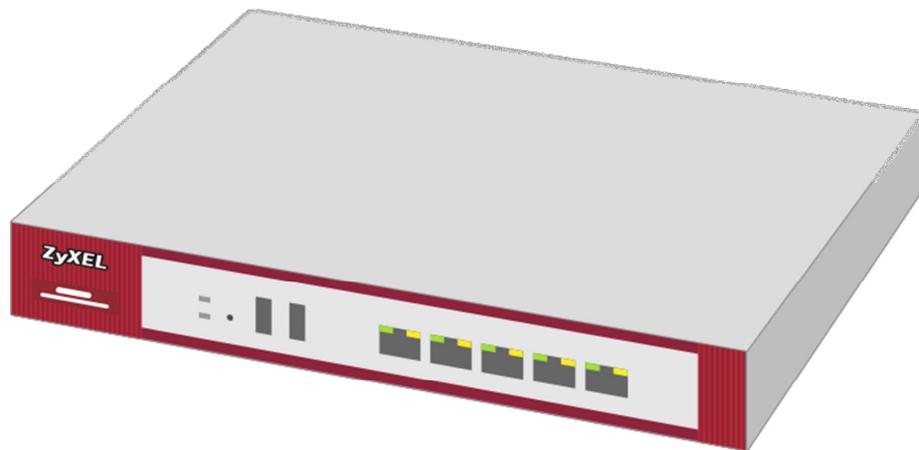


ZYXEL

Your Networking Ally



SafeSearch mit Hilfe von CNAME-Records

Zyxel USG Firewall-Serie
ab Firmware-Version 4.20

Knowledge Base KB-3679
Juni 2017

© Zyxel Corporation

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

The screenshot shows the ZyXEL ZyWALL 110 configuration interface. The left sidebar shows the navigation menu with 'Interface' selected under 'Network'. The main content area displays the 'Configuration' page for the 'Ethernet' interface. A table lists the interfaces with their status, names, IP addresses, and masks. The row for 'lan1' is highlighted with a red box.

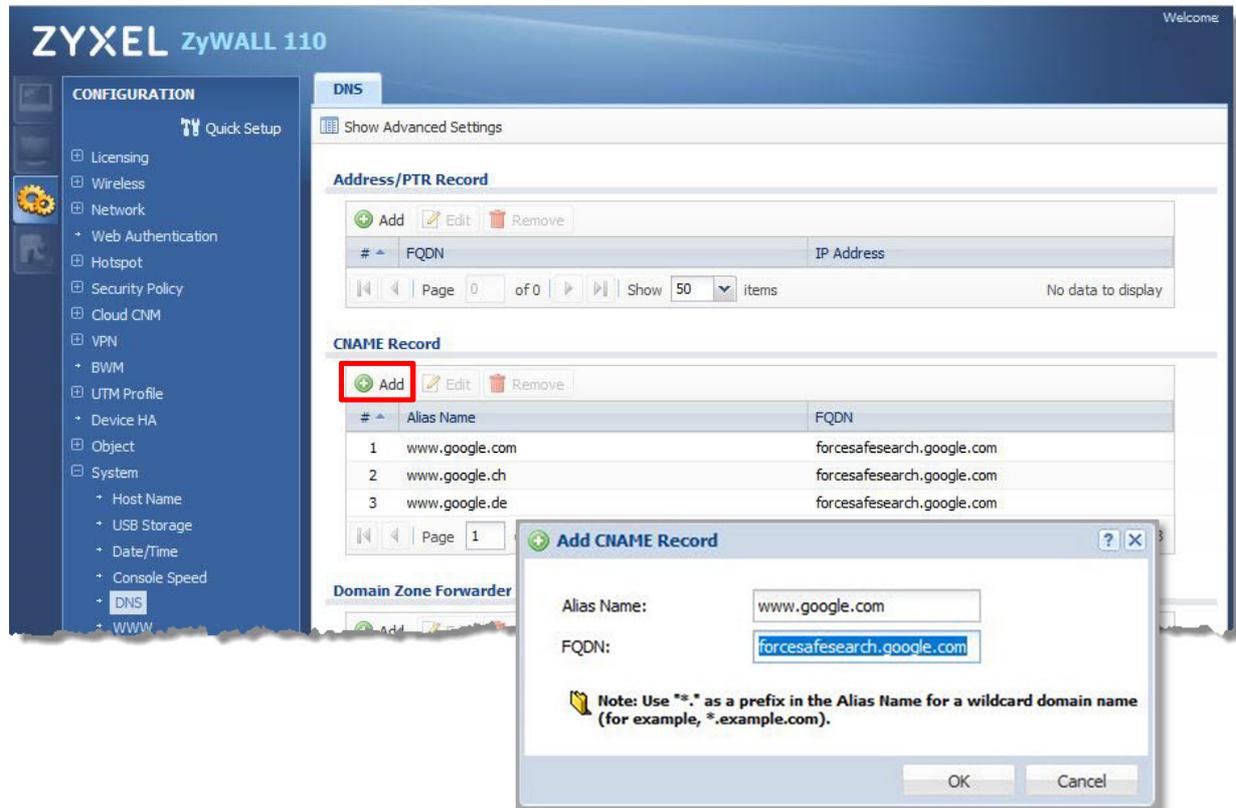
#	Status	Name	IP Address	Mask
1	🟡	wan1	DHCP -- 217.192.14.98	255.255.255.192
2	🟡	wan2	DHCP -- 0.0.0.0	0.0.0.0
3	🟡	opt	STATIC -- 0.0.0.0	0.0.0.0
4	🟡	lan1	STATIC -- 192.168.1.1	255.255.255.0
5	🟡	lan2	STATIC -- 192.168.2.1	255.255.255.0
6	🟡	reserved	STATIC -- 0.0.0.0	0.0.0.0
7	🟡	dmz	STATIC -- 192.168.3.1	255.255.255.0

