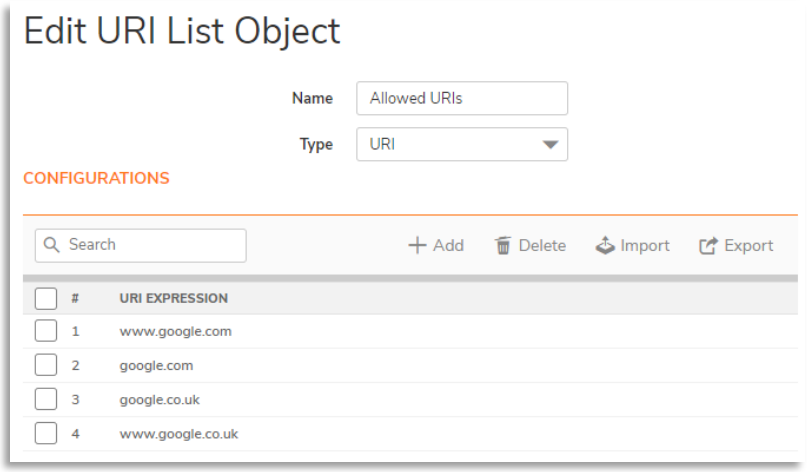
SonicWALL CFS Forcing Safe Search without DPI-SSL

To enable Safe Search Without DPI-SSL using CFS there are two ways depending on whether or not you are running an Internal DNS. This is for Google, YouTube and Bing.

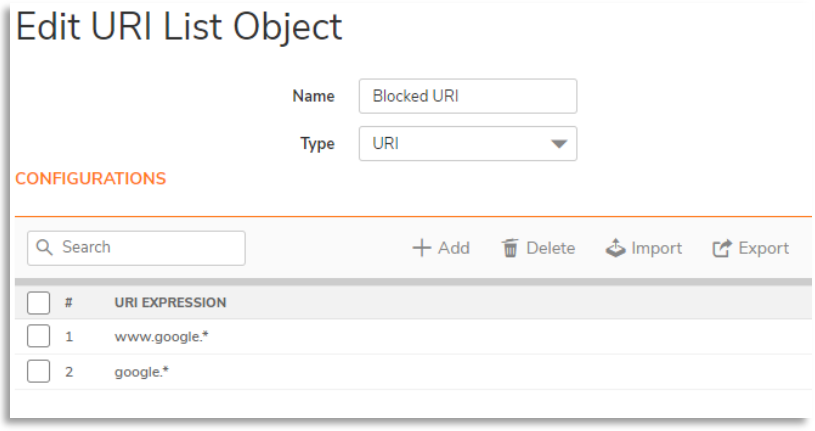
N.B. Make sure you are licenced for CFS and it is enabled in the **Policy/Security Services/Content Filter** section.

