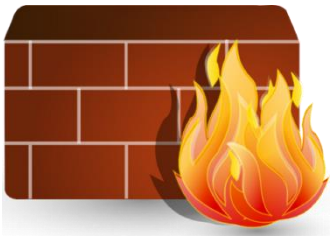
Universidade Federal do Ceará
Campus Quixadá



Squid

Prof. Michel Sales Bonfim

Disciplina: Auditoria de Segurança de SI | **Curso**: Sistemas de Informação

Servidor proxy/cache

- O objetivo principal de um servidor proxy é possibilitar que máquinas de uma rede privada possam acessar uma rede pública, como a Internet, sem que para isto tenham uma ligação direta com esta.

- O servidor proxy costuma ser instalado em uma máquina que tenha acesso direto à internet, sendo que as demais efetuam as solicitações através desta. Justamente por isto este tipo é chamado de Proxy, pois é um procurador, ou seja, sistema que faz solicitações em nome de outros.

Servidor proxy/cache

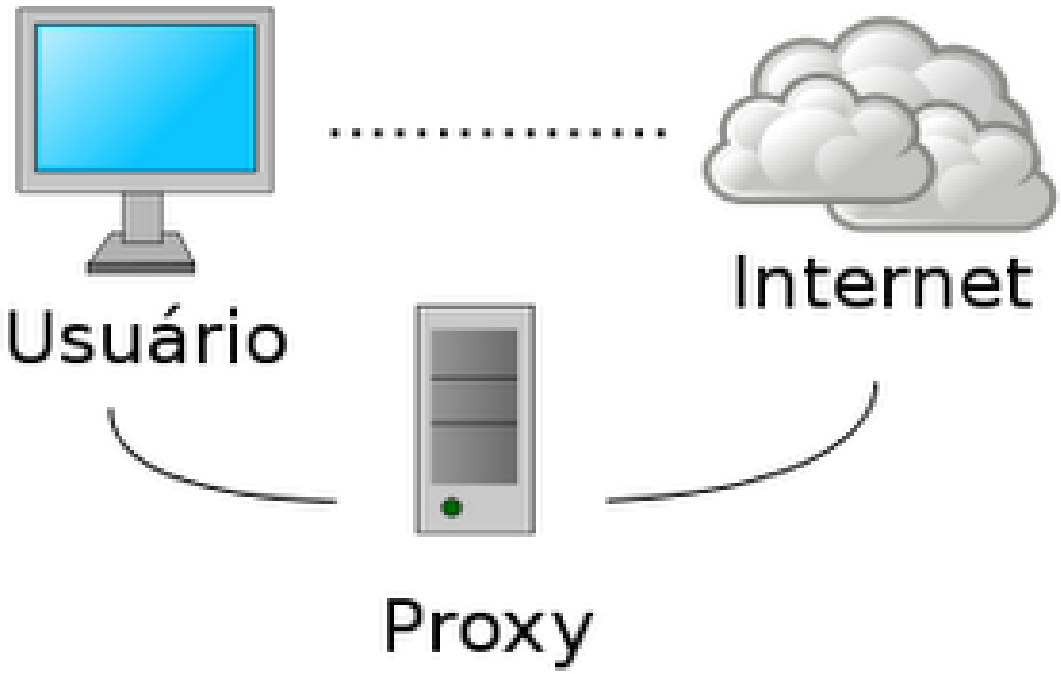


Figura 01: esquema de uso de um servidor proxy

Squid - Instalação

- Utilizando o apt:

```
# apt-get update
# apt-install squid
```

Os pacotes de instalação serão baixados e instalados no sistema.

Squid - Configuração

- O arquivo de configuração do squid se encontra em:

  /etc/squid/squid.conf

  Salve o arquivo original:

```
# cd /etc/squid3
# cp ./squid.conf ./squid.conf.original
```

Squid - Configuração

http_port 3128

Esta opção é utilizada para definir em quais portas o Squid espera por conexões http.

A porta padrão é 3128, mas é possível especificar outra.

Squid - Configuração

cache_dir ufs /var/spool/squid 100 16 256

Define em quais diretórios serão armazenados os objetos.

Tipo: tipo de sistema de armazenamento (ufs)

Diretório: diretório do arquivo que mantém os metadados dos objetos armazenados no disco. Este arquivo é utilizado para recriar o cache durante a inicialização do Squid.

Mbytes: espaço em disco que deverá ser utilizada sob este diretório. O valor padrão é 100 MB.

Nível-1 e Nível-2 :número de diretórios de primeiro e segundo nível a serem criados. Os valores padrão são 16 e 256.

Squid - Configuração

cache_mem 8MB

O Squid utiliza muita memória por razões de desempenho. O proxy armazena em memória os objetos mais acessados.

Esse parâmetro não é o total de memória que o Squid usa, ele apenas põe um limite na área de armazenamento de objetos.

Squid - Configuração

maximum_object_size_in_memory 64 KB

Esta linha é responsável por limitar o tamanho dos arquivos que serão armazenados no cache da memória RAM.

cache_access_log /var/log/squid3/access.log

Define onde serão armazenados os registros de log do Squid.

Squid - Configuração

Controles de acesso:

O controle de acesso do *Squid* tem recursos suficientes para definir com precisão quais tipos de serviços podem ser acessados por quais máquinas e em quais horários.

