Table of Contents

It is sometimes difficult to add https site into the "white" or "black" list by its IP address as many widely accessed sites use CDN (Content Delivery Networks) or use various methods of geographic reservation and balancing. As a result, site's addresses returned by nslookup or dig commands can be time dependent, or vary with the DNS server used, or be dependent on other factors. This list may include hundreds or thousands addresses in case of CDS. And other sites can be available by these addresses as well.

The blocking or access by the name of SSL certificate of such site can help in this case[1]. These certificates are issued by trusted companies for the particular name and typically are not free. Most browsers block the site access if its name and the name on its certificate are different.

One can check the name for which the certificate is issued (CN, Common Name, etc.) in a browser: in https page properties:

Alternatively, one can execute the following CenOS instruction:

```
openssl s_client -connect www.facebook.com:443
```

Here www.facebook.com is the name of https site in question,
and then find the record 0 in the returned chain of certificates:
Certificate chain 0 s:/C=US/ST=CA/L=Menlo Park/O=Facebook, Inc./CN=*.facebook.com

Here *.facebook.com - is the name to use.

[1] This option is available on symmetric traffic only