Configuring transparent proxy for HTTPS protocol in Squid 2.6

(Steps tested on Squid 2.6 running at RHEL 5.0)

Configuring transparent proxy on port 80 fis simple whereas some extra configuration is required to use transparent proxy with HTTPS protocol.

Why Needed?

This configuration is required because if we block a website like www.facebook.com it cannot be accessed by users on port 80 via http protocol but site remains still accessible via HTTPS (If NAT and IP Forwarding is enabled).
Thus bypassing our security measures.

STEPS:

Below are the steps needed to configure HTTPS protocol to use transparent proxy.

1- Create two iptables rules (First rule might already be present then create second rule)

```
#iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128
#iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 3130
```

Note: In above example eth0 is local network Interface, adjust it according to your topology)

2- Generate Certificate and public key/ private key

Install rpm crypto-utils

```
#rpm -ivh crypto-utils-2.3
#genkey -days 365 squidserver.hostname.com
```

Note: Check your system hostname and enter your hostname here e.g #genkey -days 365 squidserver.corvit.com)
Hit next.
Select number of bits for data encryption. Default is 1024. This command will generate random bits.
Generate the certificate. This may take little bit time.
Option dispays Generate CSR
Select No
Give details of your certificate
Hit next
Do nothing and Hit next
It is suggested NOT to use the passphrase for key, because if you assigns passphrase to key then along with public key we need to share passphrase.

The certificate is created and the Certificate and key are stored at /etc/pki/tls/certs/ and /etc/pki/tls/private/

3 - In squid.conf make necessary changes like below

```
http_port 3128 transparent

https_port 3130 transparent cert=/etc/pki/tls/certs/squidserver.hostname.com.cert key=/etc/pki/tls/private/squidserver.hostname.com.key
```

Restart squid service and now when the client tries to access a https website they will get message that secure connection failed and at end of message there is a hyperlink "YOU CAN ADD AN EXCEPTION" click on it, then click on ADD EXCEPTION, click GET CERTIFICATE and click CONFIRM SECURITY EXCEPTION. your website will be opened if there is no rule denying it or will get blocked if blocking ACL exists for that site.

You have to add a certificate only one time when the user tries to access https website for the first time, second time the site opens normally without asking for exception addition.

If you want to get rid of the hassle of manually exception adding in the browser every time they visit a new https website then you will have to get your SSL certificate approved by a company like verisign or other CA that the browser trusts.

Above doc is prepared by Ahmad Fiaz which can be reached at fiaz_gullgee@yahoo.com