Setting up using the SonicWall as a DNS Proxy Server

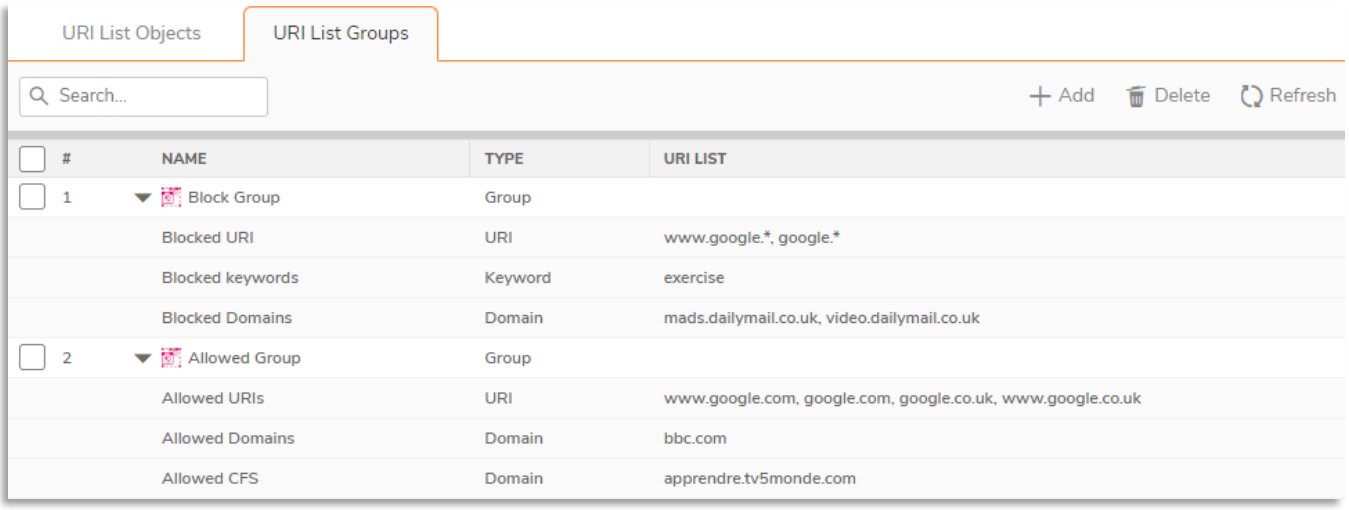
1. Setup CFS to Block the Safe Search from other countries other than .com or .co.uk (you can change the settings according to your default country).
   To do this you need to go to **Object/Match Objects/URI Lists** and add an Allowed URI List object as below:



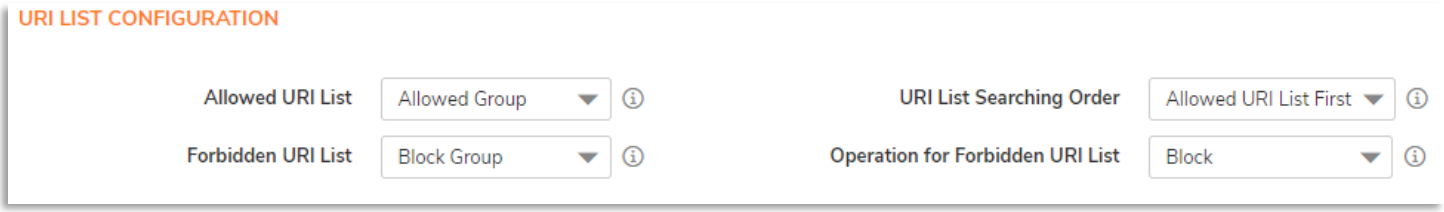
2. Create another URI List Object but this time name it Blocked URI.



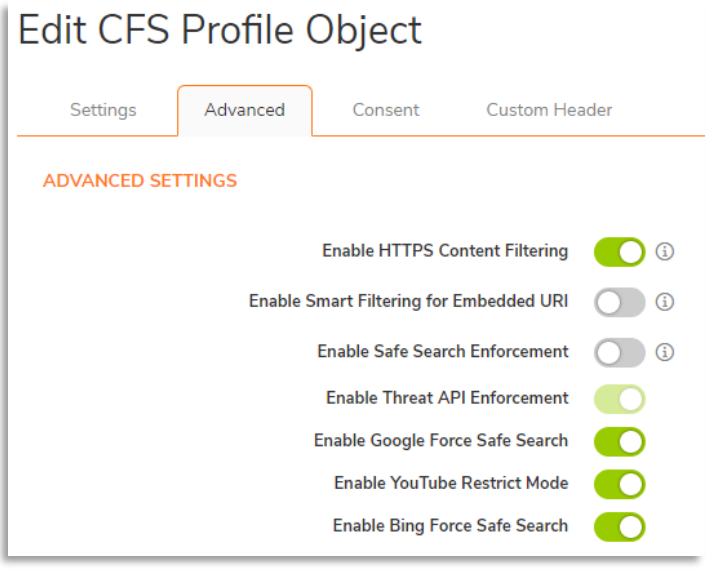
3. You can then add these to other **URI List Groups** if needed like in the below example.



