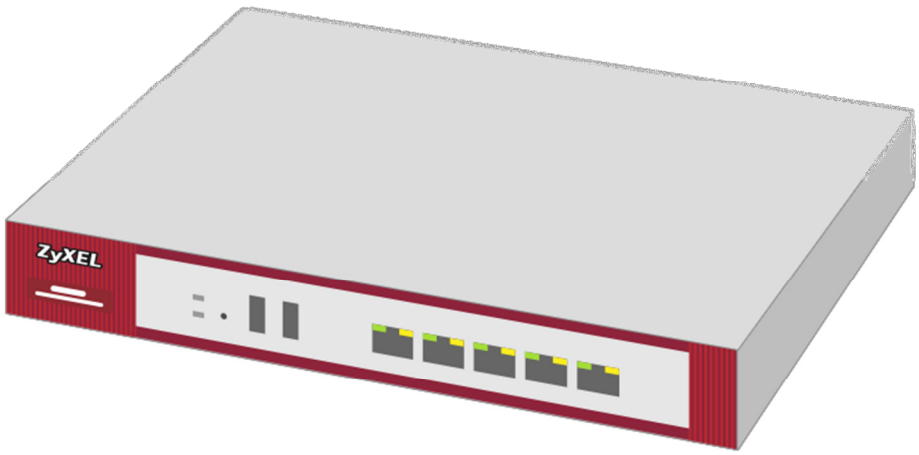
ZYXEL
Your Networking Ally



SafeSearch mit Hilfe von CNAME-Records

Zyxel USG Firewall-Serie
ab Firmware-Version 4.20

Knowledge Base KB-3679
Juni 2017

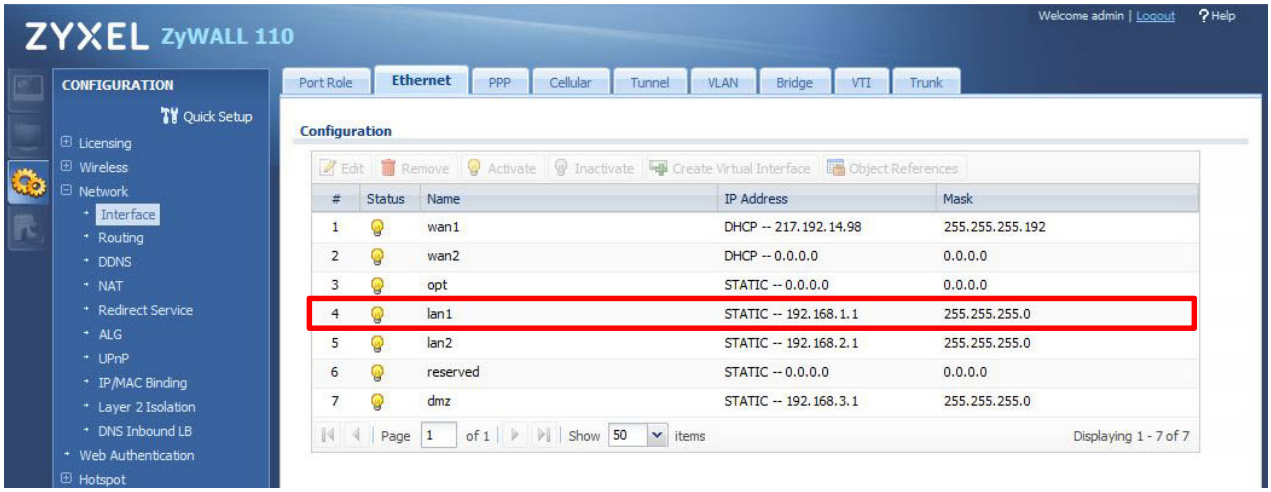
GOOGLE SAFESEARCH EINRICHTEN

Während das Filtern von WEB-Sites über den Content Filter einfach zu realisieren ist, ist das Entfernen von ungeeigneten Bildern aus den Resultaten von Suchmaschinen mit wesentlich mehr Aufwand verbunden. Im Zuge von „Schulen ans Internet“ bieten die Suchmaschinen Google und Bing eine Möglichkeit, um den SafeSearch Modus auf Netzwerkeben zu aktivieren. Der Client hat in diesem Fall keine Möglichkeit, diesen Modus zu deaktivieren. So lassen sich Bildabfragen ohne grossen Aufwand filtern.