As regras da lista de controle de acesso (*Access Control List* ou simplesmente ACLs) tem uma sintaxe bastante simples e são incluídas no arquivo ***squid.conf***.

acl <nome da acl> <elemento> <valor>

Servidor proxy/cache

Controles de acesso:

Tipos de elementos de ACL:

- src: endereço IP de origem (cliente);
- dst: endereço IP de destino (servidor);
- srcdomain: um domínio de origem (cliente);
- dstdomain: um domínio de destino (servidor);
- srcdom_regex: padrão de texto, ou expressão regular, que conste no conteúdo da origem (cliente);
- dstdom_regex: padrão de texto, ou expressão regular, que conste no conteúdo do destino (servidor);
- time: hora do dia e dia da semana;

Servidor proxy/cache

Controles de acesso:

Tipos de elementos de ACL:

- url_regex: comparação de URL baseada em expressão regular;
- port: número da porta do destino (servidor);
- proto: protocolo de transferência (http, ftp, etc);
- method: método http de requisição (get, post, etc);
- proxy_auth: autenticação do usuário via um processo externo;
- proxy_auth_regex: expressão regular que consta em uma autenticação de usuário via um processo externo;
- maxconn: um número máximo de conexões de um mesmo endereço IP de cliente

Servidor proxy/cache

Controles de acesso:

Cada elemento de ACL deve ser relacionado com somente um nome. Um elemento ACL com determinado nome consiste em uma lista de valores. Quando forem sendo feitos os testes, os múltiplos valores utilizarão o operador lógico OR. Em outras palavras, um elemento ACL será válido, quando qualquer um de seus valores forem verdadeiros.

Você não pode dar o mesmo nome para diferentes tipos de elementos ACLs. Isto ocasionará um erro de sintaxe.

Você poderá colocar diferentes valores para a mesma ACL em diferentes linhas. O Squid os combinará em uma lista.

Servidor proxy/cache

Listas de acesso:

Uma regra de lista de acesso consiste da palavra allow (permitir) ou deny (negar), seguido de uma lista de nomes de elementos ACL.

Uma lista de acesso consiste em uma ou mais regras de acesso.

As listas de acesso são verificadas na mesma ordem em que foram escritas. A pesquisa na lista termina assim que uma requisição satisfazer uma regra.

Se uma regra possuir múltiplos elementos de ACL, esta usará o operador lógico AND. Em outras palavras, todos os elementos de uma regra precisarão ser validos para que esta regra seja válida. Isto significa que é possível escrever uma regra que nunca será válida.

http_access: permite clientes http (browsers) acessarem a porta http. Esta ACL é a primária

Por exemplo, um número de porta nunca poderá ser igual a 80 e 8000 ao mesmo tempo.

Servidor proxy/cache

Exemplos práticos:

Se você quiser impedir que qualquer usuário acesse paginas que contenham a palavra "cracker" na URL, acrescente as seguintes linhas no seu *squid.conf*:

```
acl proibir_cracker url_regex cracker
http_access deny proibir_cracker
```

Servidor proxy/cache

Exemplos práticos:

Usuário da máquina cujo IP é 10.0.0.95 ocupando muito a sua rede com transferência de arquivos de música em formato MP3.

Para bloquear este usuário especifico, use a regra como a de baixo:

```
acl mp3 url_regex mp3
acl usr_ofensor src 10.0.0.95/255.255.255.255
http_access deny usr_ofensor mp3
```

Servidor proxy/cache

Exemplos práticos:

Proibir todos os usuários de acessarem um determinado site:

```
acl site_proibido dstdomain .orkut.com
http_access deny all site_proibido
```

Servidor proxy/cache

Exemplos práticos:

Existem casos que uma empresa gostaria de liberar o acesso a internet apenas durante o horário de almoço. Para isso, a seguinte regra poderia ser aplicada:

```
acl funcionários src 10.0.0.0/0
acl acesso_almoco time MTWHF 12:00-13:00
http_access allow funcionários acesso_almoco
http_access deny funcionários
```

Servidor proxy/cache

Exemplos práticos:

Dependendo do número de domínios ou de palavras-chave listadas em ACLs é aconselhável construir uma lista em um arquivo separado e indicá-lo no squid.conf. O arquivo com uma lista de domínios ou de expressões regulares a serem bloqueadas deve conter uma entrada por linha, como no exemplo:

Orkut
Playboy
Sexo
Blog
Fotolog

Servidor proxy/cache

Exemplos práticos:

Caso o arquivo seja "/etc/squid3/sites_proibidos", por exemplo podemos indicá-lo no arquivo de configuração do squid da seguinte maneira:

```
acl funcionarios src 10.0.0.0/0
acl proibidos url_regex "/etc/squid3/sites_proibidos"
http_access deny funcionarios proibidos
```

Servidor proxy/cache

Exemplos práticos:

Após incluir todas as regras restritivas, não se deve esqueçer de incluir regras especificando que tudo o que não estiver expressamente proibido deve ser permitido. Na configuração original do squid.conf, as linhas serão como a que segue:

```
acl rede_local src 10.0.0.0/255.0.0.0
http_access allow all rede_local
```

Note que deve-se definir a "rede_local" como conjunto de endereço IP e máscara que melhor descrevem a sua rede.

Servidor proxy/cache

Exemplos práticos:

Normalmente o arquivo squid.conf virá com linhas como as que seguem:

```
#
# INSERT YOUR OWN RULE(S) HERE ALLOW ACCESS FROM YOUR CLIENTS
#
http_access deny all
```

Ela serve para bloquear o acesso ao Squid até que ele seja configurado, e é interessante deixá-lo como última regra, pois desta forma, se a requisição não satisfazer nenhuma regra o squid irá bloqueá-la.