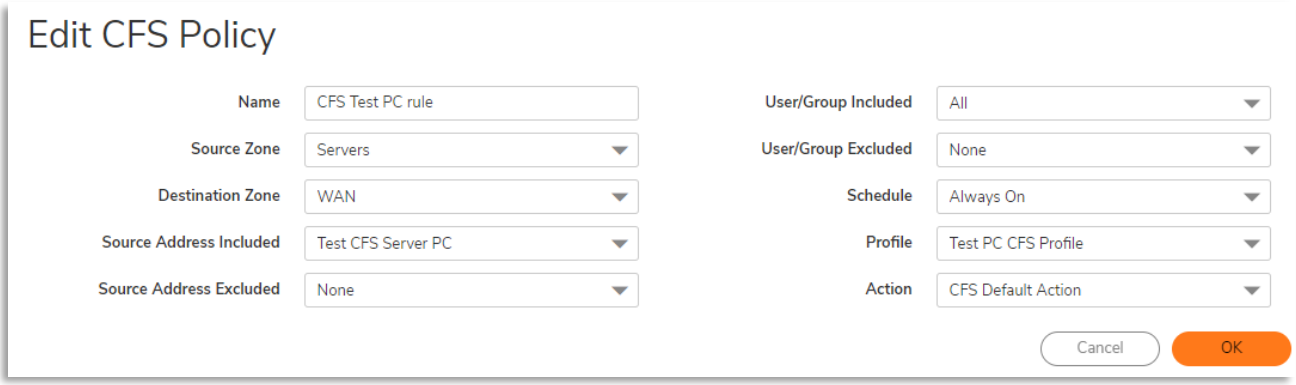
4. Browse to **Object/Profile Objects/Content Filter** and edit the profile to which you want to apply the Safe Search. Based on the settings I've used, set the options as below choosing the Allow and Block groups and Allowed URI for the Searching Order.



5. In the Advanced tab, set things as in the below screenshot. You will notice that I've selected Safe Search but this won't work correctly with all browsers and devices until we add some more settings.