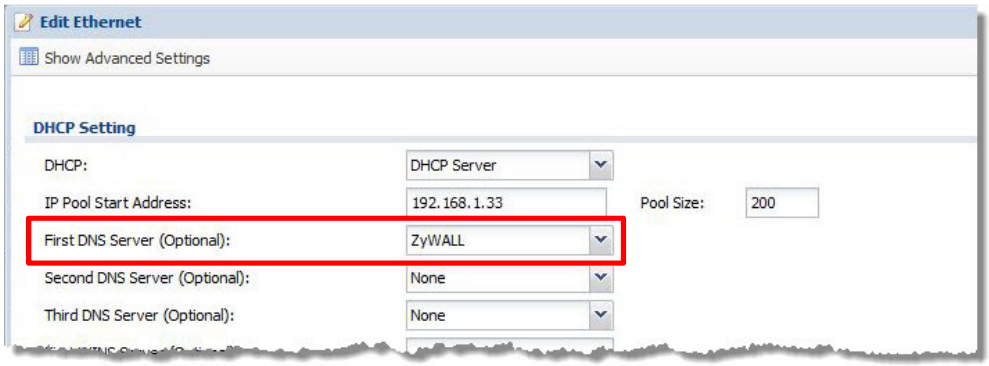
In diesem Beispiel zeigen wir, wie Google SafeSearch auf Netzwerkbasis verwendet werden kann. SafeSearch ist hier für alle Clients im LAN1 aktiviert.

Zuerst muss sichergestellt werden, dass die LAN1 Zone den Zywall DNS-Server verwendet:

Configuration>Network>Interface>Ethernet>lan1

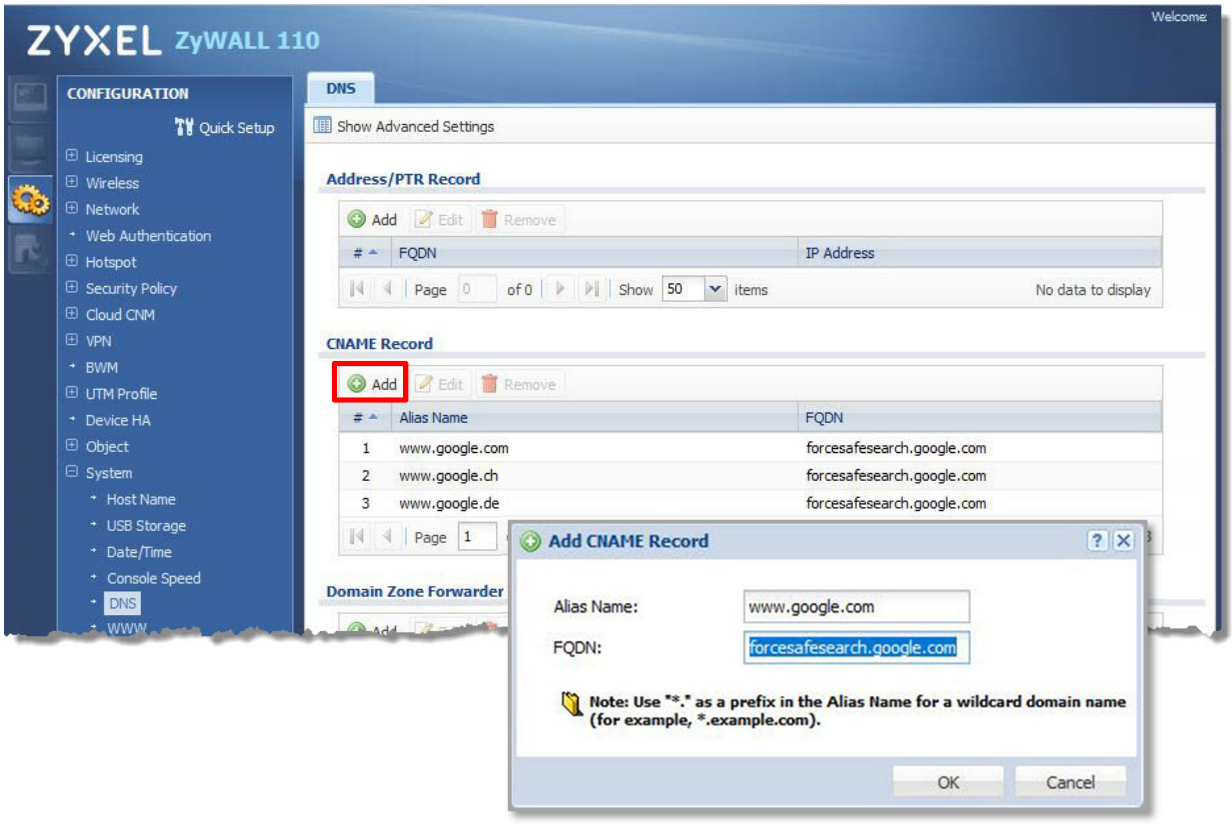


Dazu wird als **First DNS Server: ZyWALL** gewählt



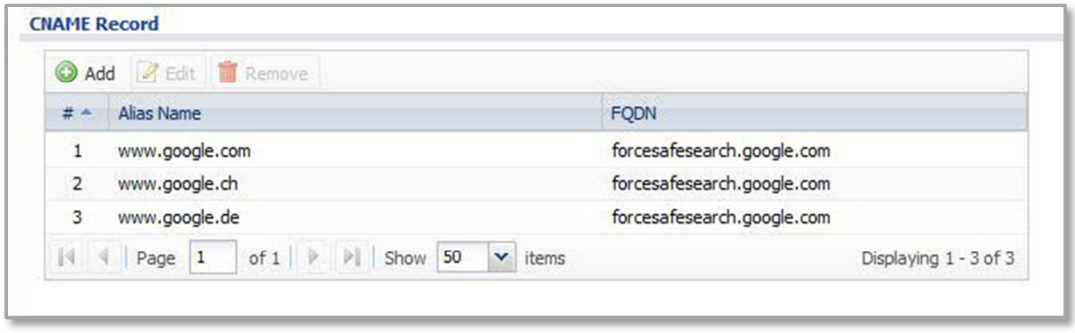
Als nächstes werden in den DNS-Einstellungen die notwendigen Umleitungen erstellt. Dazu werden die CNAME-Records verwendet.

