INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Aula 08: Servidor Proxy (Squid).

Olá, meus amores!!. Como é que vocês vão? Aproveitando para aprender muito? Oportunidade perdida não volta atrás. Hoje iremos entender o que é servidor proxy, fazer a instalação e configuração do servidor Squid na versão compilada e configurar regras de acesso ACL Vamos lá!!! Preparados???

Proxy

O serviço proxy tem por função limitar o tipo de tráfego que passa por ele. Instalado na borda de uma rede, efetua o monitoramento dos pacotes e, se for o caso, barra o trânsito. Atuando como um filtro de pacotes nas camadas mais altas, podendo limitar determinados tipos de protocolos, por exemplo o ICMP (ping).

Por funcionar analisando o tráfego, pode examinar o conteúdo do pacote na camada 7 (aplicação). Um exemplo clássico é procurar nos pacotes por palavras que constem em uma lista proibitiva, tal como "sexo". Todo pacote que contiver essa palavra será descartado, impedindo o acesso a páginas que contenham conteúdo impróprio ou estranho às necessidades da rede, seja uma rede residencial, de empresa ou de escola.

Outra finalidade do proxy é atuar como cache. Nesse caso, o servidor reserva uma área em memória para armazenar os conteúdos estáticos acessados com maior frequência pelos usuários de rede interna. Quando o usuário busca por determinada informação, o servidor proxy cache o entrega diretamente sem acessá-lo na internet. Considere por exemplo um grande portal de notícias da internet. A primeira pessoa a acessá-lo fará com que o conteúdo dessa página fique armazenado no cache do servidor. As próximas pessoas que acessarem essa mesma página, dentro do tempo de expiração programado, obterão o conteúdo do servidor, em vez do conteúdo da internet.

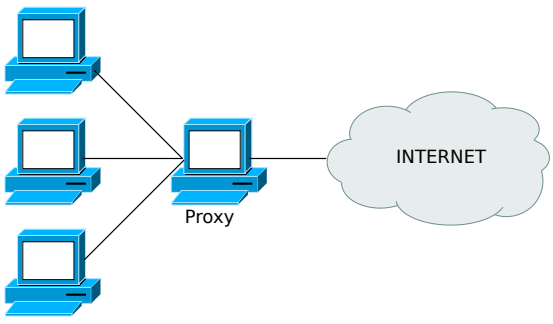

Figura 1: Funcionamento do Proxy cache

Portanto, essas duas soluções apresentam, por motivos diferentes, melhoria no tráfego da rede. O proxy bloqueia o tráfego considerado inadequado pela política de utilização da rede da empresa, enquanto o cache contribui para reduzir o montante de tráfego no link externo da rede.

Squid

Squid é um dos proxies mais utilizados na internet. Considerado simples e confiável, é um recurso praticamente obrigatório em qualquer tipo de organização que utilize serviços de internet, desde pequenas empresas aos grandes provedores de acesso.

A grande vantagem do Squid é a capacidade de armazenar documentos da internet e criação de regras de acesso, que permitem ou bloqueiam o acesso a determinadas páginas.

1. O primeiro passo é instalar o pacote squid. A partir de um terminal, digite:

```
sudo apt-get install squid
```

Iremos configurar o squid através do arquivo de configuração. O arquivo principal de configuração está localizado em "/etc/squid/squid.conf". O arquivo de configuração padrão possui uma quantidade significativa de comentários com objetivo de documentar várias diretivas de configuração. Antes de começar a configuração copie o arquivo original para um arquivo de *backup* ("/etc/squid/squid.conf.bkp").