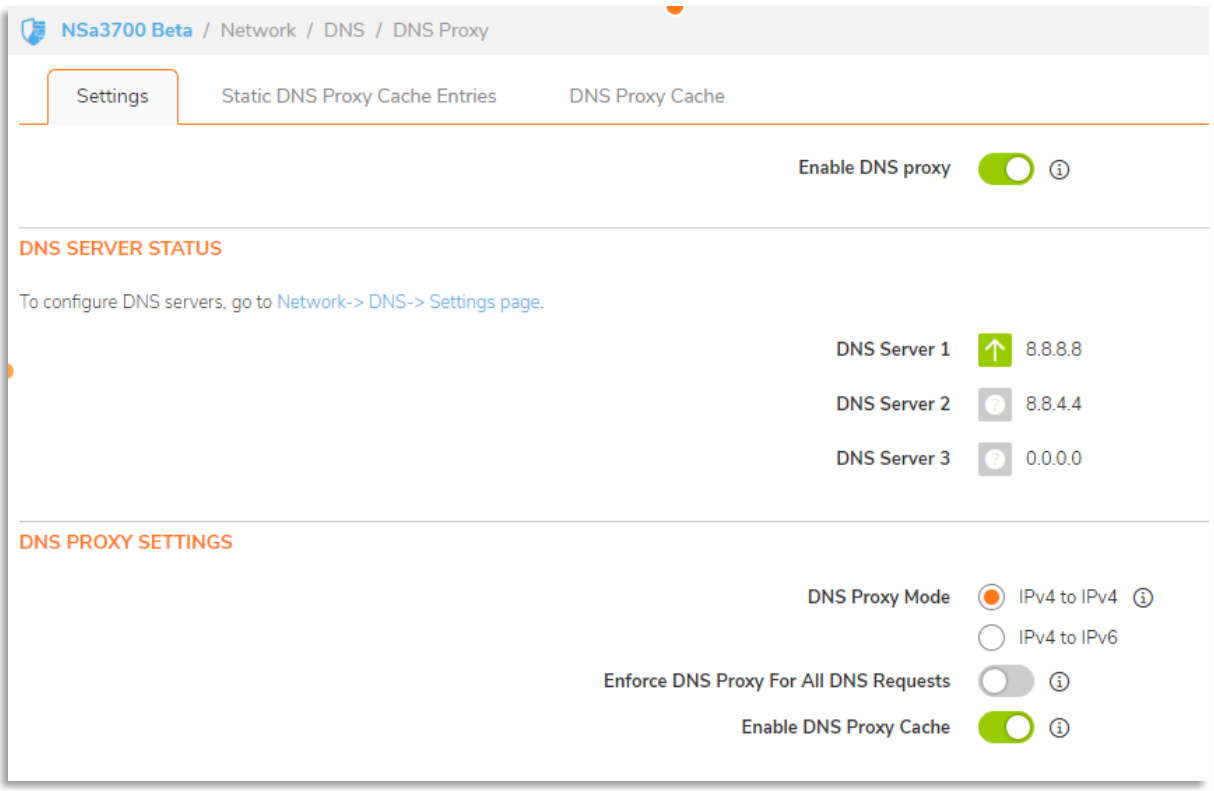


6. Make sure that under **Policy/Rules and Policies/Content Filter Rules** you have set the correct Source and Profile to use. In this example I'm testing from a test pc in my Servers zone.

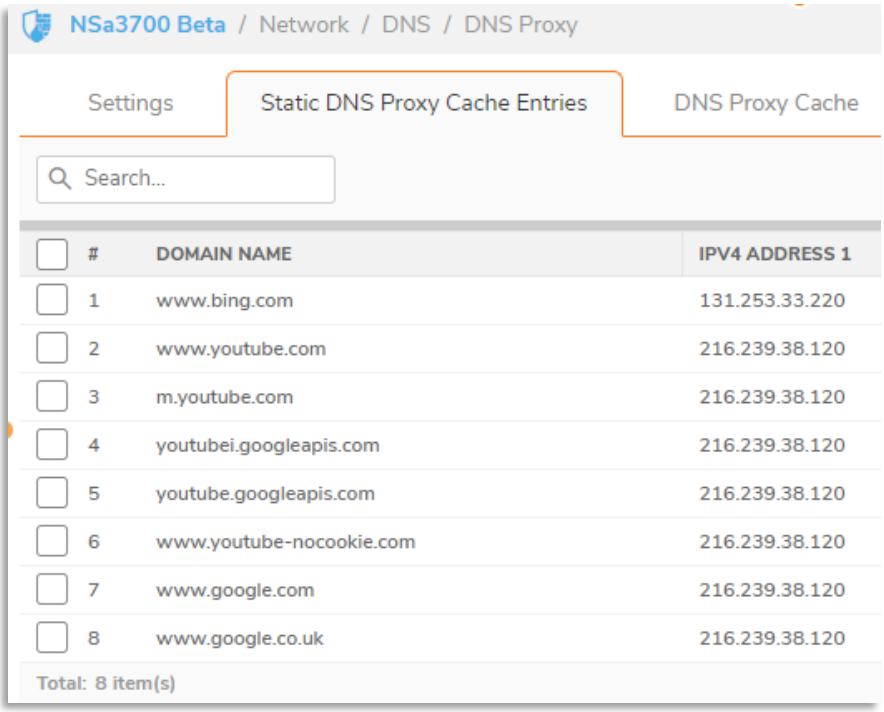


7. **NB. If you have an Internal Windows DNS server, go to the "Setting up with a Windows DNS Server" after step 13.**