Configuration>System>DNS>CNAME Record

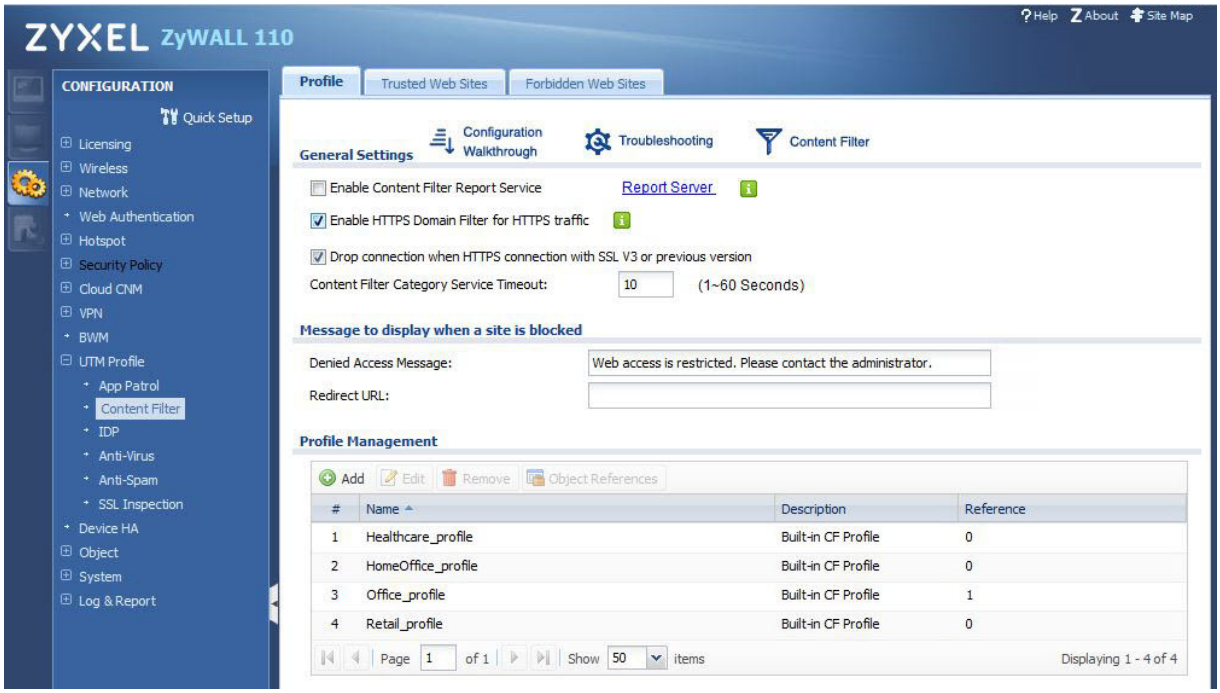


Für jede gewünschte Länder-Domäne muss ein CNAME-Record erfasst werden.

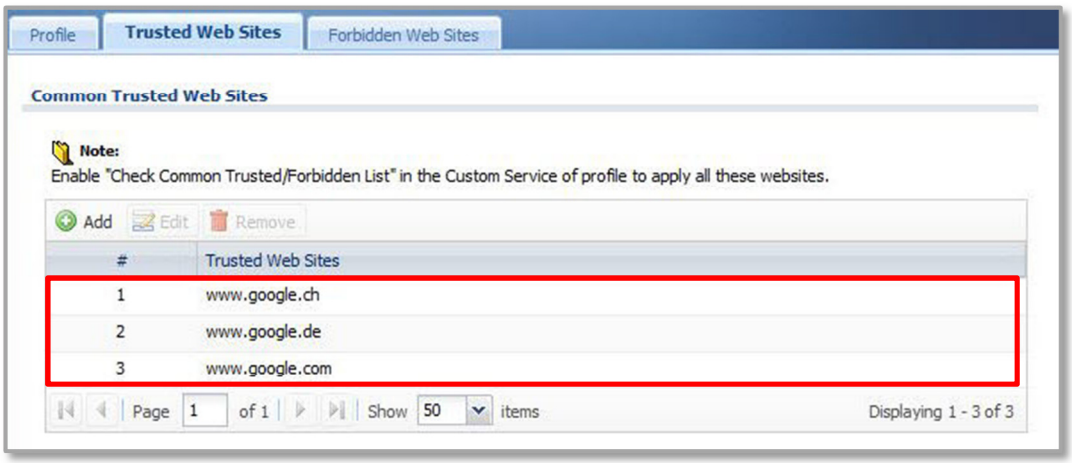
Alias Name	FQDN
www.google.com	forcesafesearch.google.com
www.google.ch	forcesafesearch.google.com
www.google.de	forcesafesearch.google.com



Damit alle anderen Länder gesperrt werden, muss ein entsprechendes Content-Filter-Profil erstellt werden.

