

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:

Edit URI List Object

Name: Allowed URIs
Type: URI

CONFIGURATIONS

| # | URI EXPRESSION |
|---|------------------|
| 1 | www.google.com |
| 2 | google.com |
| 3 | google.co.uk |
| 4 | www.google.co.uk |

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

Edit URI List Object

Name: Blocked URI
Type: URI

CONFIGURATIONS

| # | URI EXPRESSION |
|---|----------------|
| 1 | www.google.* |
| 2 | google.* |

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

| URI List Objects | | URI List Groups | | |
|--|---|------------------|---------|--|
| <input type="text" value="Search..."/> + Add Delete Refresh | | | | |
| <input type="checkbox"/> | # | NAME | TYPE | URI LIST |
| <input type="checkbox"/> | 1 | ▼ Block Group | Group | |
| | | Blocked URI | URI | www.google.*, google.* |
| | | Blocked keywords | Keyword | exercise |
| | | Blocked Domains | Domain | mads.dailymail.co.uk, video.dailymail.co.uk |
| <input type="checkbox"/> | 2 | ▼ Allowed Group | Group | |
| | | Allowed URIs | URI | www.google.com, google.com, google.co.uk, www.google.co.uk |
| | | Allowed Domains | Domain | bbc.com |
| | | Allowed CFS | Domain | apprendre.tv5monde.com |

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.

URI LIST CONFIGURATION

| | | | |
|--------------------|-------------------|----------------------------------|----------------------------|
| Allowed URI List | Allowed Group ▼ ⓘ | URI List Searching Order | Allowed URI List First ▼ ⓘ |
| Forbidden URI List | Block Group ▼ ⓘ | Operation for Forbidden URI List | Block ▼ ⓘ |

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.

Edit CFS Profile Object

Settings **Advanced** Consent Custom Header

ADVANCED SETTINGS

- Enable HTTPS Content Filtering ⓘ
- Enable Smart Filtering for Embedded URI ⓘ
- Enable Safe Search Enforcement ⓘ
- Enable Threat API Enforcement
- Enable Google Force Safe Search
- Enable YouTube Restrict Mode
- Enable Bing Force Safe Search

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.

Edit CFS Policy

| | | | |
|-------------------------|---|---------------------|--|
| Name | <input type="text" value="CFS Test PC rule"/> | User/Group Included | <input type="text" value="All"/> |
| Source Zone | <input type="text" value="Servers"/> | User/Group Excluded | <input type="text" value="None"/> |
| Destination Zone | <input type="text" value="WAN"/> | Schedule | <input type="text" value="Always On"/> |
| Source Address Included | <input type="text" value="Test CFS Server PC"/> | Profile | <input type="text" value="Test PC CFS Profile"/> |
| Source Address Excluded | <input type="text" value="None"/> | Action | <input type="text" value="CFS Default Action"/> |

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.

NSa3700 Beta / Network / DNS / DNS Proxy

Settings Static DNS Proxy Cache Entries DNS Proxy Cache

Enable DNS proxy ⓘ

DNS SERVER STATUS

To configure DNS servers, go to [Network->DNS->Settings page](#).

| | | |
|--------------|-------------------------------------|---------|
| DNS Server 1 | <input checked="" type="checkbox"/> | 8.8.8.8 |
| DNS Server 2 | <input type="checkbox"/> | 8.8.4.4 |
| DNS Server 3 | <input type="checkbox"/> | 0.0.0.0 |

DNS PROXY SETTINGS

| | |
|--|---|
| DNS Proxy Mode | <input checked="" type="radio"/> IPv4 to IPv4 ⓘ |
| | <input type="radio"/> IPv4 to IPv6 |
| Enforce DNS Proxy For All DNS Requests | <input type="checkbox"/> ⓘ |
| Enable DNS Proxy Cache | <input checked="" type="checkbox"/> ⓘ |

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.

NSa3700 Beta / Network / DNS / DNS Proxy

Settings **Static DNS Proxy Cache Entries** DNS Proxy Cache

Search...

| # | DOMAIN NAME | IPV4 ADDRESS 1 |
|---|--------------------------|----------------|
| 1 | www.bing.com | 131.253.33.220 |
| 2 | www.youtube.com | 216.239.38.120 |
| 3 | m.youtube.com | 216.239.38.120 |
| 4 | youtubei.googleapis.com | 216.239.38.120 |
| 5 | youtube.googleapis.com | 216.239.38.120 |
| 6 | www.youtube-nocookie.com | 216.239.38.120 |
| 7 | www.google.com | 216.239.38.120 |
| 8 | www.google.co.uk | 216.239.38.120 |

Total: 8 item(s)

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

General **Advanced**

ADVANCED SETTINGS

Override Speed

Link Speed 10 Gbps - Full Duplex

Use Default MAC Address -

Override Default MAC Address

Shutdown Port

Enable Auto-Discovery of SonicWall Switches

Enable flow reporting

Enable Multicast Support

Enable 802.1p tagging

Exclude from Route Advertisement (NSM, OSPF, BGP, RIP)

Management Traffic Only

Enable DNS Proxy

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.

