Prática dirigida

Filtragem de conteúdo no Proxy Server com o SquidGuard

Algumas das dificuldades dos administradores de servidores proxy é a gestão dos utilizadores através das regras de ACL do Squid. O SquidGuard minimiza este problema proporcionando uma configuração mais eficiente.

Nas distribuições derivadas do Debian, você pode instalá-lo rapidamente via apt-get:

#apt-get install squidguard

A configuração é feita em três fases. O primeiro passo é baixar os ficheiros das listas desejadas e descompactá-los no diretório "/var/lib/squidguard/db". Em seguida, é necessário configurar o ficheiro "/etc/squid/squidGuard.conf", especificando os ficheiros de listas que serão usados e o comportamento do SquidGuard ao bloquear os acessos e, finalmente, editar o /etc/squid/squid.conf", adicionando a linha que ativa o uso do SquidGuard.

Vamos começar baixando as listas. Vou usar como exemplo as listas do Shalla e do MESD, mas você pode usar os mesmos passos para usar outras listas que desejar.

Comece baixando as listas em um diretório qualquer, como em:

#wget -c https://squidguard.mesd.k12.or.us/blacklists.tgz
#wget -c https://www.shallalist.de/Downloads/shallalist.tar.gz

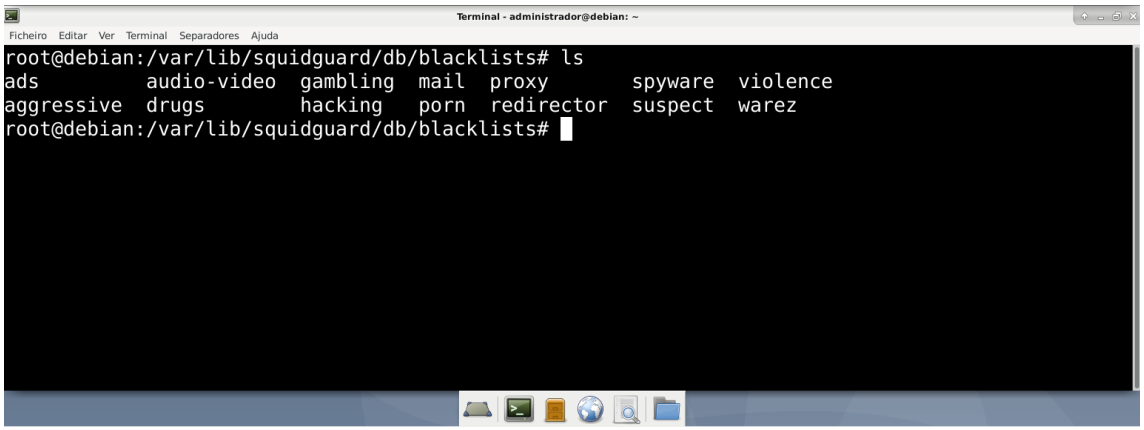
Copie os dois ficheiros para o diretório "/var/lib/squidguard/db" e descompacte-os, como em:

#cp blacklists.tgz shallalist.tar.gz /var/lib/squidguard/db/
#cd /var/lib/squidguard/db/
#tar -zxvf blacklists.tgz
#tar -zxvf shallalist.tar.gz

Aproveite para remover os dois ficheiros, já que não precisaremos mais deles:

#rm -f blacklists.tgz shallalist.tar.gz

Com isso, você terá as pastas “BL” (as listas do Shalla) e “blacklists” (listas do MESD) dentro do diretório, cada uma contendo um conjunto de subpastas, como neste screenshot:



Como pode ver, as listas são divididas por assunto. A lista do MESD é concentrada em temas ilegais, enquanto a lista do Shalla inclui listas relacionadas a temas diversos, que você pode bloquear ou não de acordo com a situação. Dentro de cada pasta, você encontra dois ficheiros, “domains” e “urls”, o primeiro contendo domínios que são bloqueados completamente e o segundo contendo URLs isoladas.

