8080.
  - mostre as páginas de erro em português.
- Altere as definições no *browser* tendo em conta estas alterações.
- Analise o ficheiro de logs de acesso.

Exercício 4

- Altere as configurações do *Squid* por forma a que o mesmo:
  - bloqueie o acesso aos sites do domínio *sapo.pt* e *publico.pt*
  - bloqueie o acesso a URLs que contenham as palavras:
    - torrent, sexo, sex
    - Dica: `acl Badwords url_regex -i palavra`
  - bloqueie acesso a sites FTP.
  - bloqueie a receção de imagens JPEG e PNG.
  - limite a 5 o número de ligações estabelecidas que um cliente pode ter.
  - limite a navegação web apenas em horário laboral e nos dias úteis.
  - bloqueie pedidos HTTP POST.

Authenticação

- Nesta secção poderemos definir e personalizar dados relativos à autenticação de utilizadores no *proxy*.
- A *tag* `auth_param` permite definir os parâmetros utilizados para a autenticação dos clientes do *proxy*.
- Sintaxe:
  - `auth_param <esquema> <parâmetro> [valor]`
- Tipos de esquema:
  - basic
  - digest
  - NTLM
  - negotiate

Exemplo de Autenticação “basic”

- `sudo apt-get install apache2-utils`

  `sudo htpasswd -c /etc/squid3/squid_passwd ss`

- Editar `/etc/squid3/squid.conf`

```
auth_param basic program
/usr/lib/squid3/basic_ncsa_auth
/etc/squid3/squid_passwd

auth_param basic utf8 on

auth_param basic children 5

auth_param basic realm Autenticação

auth_param basic credentialsttl 2 hours
```

Exercício 5

- Altere as configurações do *Squid* por forma a que o mesmo:
  - exija que todos os utilizadores se tenham de autenticar antes de poderem navegar na Internet.
  - Utilize o esquema de autenticação `basic`.
  - Mostre na janela de autenticação o `realm` “Autenticação no PROXY de SS”.
  - garanta que as credenciais dos utilizadores autenticados tenham 3 hora de tempo de vida.

  Ajuda: https://www.linode.com/docs/networking/squid/squid-http-proxy-ubuntu-12-04