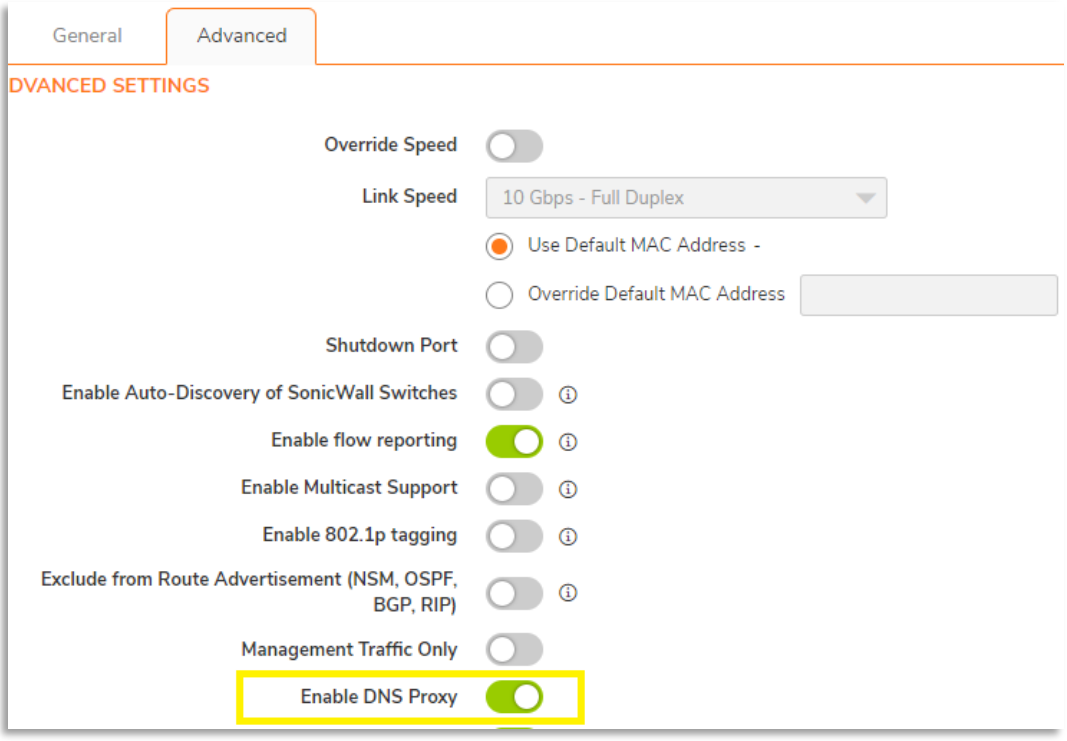
   If not using an internal DNS server, go to **Network/DNS/DNS Proxy** and set as below. In my example I'm only going to enforce this on one zone so I've left the **Enforce DNS Proxy For All DNS Requests** disabled but if you want to use across the whole firewall you can enabled this.



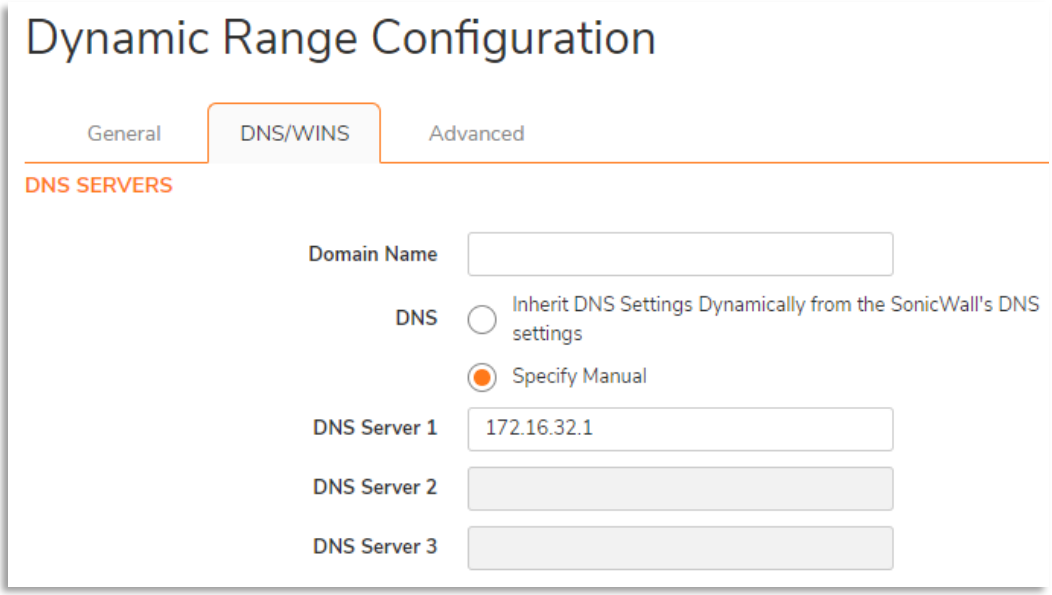
8. Next, on the tab called **Static DNS Proxy Cache Entries,** select **+ ADD** and add the entries as in the below image. I have added this list at the end of this document so you can copy and paste them. This will redirect the DNS requests to forcesafesearch.google.com, for Google and the Youtube entries and strict.bing.com for Bing.