Com isso, você tem as duas listas à disposição e pode escolher qual das duas utilizar, ou mesmo combinar seções de ambas para incrementar o filtro.

O próximo passo é configurar o ficheiro “/etc/squid/squidGuard.conf”, especificando as listas a utilizar. Um exemplo básico de ficheiro de configuração, usando apenas duas das seções da lista do MESD, seria:

```
# /etc/squid/squidGuard.conf
dbhome /var/lib/squidguard/db/blacklists
logdir /var/log/squid

dest porn {
domainlist porn/domains
```

```
urllist porn/urls
}
dest proxy {
domainlist proxy/domains
urllist proxy/urls
}
acl {
default {
pass !porn !proxy all
redirect https://www.ispgaya.pt/site/
}
}
```

As duas primeiras linhas indicam o diretório contendo as blacklists e o diretório onde serão armazenados os logs. No exemplo estou usando as listas do MESD, daí o "/var/lib/squidguard/db/blacklists" e estou orientando o SquidGuard a salvar o log no mesmo diretório utilizado pelo Squid, gerando o ficheiro "/var/log/squid/squidGuard.log".

Em seguida, temos duas ACLs, batizadas de "porn" e proxy", cada uma incluindo os dois ficheiros da categoria correspondente dentro das listas. Para que fossem adicionadas mais seções, bastaria adicionar uma nova ACL para cada uma.

No final, a opção "pass" indica como as duas ACLs serão usadas. No exemplo, usei a linha "pass !porn !proxy all", que indica que os acessos a páginas citadas nas listas deve ser bloqueados, mas o acesso a outras páginas é aceito.

Concluindo, usei a linha "redirect https://www.ispgaya.pt/site/", que faz com que todos os acessos bloqueados sejam redirecionados de forma transparente à URL especificada. Dessa forma, o utilizador tentando aceder páginas impróprias é sutilmente direcionado a uma página com conteúdo mais saudável. Você pode substituí-la pelo site da empresa, ou mesmo pela localização de uma página de aviso.
Antes que possam ser efetivamente utilizadas, as listas precisam ser convertidas para o formato Berkeley DB, que permite um acesso muito mais rápido do que seria possível ao manipular diretamente os ficheiros em texto. Para isso, use (depois de configurar o ficheiro "/etc/squid/squidGuard.conf", o comando:

```
#squidGuard -C all
```

Embora não seja necessário em muitas configurações, é recomendável usar também o comando abaixo para ajustar as permissões de acesso aos ficheiros, garantindo que o

Squid tenha acesso a eles. O "proxy:proxy" indica o utilizador e o grupo utilizados pelo Squid, que podem eventualmente ser diferentes, de acordo com a distribuição usada:

#chown -R proxy:proxy /var/lib/squidguard/db/*

Os dois comandos a seguir complementam a configuração, fazendo com que todos os ficheiros dentro da pasta sejam configurados com permissões 644 e as pastas com 755, que é a configuração correta. Isso previne o aparecimento de erros diversos relacionados a permissões incorretas para os ficheiros:

#find /var/lib/squidguard/db -type f | xargs chmod 644
#find /var/lib/squidguard/db -type d | xargs chmod 755

Depois de gerar a configuração do SquidGuard, o próximo passo é alterar a configuração do Squid, para que ele seja utilizado. Para isso, edite o ficheiro "**/etc/squid/squid.conf**", adicionando a linha:
redirect_program /usr/bin/squidGuard

