Squid

Servidor de Proxy

O Squid é uma aplicação de proxy para filtro de conteúdo, sendo funcional em diversas plataformas. Ele aplica regras aos pacotes que são trafegados na rede interna e também com destino a internet. É diferente de um Firewall, pois não filtra pacotes que chegam da rede externa. Neste exemplo, vamos nos basear na plataforma Linux, na distribuição Ubuntu.

INSTALAÇÃO

Para instalar o SQUID, basta digita o comando abaixo:

sudo apt install squid

Após a instalação, os arquivos de configuração ficarão em /etc/squid.

CONFIGURAÇÃO

Dentro do diretório /etc/squid existe o arquivo de configuração squid.conf. Uma boa prática é fazer uma cópia do arquivo de configuração original, para uso em caso de erros na configuração personalizada. Então execute o comando:

sudo cp squid.conf squid.conf.original

CONFIGURANDO O SQUID - AUTENTICAÇÃO

```
auth_param basic program /usr/lib/squid/pam_auth
auth_param basic children 10
auth_param basic realm Faça seu login
auth_param basic credentialsttl 4 hours
auth_param basic casesensitive off
```

Agora iremos abrir o arquivo de configuração para personalizá-lo. Abra com o editor de sua preferência e observe as características do arquivo. Ele é bastante extenso, pois já vem com várias configurações padrão, a maioria delas comentadas, com exemplos e explicações. Como é um arquivo muito grande, uma operação comum é apagar todo o conteúdo e inserir apenas o necessário, lembrando que temos um backup para consulta e recuperação. Vamos observar algumas configurações possíveis, analisando linha a linha. Observe o quadro acima.

A primeira linha especifica qual script será responsável por processar a autenticação, neste caso utilizando as próprias contas de usuários da rede. A configuração children refere-se a quantidade de processos simultâneos serão suportados, a fim de evitar múltiplas autenticações ao mesmo tempo. A terceira linha é uma frase que irá aparecer ao usuário na caixa de autenticação do Squid. A quarta linha especifica o tempo máximo de 4 horas para o usuário permanecer autenticado (ou até ele fechar o navegador). A última linha ignora a diferença entre maiúsculas e minúsculas na autenticação.

CONFIGURANDO O SQUID - ACL

```
acl all src all
acl localhost src 127.0.0.1/32
acl usuarios proxy_auth REQUIRED
```

O proxy Squid funciona por meio de regras chamadas ACL (Access Control List), que pode ser uma lista de endereços IP ou de URL bloqueadas/liberadas para acesso na rede. O próprio Squid já possui na instalação uma grande quantidade de ACL prontas como controle por horários, dia da semana, endereços localhost (pacotes de sua própria máquina), portas TCP, navegadores, etc ., o que permite um controle total da rede. Observe as ACL criadas à esquerda

Essas são três ACL essenciais para o controle. A primeira define todas as regras possíveis para quaisquer situações. É interessante criá-la para quando precisamos liberar plenamente o proxy, por algum motivo

(manutenção, testes, etc). A segunda ACL controla os pacotes oriundos da própria máquina onde o Squid está instalado, por exemplo, para testes no servidor Web. A última regra (chamamos hipoteticamente de 'usuarios') diz que a autenticação é obrigatória para conseguir passar pelo proxy. Podemos também criar nossas próprias ACL, de acordo com a necessidade de controle. Para exemplo, vamos criar listas de controle para termos ou palavras contidas em endereços de site e também para extensões de arquivos. Acompanhe o quadro abaixo.

CONFIGURANDO O SQUID - ACL

```
acl bloqueados url_regex sexo download ultrasurf
acl liberados url_regex sexoesaude
acl downloads urlpath_regex \.mp3$ \.avi$
```

Na primeira regra, criamos uma ACL chamada "bloqueados" utilizando o comando url_regex para indicar os termos que não serão aceitos pelo proxy, isto é, não poderão estar contidos na URL. A mesma lógica é usada na segunda ACL, onde adicionamos possíveis exceções para a regra anterior. A terceira ACL são para controles de extensões de arquivos, através do comando urlpath_regex. Como geralmente as extensões vêm no final da URL, é necessário colocar o cifrão ($) para indicar o final do arquivo. É possível também indicar um arquivo de texto contendo palavras bloqueadas ou permitidas. Para isto, utilize o comando –i para descartar diferenças entre maiúsculas e minúsculas e o caminho completo do arquivo, por exemplo,url_regex –i "/etc/squid/bloqueados.txt".