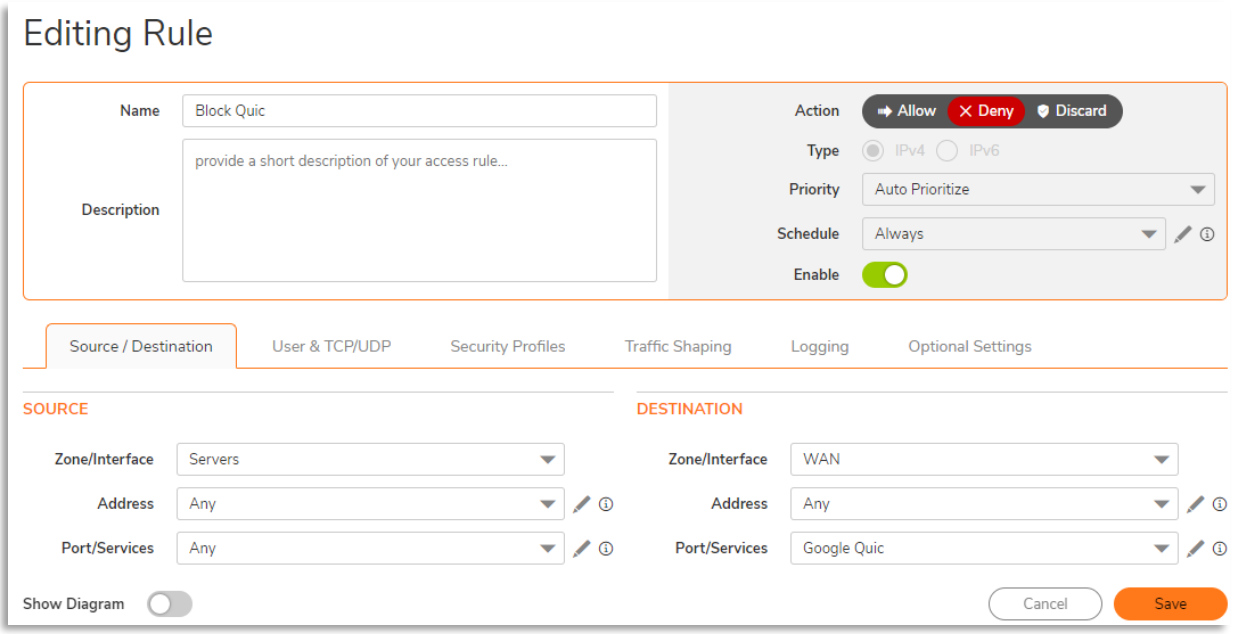
9. Now we need to enable DNS Proxy on the Interface as below:



10. Now when you set up DHCP on the SonicWall for that interface, it will auto populate the DNS address as the SonicWall Interface IP.