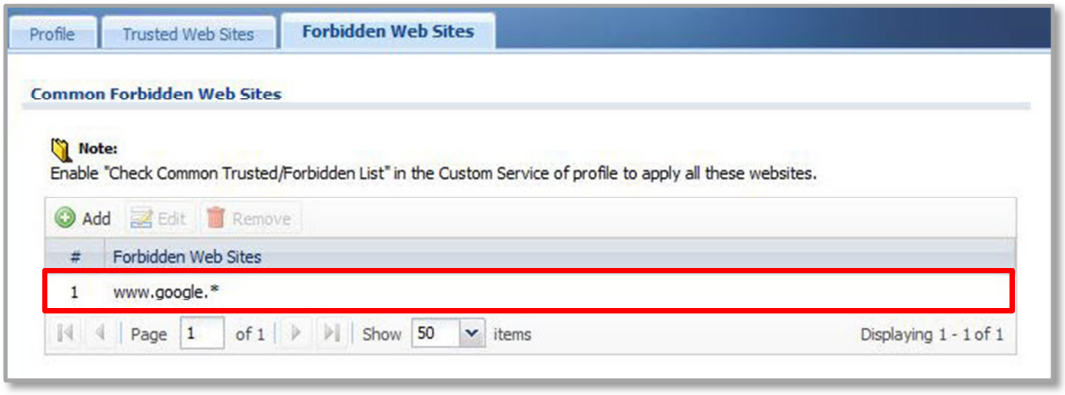


Unter ***Configuration>UTM Profil>Content Filter>Trusted Web Sites*** werden nun alle zugelassenen Adressen erfasst und mit **Apply** bestätigt.

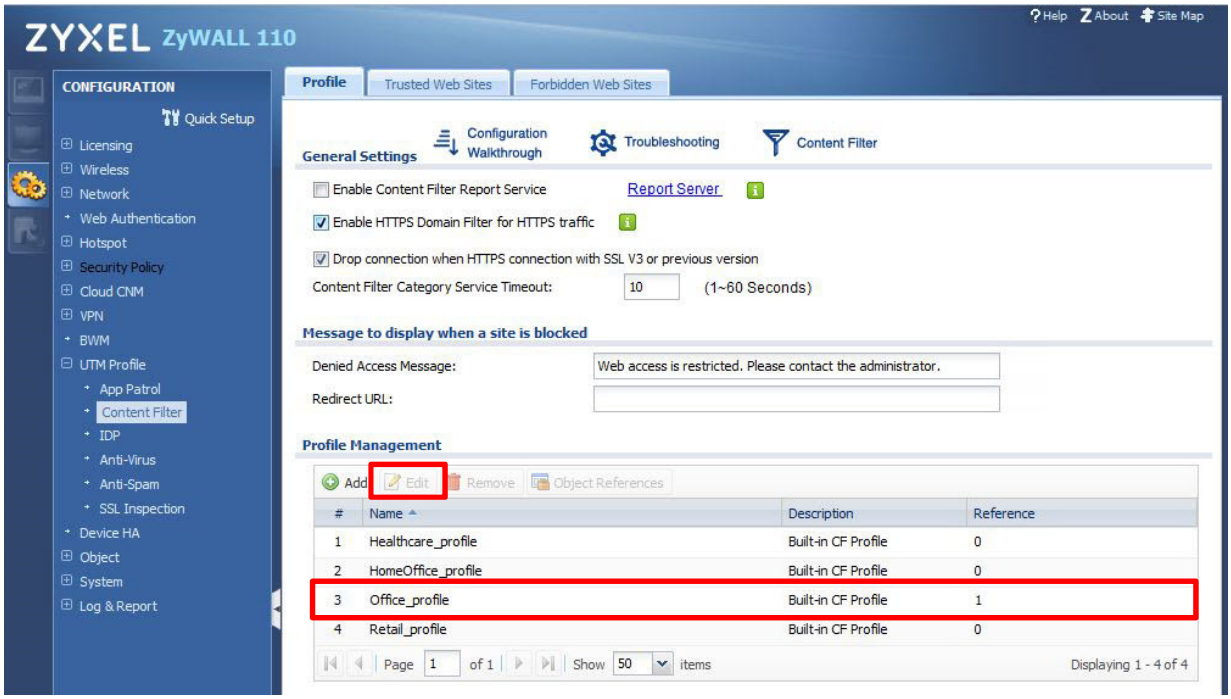


Für alle anderen Länder wird eine Regel unter ***Forbidden Web Sites*** erstellt, die den Zugriff für alle nicht zugelassenen Google Domains verhindert:

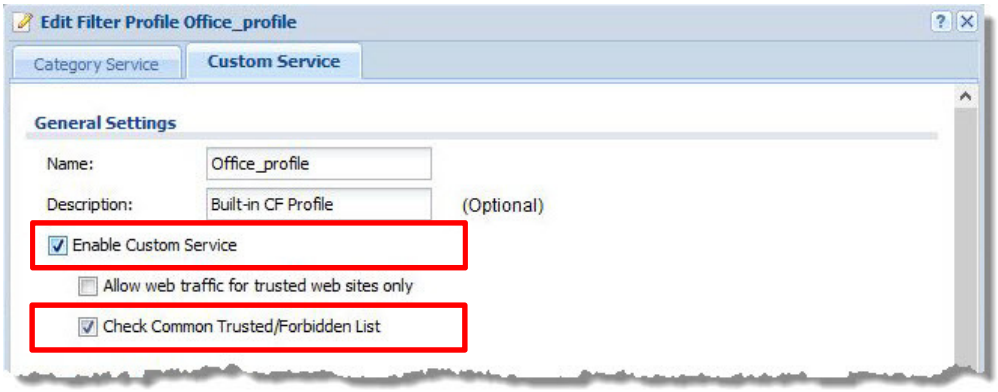
www.google.*



Damit die soeben erstellte Regel zur Anwendung kommt, muss diese im Content-Filter-Profil angegeben werden. Unter ***Configuration>UTM Profil>Content Filter Profile*** wird das gewünschte Profil geöffnet, hier z.B. **Office_profile**.

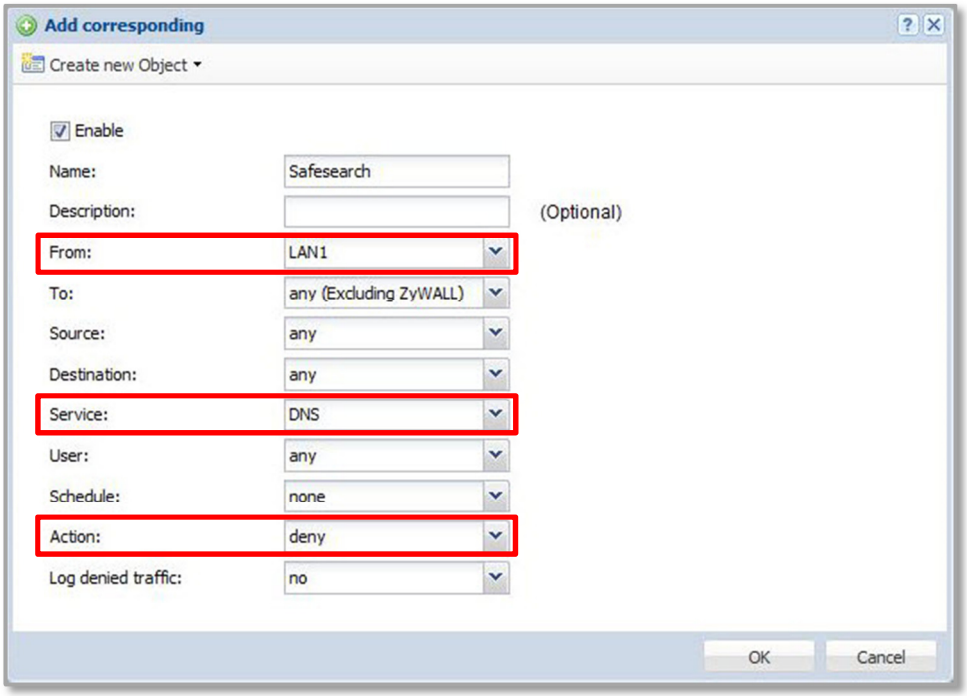


Unter ***Custom Service*** muss nun die die Opton **Enable Custom Service** und **Check Common Trusted/Forbidden List** aktiviert werden

