SQUID 3 COM BLOQUEIO HTTPS

Igual a outros usuários, tive grandes problemas com o *Squid* em relação ao bloqueio de páginas com protocolo HTTPS, apesar da imensa quantidade de how-tos e tutoriais sempre ocorria algum problema ou relacionado aos certificados ou a compilação do Squid. Após pesquisas no Google e no próprio VOL, vou compartilhar o processo utilizado que tornou possível esta função.

Os testes foram realizados em uma VM rodando o *Debian Wheezy*com o *Squid 3* previamente instalado. A priori foi escolhida a versão 3.3.

Com o Squid 3 instalado, foi realizado o download da versão 3.3 diretamente do site squid-cache.org, decidi utilizar a pasta /usr/src para o download e demais processos:

```
# wget http://www.squid-cache.org/Versions/v3/3.3/squid-3.3.13.tar.gz
```

Descompactando o arquivo:

```
# tar xvzf squid-3.3.13.tar.gz
```

Navegue até a pasta:

```
# cd squid-3.3.13
```

A partir deste ponto, durante o processo de compilação iremos informar ao Squid quais opções serão setadas para possibilitar o bloqueio de páginas HTTPS, além destas serão setadas opções relacionadas as pastas padrões do Squid. Primeiramente resolva as dependências:

```
# apt-get build-dep squid3 && apt-get install build-essential libssl-dev
```

Após isso execute:

```
# ./configure --enable-icap-client --enable-ssl --enable-ssl-crtd --prefix=/usr --includedir=${prefix}/include --
```

```
mandir=${prefix}/share/man --infodir=${prefix}/share/info --sysconfdir=/etc --localstatedir=/var --libexecdir=/lib/squid3 --srcdir=. --datadir=/usr/share/squid3 --sysconfdir=/etc/squid3 --mandir=/usr/share/man --with-default-user=squid --with-cppunit-basedir=/usr --with-logdir=/var/log/squid3 --with-pidfile=/var/run/squid3.pid
```

> NOTA: Crédito para correção do comando acima ao membro Wanderton Carlos Vasconcelos Belém.

Ao término do processo de interrompa a execução do Squid:

```
# service squid3 stop
```

Execute o make:

```
# make all && make install
```

Adicione o usuário "squid" e modifique o proprietário da pasta /var/log/squid3:

```
# useradd squid && chown -R squid:squid /var/log/squid3
```

A opção "-R" refere-se à modificação de forma recursiva, todo novo arquivo criado em /var/log/squid3 será de propriedade do usuário squid.

Um dos principais objetivos de realizar a compilação tendo o Squid 3 já instalado é a possibilidade da cópia dos binários:

```
# mv /usr/sbin/squid3 /usr/sbin/squid3.old && mv /usr/sbin/squid /us/sbin/squid3
```

Crie na pasta do Squid 3 em /etc/squid3 uma pasta para criação dos certificados que depois serão importados para os navegadores dos clientes:

```
# cd /etc/squid3 && mkdir ssl_cert && cd ssl_cert
# openssl req -new -newkey rsa:1024 -days 365 -nodes -x509 -keyout myCA.pem -out myCA.pem
```

Durante o processo de compilação do Squid foi setada a opção "--libexecdir=/lib/squid3" nesta pasta estão os arquivos necessários à execução, um destes arquivos, ssl_crtd será usado para a criação de certificados dinâmicos:

```
# /lib/squid3/ssl_crtd -c -s /var/lib/ssl_db -M 4MB
```

Mude o proprietário do arquivo:

```
# chown -R squid:squid /var/lib/ssl_db
```

A partir deste ponto o Squid 3 estará apto a realizar os bloqueios na porta 443, lembrando que a partir da versão 3.2 não se usa mais a opção transparent e sim a intercept:

```
http_port 3128 intercept
https_port 3127 intercept ssl_bump generate_host_certificates=on
dynamic_cert_mem_cache_size=4MB cert=/etc/squid3/ssl_cert/myCA.pem
ssl_bump none localhost
ssl-bump server-first all
sslcrtd_program /lib/squid3/ssl_crtd -s /var/lib/ssl_db -M 4 MB
sslcrtd_children 5
```

Adicione ao script do firewall as linhas:

```
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 443 -j REDIRECT --to-port 3127
iptables -I INPUT -p tcp -m tcp --dport 3127 -j ACCEPT
```

Reinicie a execução do Squid 3:

```
# service squid3 restart
```

Para aqueles que usam o Sarg é necessário modificar o sarg.conf, atualizando a TAG access_log:

```
access_log /var/log/squid3/access.log
```

Com isso o Squid 3 poderá realizar o bloqueio do tão famigerado HTTPS. Espero que esta dicas ajudem à todos aqueles que passam pelo problema do HTTPS e àqueles que puderem contribuir com alguma melhora neste pequeno how-to, fiquem à vontade e sirvam-se.

O conhecimento sempre é livre!