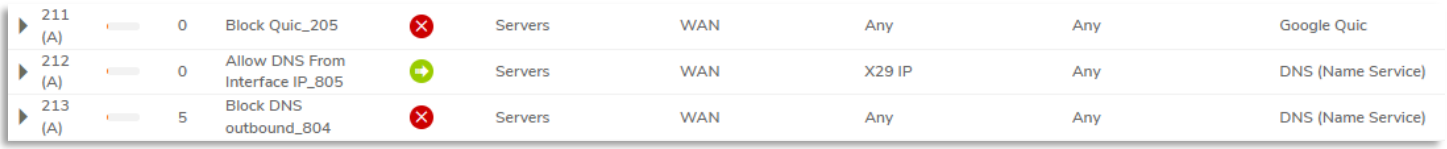


11. We now need to create an Access rule to block outbound **Google Quic Protocol (UDP 443)** as below for traffic destined for the WAN from the zone you want to apply the CFS to.



12. The final things that we need to do at this point are to create two firewall rules: the first to allow DNS traffic from the interface IP to the WAN and then a second rule to block all other DNS traffic to the WAN. Without this step, users can just change their DNS settings to get round the SafeSearch.

    You will need to create two rules as per the screenshot below – in our example the interface in use is X29 however this will likely be different for your setup:



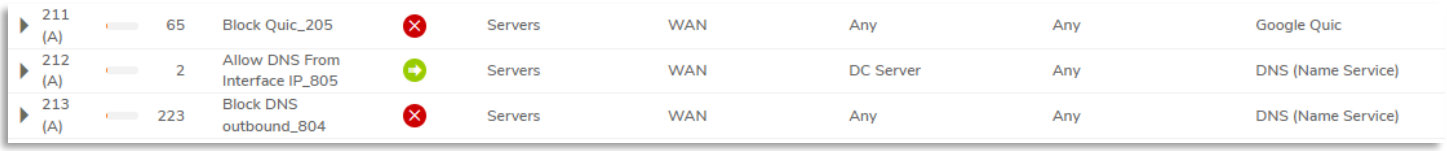
211 (A)	0	Block Quic_205	Servers	WAN	Any	Any	Google Quic
212 (A)	0	Allow DNS From Interface IP_805	Servers	WAN	X29 IP	Any	DNS (Name Service)
213 (A)	5	Block DNS outbound_804	Servers	WAN	Any	Any	DNS (Name Service)

13. After setting this up make sure to clear the cache on the DNS server and clients if needed.

Now if you browse to Google.com or Google.co.uk, Bing.Com or Youtube.com Safe Search will be enforced.

Setting up with a Windows DNS Server

1. As with the internal DNS setup earlier in this guide you will need to add three firewall rules. The first is as per step 11 of the guide above: to block **Google Quic Protocol (UDP 443)**. The second rule is to allow DNS traffic from your DNS server to the WAN. The third rule is to block all other DNS traffic to the WAN from your network.

