Guia – Squid

Objetivos:

- Estudar o funcionamento de uma Proxy HTTP
- Configurar uma Proxy com cache para tráfego HTTP
- Nas configurações apresentadas neste guia, o caractere #, no inicio de uma linha, representa um comentário – não é necessário copiar.

Pré - requisitos

1. A máquina virtual em que vai instalar o Squid deverá estar configurada com Bridge (no software de virtualização)

2. Tem de existir conectividade entre a máquina virtual e a máquina física

3. A máquina onde vai instalar e configurar a *proxy/cache* deverá ser um Linux Ubuntu (ou variante)

Pré – requisitos (Alternativa)

1. Use a mesma máquina como proxy e como cliente (Browser)

HTTP Proxy

1. Instalar o Squid

```
sudo apt update
sudo apt install squid
```

2. Configurar o Squid como Proxy

   a) Fazer uma cópia do ficheiro de configuração

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.bak
```

   b) Editar o ficheiro de configuração

```
sudo nano /etc/squid/squid.conf
```

   c) Dentro do ficheiro encontre a regra *`http_access deny all`*

   d) Adicione as suas Regras de Permissão (*`Allow`*). Para isso, imediatamente antes da linha *`http_access deny all`*, adicione as seguintes linhas. (Isto cria uma lista de acesso (ACL) chamada localnet para os intervalos de IP privados comuns e, em seguida, permite o tráfego a partir dela.)

```
# Define as nossas redes privadas locais
acl localnet src 10.0.0.0/8       # Para redes como 10.x.x.x
acl localnet src 172.16.0.0/12  # Para redes como 172.16.x.x
acl localnet src 192.168.0.0/16 # Para redes como 192.168.x.x

# Permitir acesso da nossa rede local
http_access allow localnet

# Esta linha já deve existir, mantenha-a no fim
http_access deny all
```

   e) Iniciar e Activar o Squid

```
sudo systemctl restart squid
sudo systemctl status squid
```

3. Configurar o Cliente

O passo final é dizer aos outros dispositivos (como o seu PC Windows, Mac ou outra máquina Linux) para o usarem.

Vá às definições de Rede ou Proxy do seu dispositivo.

Procure pela secção "Proxy HTTP" ou "Configuração Manual de Proxy".

Insira o seguinte:

IP do Proxy / Servidor: O endereço IP do seu servidor Linux (ex: 192.168.1.10).

Porta: 3128

Guarde as definições.

4. Testar as configurações

Com base no que aprendeu nos exercícios das aulas anteriores, como pode testar que tudo está bem configurado e a funcionar?

CENTRO 2030 Os Fundos Europeus mais próximos de si. PORTUGAL 2030 Cofinanciado pela União Europeia

Configurar a Cache no Proxy

A configuração, permitirá ao Squid armazenar ficheiros acedidos frequentemente em disco em RAM (que é o seu principal objetivo).

1. Adicionar três diretivas principais ao ficheiro */etc/squid/squid.conf*. As linhas podem ser colocadas como novas linhas, perto do topo, logo abaixo da linha *http_port 3128*.

```
# === Adicione estas linhas para a cache ===

# 1. cache_dir: Define a cache em disco
#    "ufs" é o formato de armazenamento padrão.
#    "/var/spool/squid" é o diretório padrão.
#    "10000" é o tamanho da cache em MB (10GB). **Altere este valor**
para se ajustar ao seu espaço em disco.
#    "16" e "256" definem a estrutura de subdiretórios para a cache.
cache_dir ufs /var/spool/squid 10000 16 256

# 2. cache_mem: Define quanta RAM usar para "hot objects" (objetos mais
acedidos).
#    "256 MB" é um bom ponto de partida. Aumente isto se o seu servidor
tiver muita RAM.
cache_mem 256 MB

# 3. maximum_object_size: O maior ficheiro que o Squid guardará na
cache.
#    Isto impede que ficheiros enormes (como ISOs) encham a cache.
#    "100 MB" é um valor padrão moderno e razoável.
maximum_object_size 100 MB

# === Fim das novas linhas de cache ===

# As suas regras de acesso existentes do passo anterior
acl localnet src 10.0.0.0/8
acl localnet src 172.16.0.0/12
acl localnet src 192.168.0.0/16

http_access allow localnet
http_access deny all
```

2. Inicializar o Diretório de Cache

   a) Parar o Squid server

   ```
   sudo systemctl stop squid
   ```

   b) Definir Permissões e Criar a Cache

O pacote Squid geralmente cria o diretório `/var/spool/squid`, mas vamos garantir que as permissões estão corretas. O utilizador com que o Squid corre precisa de ser o dono (owner) deste diretório.

```
sudo mkdir -p /var/spool/squid

sudo chown squid:squid /var/spool/squid
```

c) Inicialize a Cache (constrói as sub-pastas 16x256)

```
sudo squid -z
```

d) Inicie o Squid

```
sudo systemctl start squid
```

e) Testar as configurações

Com base no que aprendeu nos exercícios das aulas anteriores, e com a informação seguinte, verifique se as configurações estão a funcionar.

Pode ver o log de acesso do Squid em tempo real com este comando:

```
sudo tail -f /var/log/squid/access.log
```

Veja as linhas com a seguinte informação `TCP_MISS/200`, `TCP_HIT/200` ou `TCP_MEM_HIT/200`. O que significam?

1. Num computador cliente, visite um site (ex: cnn.com).
2. No log, verá muitas linhas com **`TCP_MISS/200`**. Isto significa que o Squid teve de *falhar* a cache (não encontrou o objeto) e foi buscá-lo à internet.
3. Atualize (refresh) a página web no cliente.
4. Deverá agora ver linhas para os mesmos objetos (como imagens) com **`TCP_HIT/200`** ou **`TCP_MEM_HIT/200`**. Isto significa que o objeto foi servido a partir do disco (`HIT`) ou da RAM (`MEM_HIT`) do seu servidor, o que é muito mais rápido!

Bloquear domínios especificos

Impedir que os utilizadores da sua rede (definidos na `acl localnet`) acedam ao Facebook e aos seus serviços associados.

1. Editar o ficheiro de configuração */etc/squid/squid.conf*.

2. Definir a lista de bloqueio

Perto de onde definiu a sua `acl localnet`, adicione uma nova ACL para os sites que deseja bloquear. Para bloquear o Facebook eficazmente, precisa de bloquear mais do que apenas `facebook.com`; precisa de bloquear também as suas redes de entrega de conteúdo (CDN) e outros domínios, como o Instagram.

Adicione estas linhas:

```
# NOVA ACL: Define os sites que queremos bloquear acl sites_bloqueados
dstdomain .facebook.com .fb.com .fbcdn.net .instagram.com
```

o . (ponto): Colocar um ponto no início (`.facebook.com`) atua como um "wildcard", bloqueando `www.facebook.com`, `m.facebook.com`, `api.facebook.com`.

3. Aplicar a regra de bloqueio

Negar o tráfego que corresponde à lista que configurou anteriormente. Encontre a sua secção `http_access`.

Tem de inserir a sua nova regra `deny` **ANTES** da sua regra `allow localnet`. Se a colocar depois, o Squid permitirá o tráfego do `localnet` primeiro e nunca chegará a verificar a regra de bloqueio.

```
http_access deny sites_bloqueados
```

4. Recarregar a Configuração do Squid

```
sudo systemctl restart squid
sudo systemctl status squid
```

5. Testar as configurações

Com base no que aprendeu nos exercícios das aulas anteriores, e com a informação seguinte, verifique se as configurações estão a funcionar.