CONFIGURANDO O SQUID – HTTP_ACCESS

```
http_access allow liberados
http_access deny bloqueados
http_access deny downloads
http_access allow usuarios
http_access allow localhost
http_access deny all
```

A ordem em que as ACL são criadas é extremamente importante e indica o que será bloqueado ou não. Isto significa que na ACL "liberados", só será liberado o que não foi bloqueado antes, na regra anterior, pois a leitura do Squid ocorre de cima para baixo. Por isso, é recomendável, na última linha, bloquear tudo o que não foi liberado antes, por alguma regra. Depois de criadas as ACL, iremos controlá-las com o comando http_access, negando (deny) ou permitindo (allow) que elas passem pelo proxy, seguindo uma lógica sequencial. Acompanhe as regras aplicadas no quadro acima. Para finalizar o Squid, iremos inserir as configurações gerais do proxy. Essas configurações são necessárias para o bom funcionamento do servidor.

CONFIGURANDO O SQUID – CONFIGURAÇÕES GERAIS

```
http_port 3128
cache_mem 512 MB
maximum_object_size_in_memory 4 MB
cache_dir ufs /var/spool/squid 3000 16 256
access_log /var/log/squid/access.log squid
cache_mgr jonas@sorjonas.com.br
visible_hostname SERVIDOR
error_directory /usr/share/squid/errors/portuguese
```

A primeira linha especifica a porta aonde o Squid irá "escutar"; a porta padrão é 3128. O cache_mem especifica o tamanho da memória cache do Squid, onde é recomendado utilizar ¼ da memória RAM. A terceira linha limita o tamanho de objetos sendo manipulados na memória RAM. O cache_dir regula o funcionamento do cache, com o modo de gravação UFS (Unix File System), o local de gravação, o tamanho em MB do espaço em disco, quantidade de subdiretórios e, dentro destes, mais uma quantidade de subdiretórios. A próxima linha configura o log (o arquivo de registro das ações do usuário), com o local de gravação do log e o formato de gravação padrão do proxy (squid). Logo após vem o e-mail do administrador

do proxy, o nome do servidor que ficará visível na rede e o diretório com as páginas de erro do Squid, que podem ser configuradas com linguagem HTML. Vamos reiniciar o Squid para colocá-lo em operação. Salve o arquivo, feche-o e reinicie o Squid com a linha abaixo.

sudo service squid restart ou sudo /etc/init.d/squid restart

RELATÓRIO

Os relatórios do Squid costumam gerar grandes quantidades de texto, dificultando sua leitura e consulta. Para facilitar, existe a ferramenta SARG (Squid Analysis Report Generator) que converte os relatórios para páginas HTML. Para instalar o SARG, utilize o comando abaixo:

sudo apt-get install sarg

Após a instalação, abra o arquivo de configuração em /etc/sarg/sarg.conf e configure como sugerido a seguir:

1. Edite a linha language para Portuguese.
2. Edite também a linha access_log para a mesma linha de log do Squid.
3. Desça até a linha output_dir e edite para /var/www/sarg para armazenar as páginas diretamente no servidor web (tenha o Apache instalado).
4. Salve o arquivo, feche-o e crie o diretório “sarg” com o comando mkdir –p /var/www/sarg. Após isso, digite “sarg” (sem aspas) para gerar o relatório. Caso queira visualizar o relatório gerado, abra o navegador e digite ipdoservidor/sarg.

EXERCÍCIO

Você é o administrador da rede de uma empresa, a mesma não possui nenhum controle de acesso dos clientes, todos da rede acessam de forma indiscriminada qualquer site. Configure um servidor Proxy conforme opções abaixo:

1 - O servidor Proxy irá rodar na porta 8080;

2 – O espaço para cache do servidor deverá ter um tamanho de 1GB e o tamanho máximo dos objetos salvos na memória 64 KB;

3 - O Proxy deverá funcionar com autenticação com o programa /usr/lib/squid/ncsa_auth, com 5 instâncias máximas e exibindo a frase SERVIDOR RESTRITO

4 – Deverá conter uma ACL que negue o acesso no sábado e domingo e nos demais dias nos horários de 12:00 às 14:00

5 – Deverá também conter uma ACL que negue o acesso aos domínios de destino uol.com.br, pudim.com.br, hotmail.com, facebook.com e qualquer site que contenha a palavra “piratebay.

6 – Bloqueie também o acesso a porta 443 para sites https

7 – Bloqueie o IP do site sorjonas.com.br

Referência para comandos do Squid (Universidade Federal do Rio Grande do Norte, Prof Felipe Raulino):
https://docentes.ifrn.edu.br/filiperaulino/disciplinas/seguranca-de-redes/aulas/Aula%20extra%20squid.pdf/at_download/file