2. Criar cópia de backup.

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

3. Abra o arquivo de configuração usando o comando:

```
sudo gedit /etc/squid/squid.conf
```

Arquivo de Configuração

O arquivo de configuração do squid.conf possui grande número de parâmetros que podem ser utilizados. Ao colocar o Squid em funcionamento pela primeira vez, é recomendável incluir os parâmetros aos poucos, especialmente o ACL, justamente para que se possa per- ceber a efetividade de cada um. Alguns desses parâmetros:

- http_port: número da porta utilizada pelo servidor, em geral 3128;
- cache_mem: quantidade de memória RAM utilizada pelo proxy web (em MB), default 256 MB;
- cache_dir: define vários parâmetros de cache, como tipo de armazenamento, diretório de cache, quantidade em MB, número de diretórios de primeiro nível, número de diretórios de segundo nível. Exemplo: cache_dirufs /usr/local/squid/var/cache 500 16 256;
- access_log: localização do arquivo com logs de acesso ao conteúdo web;
- cache_log: arquivo com informações de log;
- Listas de controle de acesso (acl): são regras de acesso utilizadas pelo sistema para controlar quem pode acessar o que e quando. Por meio de um conjunto de regras encadeadas, permite bloquear ou liberar determinados tipos de acesso, além de limitar o consumo de banda em determinadas situações.

Para um bom entendimento do funcionamento das ACLs, é necessário considerar:

- As diretivas do arquivo squid.conf são lidas de cima para baixo, com cada solicitação de acesso comparada com cada regra de acesso, até que seja encontrada uma que combine ou até que seja atingido o final do arquivo.
- A última regra deve sempre bloquear todas as solicitações de acesso. Desse modo, caso nenhuma regra prévia corresponda à solicitação efetuada, haverá uma última que bloqueia o acesso.
- Não criar regras redundantes, desnecessárias ou que exijam resolução DNS, para não diminuir o desempenho do proxy.

São exemplos de acls:

```
acl rede_interna src 192.168.0.0/24
http_access allow rede_interna
```

A primeira linha associa a lista de controle de acesso rede_interna ao intervalo de endereços definido por 192.168.0.0/24. A segunda linha informa que os elementos da lista de controle de acesso rede devem ter seu acesso permitidos ao serviço http.

```
acl Safe_ports port 80
http_access deny !Safe_ports
```

A primeira linha cria um controle de acesso Safe_ports referente a porta 80 (http). A segunda linha informa que todos os acessos que não sejam da porta 80 serão bloqueados.

```
acl sites_proibidos url_regex -i "/etc/squid/sites_proibidos"

http_access deny sites_proibidos
```

Nesse exemplo é criado uma regra chamada "sites_proibidos" que bloqueará as palavras ou URLs contidas no arquivo indicado no caminho "/etc/squid/sites_proibidos". Nã o esqueça de criar este arquivo com as palavras proibidas, uma por linha. Em seguida, com a instrução deny, proibimos o acesso aos sites listados na regra que criamos na linha cima.

```
acl downloads_proibidos url_regex -i \.exe \.torrent \.avi \.mp3

http_access deny downloads_proibidos
```

Nesta regra bloqueamos o download de alguns tipos de extensões. Da mesma maneira criamos a regra primeiro e bloqueamos depois.

```
acl almoco time MTWHF 12:00-13:55
http_access allow almoco
```

ACL com controle de data e hora. A lista de acesso almoco permite o acesso durante o almoço de segunda a sexta, no horário de 12h até 13h55, negando acesso nos demais horários.

```
http_access deny all
```

ACL que bloqueia todo e qualquer acesso.

4. Apague o conteúdo do arquivo squid.conf e insira o texto mostrado abaixo:

```
http_port 3128
cache_dir ufs /var/spool/squid 1024 16 256
cache_mem 256 MB
access_log daemon:/var/log/squid/access.log squid
cache_log /var/log/squid/cache.log

#EXEMPLO DE ACL
acl sp url_regex -i "/etc/squid/sites_proibidos"
acl all src all

http_access deny sp
http_access allow all
```

Nesse exemplo, iremos apenas bloquear alguns sites que apresentam palavras chaves localizadas no arquivo "/etc/squid/sites_proibidos". Todos os demais sites terão acesso normal.