Dynamic Range Configuration

General **DNS/WINS** Advanced

DNS SERVERS

Domain Name

DNS Inherit DNS Settings Dynamically from the SonicWall's DNS settings
 Specify Manual

DNS Server 1

DNS Server 2

DNS Server 3

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.

Editing Rule

Name

Description

Action Allow Deny Discard

Type IPv4 IPv6

Priority

Schedule

Enable

Source / Destination User & TCP/UDP Security Profiles Traffic Shaping Logging Optional Settings

SOURCE

Zone/Interface

Address

Port/Services

DESTINATION

Zone/Interface

Address

Port/Services

Show Diagram

Cancel Save

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) |

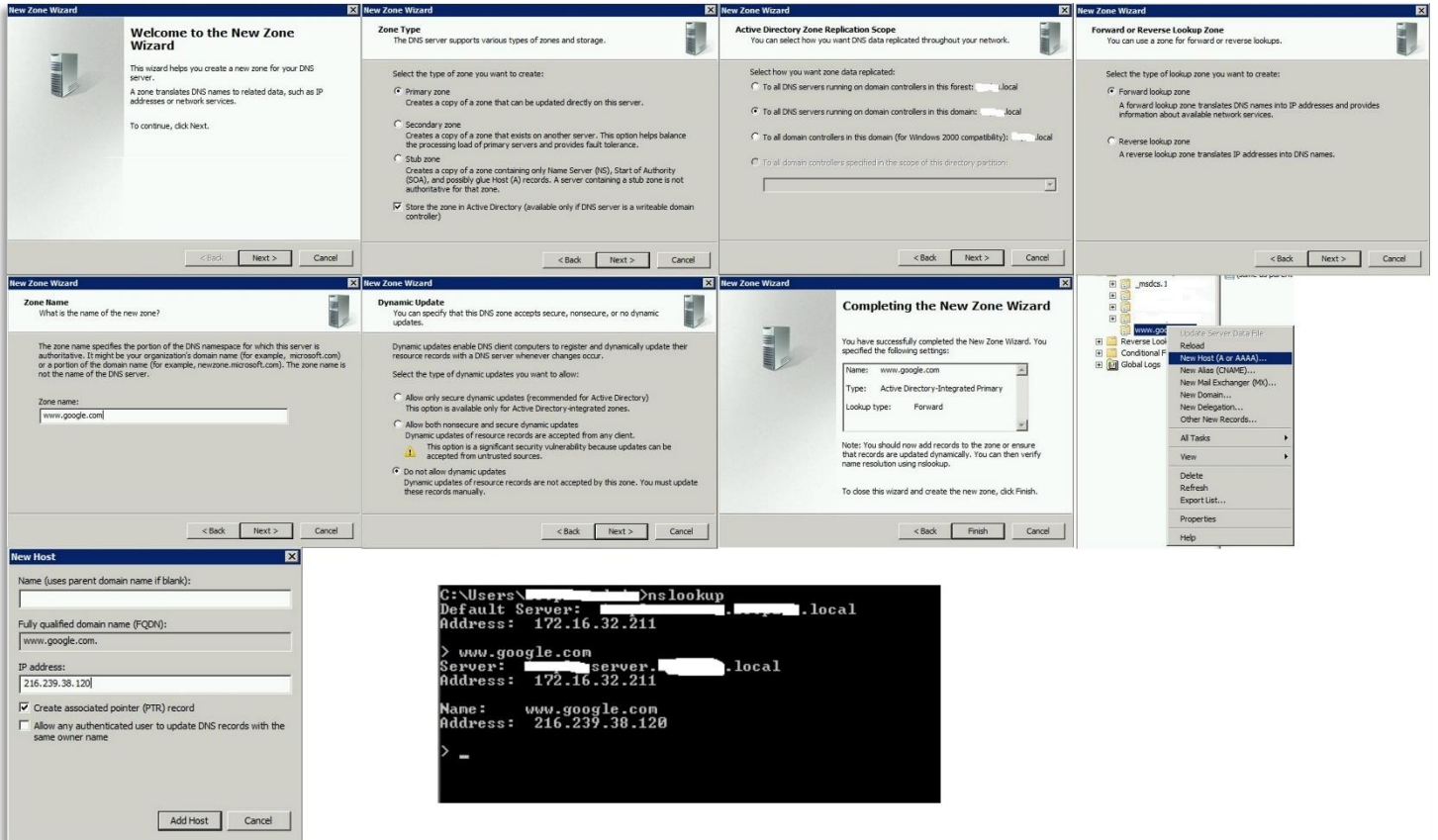
2. If you are using an Internal Windows DNS and DHCP Server you will need to add Forward Lookup Zones for the entries below:

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 don't add these to the DNS 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 don't add this to the DNS)

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.