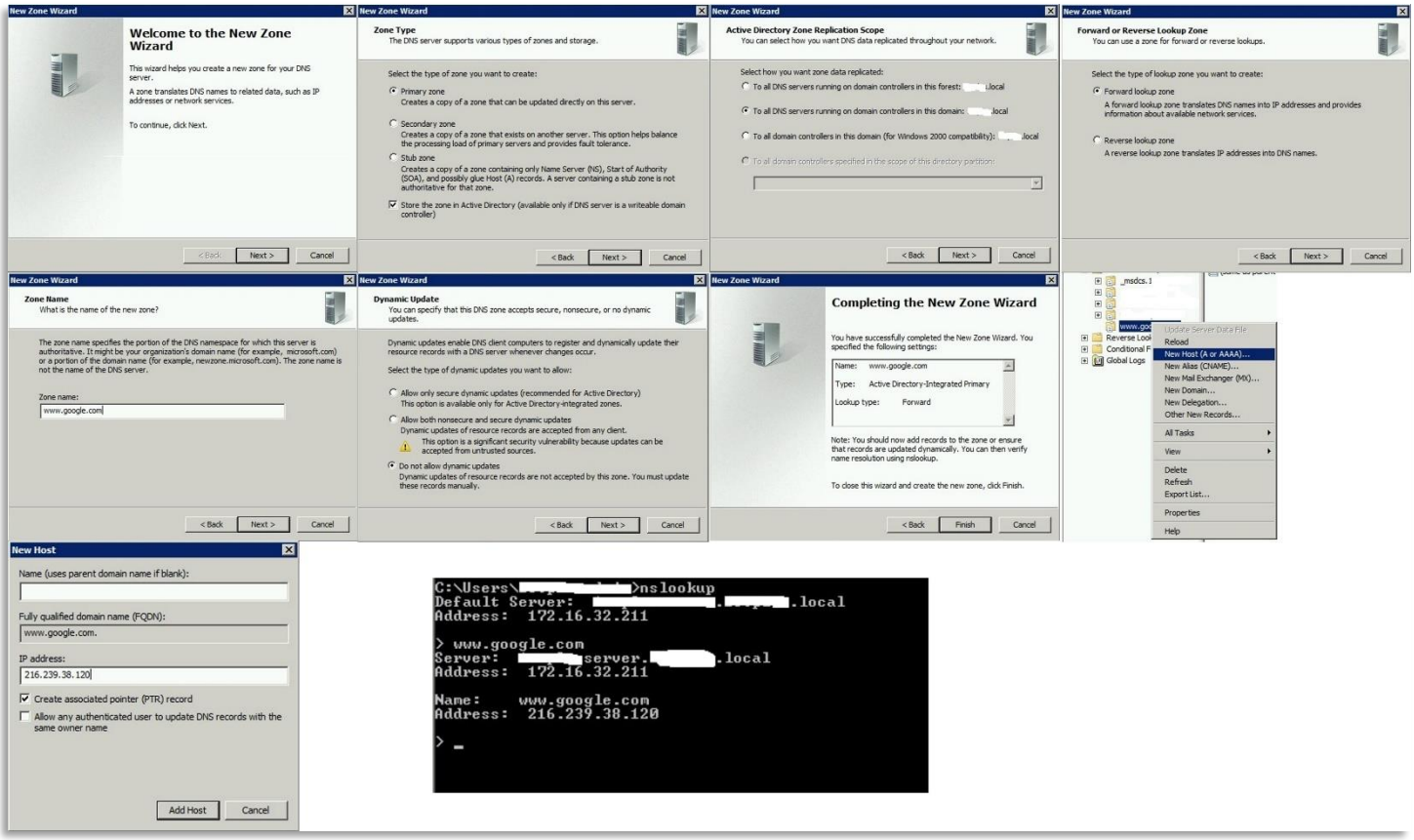


211 (A)	65	Block Quic_205	Servers	WAN	Any	Any	Google Quic
212 (A)	2	Allow DNS From Interface IP_805	Servers	WAN	DC Server	Any	DNS (Name Service)
213 (A)	223	Block DNS outbound_804	Servers	WAN	Any	Any	DNS (Name Service)

2. If you are using an Internal Windows DNS and DHCP Server you will need to add Forward Lookup Zones for the entries below:

All of the Google and YouTube Records need to point to 216.239.38.120 (they will be then redirected to forcesafesearch.google.com and restrict.youtube.com <u>don't add these to the DNS</u> just the below entries in bold)
www.google.com
www.google.co.uk
www.youtube.com
m.youtube.com
youtubei.googleapis.com
youtube.googleapis.com
www.youtube-nocookie.com
and the **www.bing.com** needs to point to 131.253.33.220 (which will be redirected to strict.bing.com <u>don't add this to the DNS</u>)

3. Here is how you set it one of the Forward Lookup Zones on the DNS Server as an example for www.google.com, you will need to repeat this procedure for all the mentioned above.



4. After setting this up, make sure to clear the cache on the DNS server and clients if needed.