5. Crie o arquivo com os sites e palavras proibidas:

O arquivo contém uma relação de conteúdo que deve ser bloqueado, seja esse conteúdo uma extensão de arquivo, uma palavra-chave ou mesmo uma URL.

```
sudo gedit /etc/squid/sites_proibidos
```

```
ifrn
ufrn
```

6. Utilize o comando para criar os diretórios de cache

```
sudo squid -z
```

7. Finalmente, reinicialize os serviços do squid para habilitar as novas configurações:

```
sudo /etc/init.d/squid restart
```

Configuração nos Navegadores

Qualquer um dos navegadores disponíveis pode ser configurado para acesso via proxy. De modo geral, por meio de uma interface de configuração, é possível informar os dados do servidor, como endereço IP e porta.

- Mozilla Firefox: deve-se acessar o menu "Preferências", "Avançado", "Rede", em "Conexões" clique em "Configurações". Agora selecione "Configurar proxy manualmente" informe o endereço IP e porta utilizados. Marque "utilizar esse proxy para todos os protocolos".

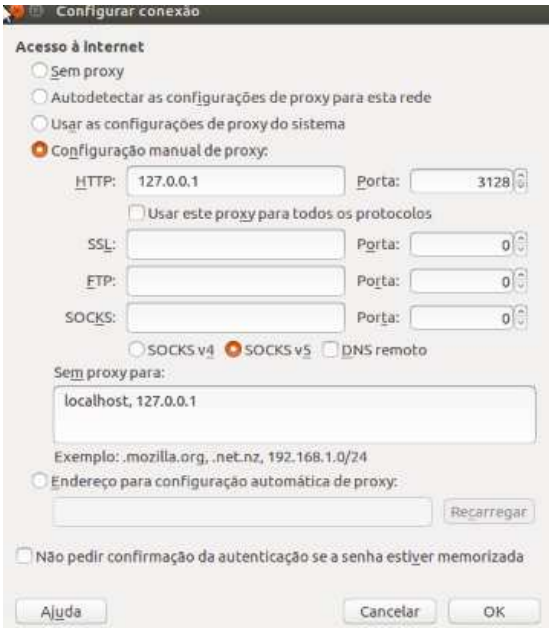

Figura 2: Configuração no Firefox

- Microsoft Edge: clique no menu "Iniciar", e em "Configurações". Nas Configurações, selecione "Rede e Internet". Vá para a aba "Proxy", e procure "Configuração de proxy Manual". Na Configuração Manual de proxy, Ative a opção "Usar um servidor proxy", no "Endereço" digite o 192.168.0.1, em "Porta" digite 3128 e clique em "Salvar".

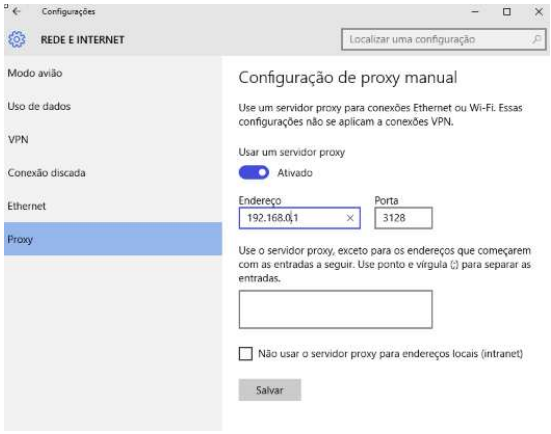

Figura 3: Configuração no Windows 10

Exercício de Fixação

1. Instale e configure o servidor proxy squid. Vá inserindo aos poucos as listas de controle de acesso:

- Acesso a rede interna;
- Bloqueio de download de arquivos com extensão .mp3 e .avi;
- Não permitir o acesso à internet nos horários de 0h as 6h e de 19h as 23:59h, durante os dias da semana;
- Bloquear acesso ao site do IFRN (`www.ifrn.edu.br`).

2. Configure um cliente proxy, e teste cada lista de controle de acesso.

3. Verifique o arquivo de log "/var/log/squid/access.log" e verifique os objetivos armazenados.

4. É possível configurar o proxy de tal forma que não seja necessário configurar o navegador na estação (tal configuração é denominada transparente). Pesquise como fazê-la e implemente-a no seu proxy.