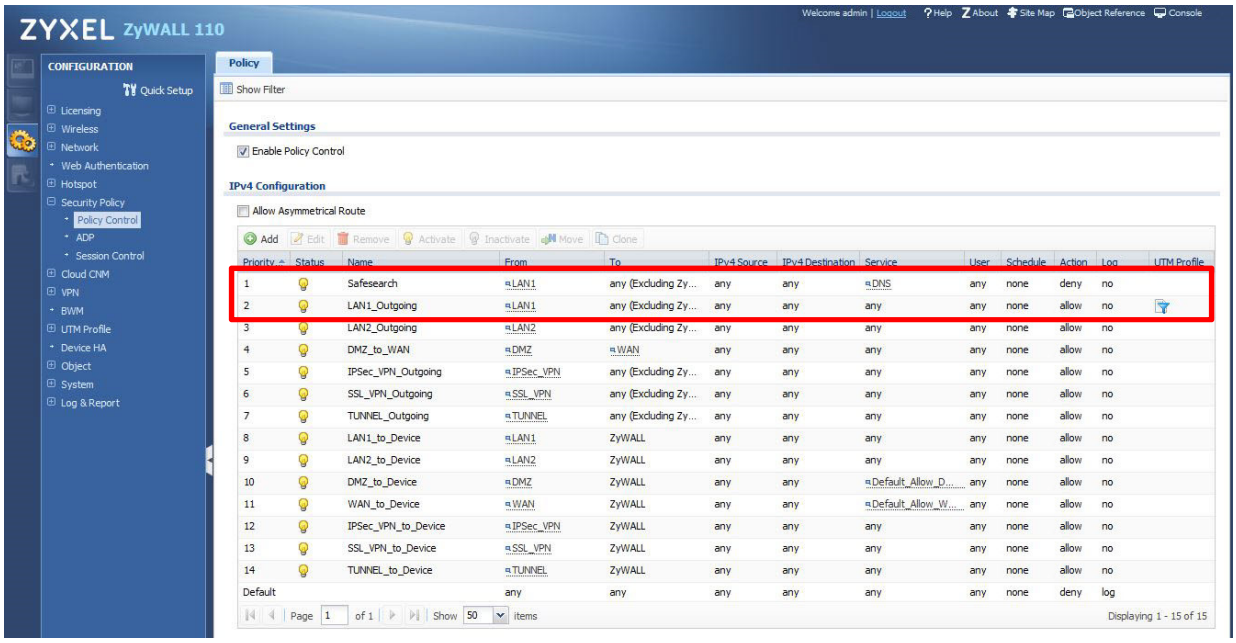


Um zu verhindern, dass ein anderer DNS-Server als die USG verwendet werden kann, wird die DNS-Service-Gruppe aus der LAN-Zone geblockt. Dazu kann die vordefinierte **DNS**-Gruppe verwendet werden.

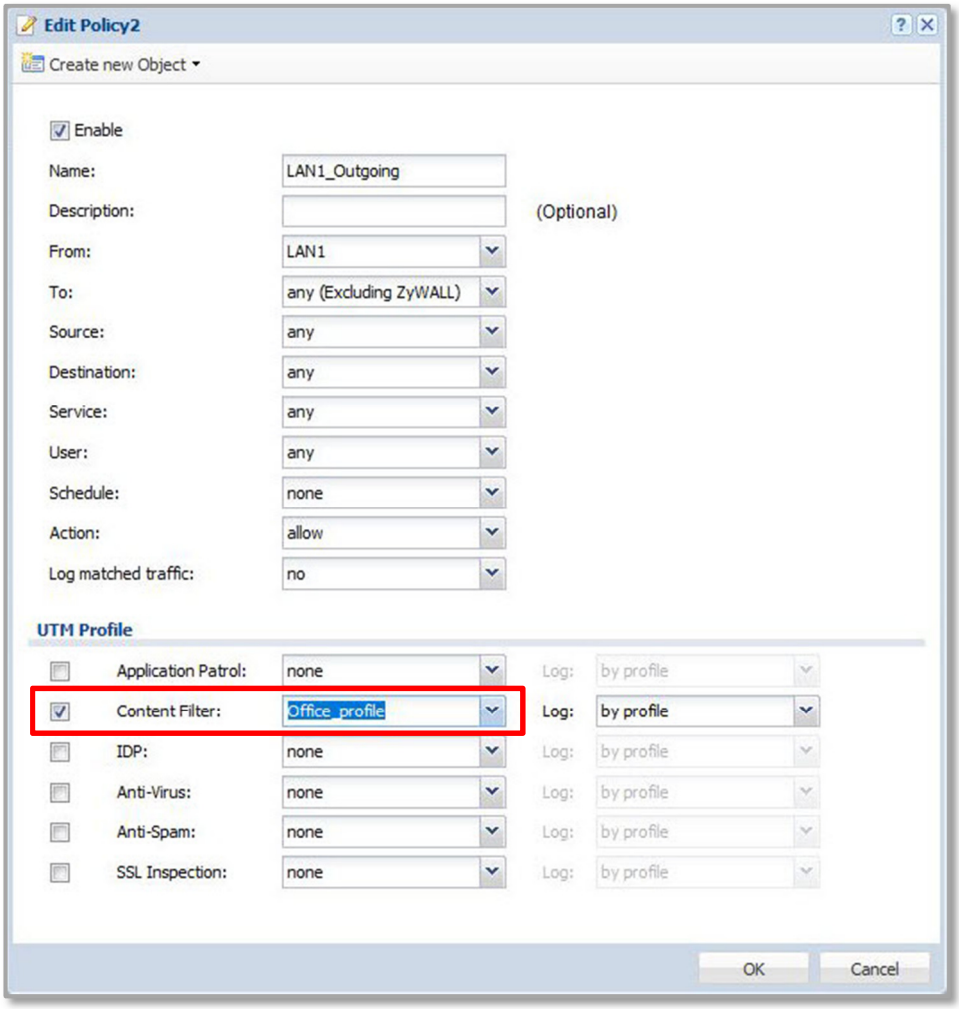
Configuration>Security Policy>Policy Control>Add