Ela deve ser colocada depois das ACLs restritivas (destinadas a bloquear acessos, como no caso das ACLs para bloquear o acesso a uma lista de sites personalizados, ou em determinados horários), mas entretanto antes das regras finais, que permitem o acesso. Um exemplo de ficheiro squid.conf completo seria:

```
# /etc/squid/squid.conf
https_port 3128 transparent
visible_hostname gdh
cache_mem 128 MB
maximum_object_size_in_memory 128 KB
maximum_object_size 512 MB
cache_dir ufs /var/spool/squid 4096 16 256
cache_access_log /var/log/squid/access.log
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 21 80 443 563 70 210 280 488 59 777 901 1025-65535
acl purge method PURGE
acl CONNECT method CONNECT
https_access allow manager localhost
https_access deny manager
https_access allow purge localhost
https_access deny purge
https_access deny !Safe_ports
```

https_access deny CONNECT !SSL_ports
redirect_program /usr/bin/squidGuard
acl redelocal src 192.168.1.0/24
https_access allow localhost
https_access allow redelocal
https_access deny all

A posição da regra que ativa o SquidGuard é importante, pois se ela for colocada depois da regra “https_access allow redelocal” (ou similar), as requisições serão liberadas antes de passar pelo SquidGuard, fazendo com que ele nunca seja usado.

Opcionalmente, você pode incluir também as duas linhas abaixo, logo após a linha que ativa o SquidGuard:

redirect_children 8
redirector_bypass on

A opção “redirect_children” ajusta o número de processos do SquidGuard que o servidor Squid manterá abertos. Aumentar o número ajuda a melhorar o desempenho do proxy em grandes redes, onde o proxy recebe um volume muito grande de requisições.

A opção “redirector_bypass on” faz com que o Squid continue funcionando mesmo que o SquidGuard trave ou deixe de funcionar por qualquer motivo. Usá-la tem seus prós e contras, já que pode ser preferível que o acesso pare completamente, até que você consiga solucionar o problema, do que permitir que o Squid funcione com os bloqueios desativados. Pense no caso de uma escola primária, por exemplo.

Depois de tudo terminado, reinicie o Squid para que a configuração entre em vigor:
#/etc/init.d/squid restart

Se você estiver configurando um servidor de produção, com utilizadors acessando o proxy enquanto está configurando, use o comando abaixo para ativar a configuração sem derrubar os utilizadores conectados:
squid -k reconfigure

Com o SquidGuard ativo, os acessos a páginas impróprias será drasticamente reduzido e você conserva a possibilidade de refinar o bloqueio, adicionando novos endereços manualmente. Não se esqueça de atualizar os ficheiros das blacklists periodicamente, já que elas são atualizadas de forma freqüente.

Com o tempo, é provável que você precise desbloquear algumas páginas manualmente, a pedido dos utilizadores. Para isso você pode criar uma lista branca, autorizando o acesso aos sites manualmente inseridos nela.

Para isso, adicione uma nova ACL no ficheiro squidGuard.conf, adicionando as seguintes linhas próximo ao início do ficheiro:

```
dest white {
domainlist white/domains
urllist white/urls
}
```

No final do ficheiro, ao especificar o uso das ACLs, inclua o parâmetro “white” (sem a exclamação) antes dos demais, como em:

```
acl {
default {
pass white !porn !proxy all
redirect https://www.aprendendolinux.com
}
}
```

Com isso, o conteúdo da ACL “white” será processado primeiro e o acesso às páginas especificadas no ficheiro será liberado. Falta agora criar a pasta e os dois ficheiros citados na configuração:

```
#mkdir /var/lib/squidguard/db/white
#touch /var/lib/squidguard/db/white/domains
#touch /var/lib/squidguard/db/white/urls
```

Use o ficheiro “domains” para incluir domínios que devem ser permitidos por completo, como em “gdhn.com.br” e o ficheiro “urls” para incluir páginas ou seções isoladas, como em “gdhn.com.br/tutoriais/”, sempre um por linha.

Depois de editar os ficheiros, é necessário fazer com que o SquidGuard atualize a conversão das listas e reiniciar o Squid para que as alterações entrem em vigor, como em:

```
#squidGuard -C all
#squid -k reconfigure
```