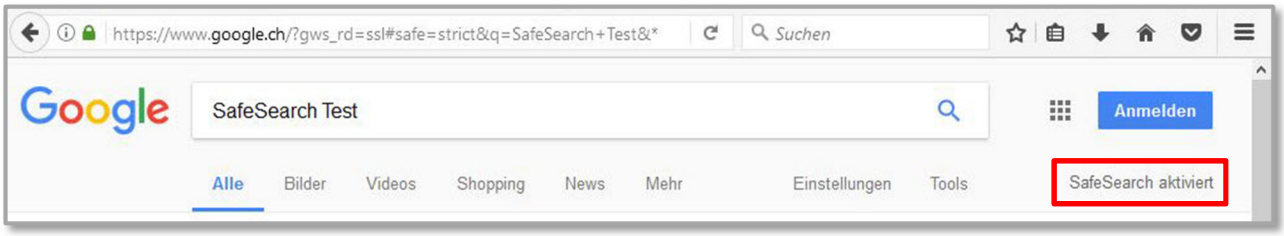
Damit diese Regel angewendet wird, muss sie vor der allgemeinen LAN-Regel stehen (**LAN1_Outgoing**).

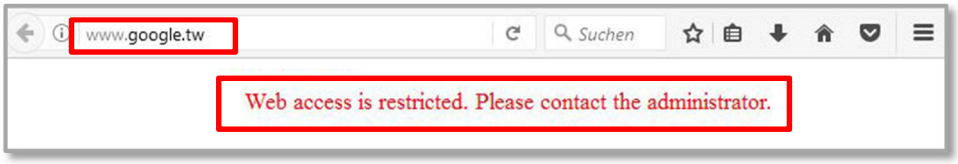


In der **LAN1_Outgoing** Regel das **Content Filter** Profil **Office_profile** aktivieren:



Google SafeSearch ist nun auf der USG aktiviert und nicht eingetragen Länder-Domänen werden blockiert:





Über CNAME lässt sich auch Bing und YouTube einschränken. Bei diesen Diensten reicht der CNAME-Eintrag:

Alias Name	**FQDN**
Bing :	
www.bing.com	strict.bing.com
YouTube Moderate Filterung:	
www.youtube.com	restrictmoderate.youtube.com
m.youtube.com	restrictmoderate.youtube.com
youtubei.googleapis.com	restrictmoderate.youtube.com
youtube.googleapis.com	restrictmoderate.youtube.com
www.youtube-nocookie.com	restrictmoderate.youtube.com
YouTube Strikte Filterung:	
www.youtube.com	restrict.youtube.com
m.youtube.com	restrict.youtube.com
youtubei.googleapis.com	restrict.youtube.com
youtube.googleapis.com	restrict.youtube.com
www.youtube-nocookie.com	restrict.youtube.com