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

The screenshot shows the 'Edit Ethernet' configuration page. Under the 'DHCP Setting' section, the 'First DNS Server (Optional)' dropdown menu is set to 'ZyWALL' and is highlighted with a red box. Other settings include 'DHCP Server' (dropdown), 'IP Pool Start Address' (192.168.1.33), and 'Pool Size' (200).

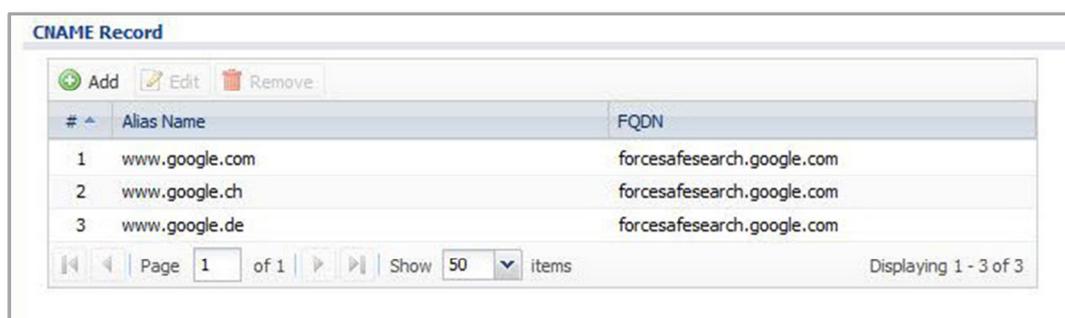
Als nächstes werden in den DNS-Einstellungen die notwendigen Umleitungen erstellt. Dazu werden die CNAME-Records verwendet.

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.

ZYXEL ZyWALL 110

Profile | Trusted Web Sites | Forbidden Web Sites

General Settings

- Enable Content Filter Report Service [Report Server](#) ⓘ
- Enable HTTPS Domain Filter for HTTPS traffic ⓘ
- Drop connection when HTTPS connection with SSL V3 or previous version
- Content Filter Category Service Timeout: (1-60 Seconds)

Message to display when a site is blocked

Denied Access Message:

Redirect URL:

Profile Management

#	Name	Description	Reference
1	Healthcare_profile	Built-in CF Profile	0
2	HomeOffice_profile	Built-in CF Profile	0
3	Office_profile	Built-in CF Profile	1
4	Retail_profile	Built-in CF Profile	0

Page 1 of 1 | Show 50 items | Displaying 1 - 4 of 4

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

Profile | **Trusted Web Sites** | Forbidden Web Sites

Common Trusted Web Sites

Note:
Enable "Check Common Trusted/Forbidden List" in the Custom Service of profile to apply all these websites.

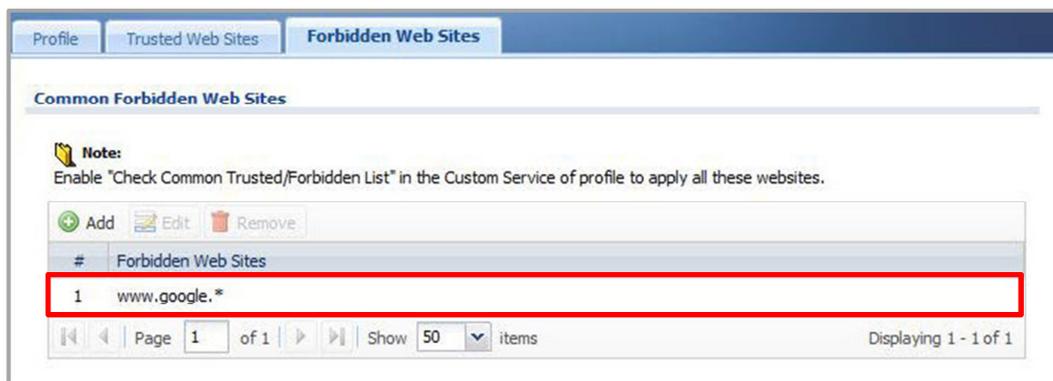
Trusted Web Sites

#	Trusted Web Sites
1	www.google.ch
2	www.google.de
3	www.google.com

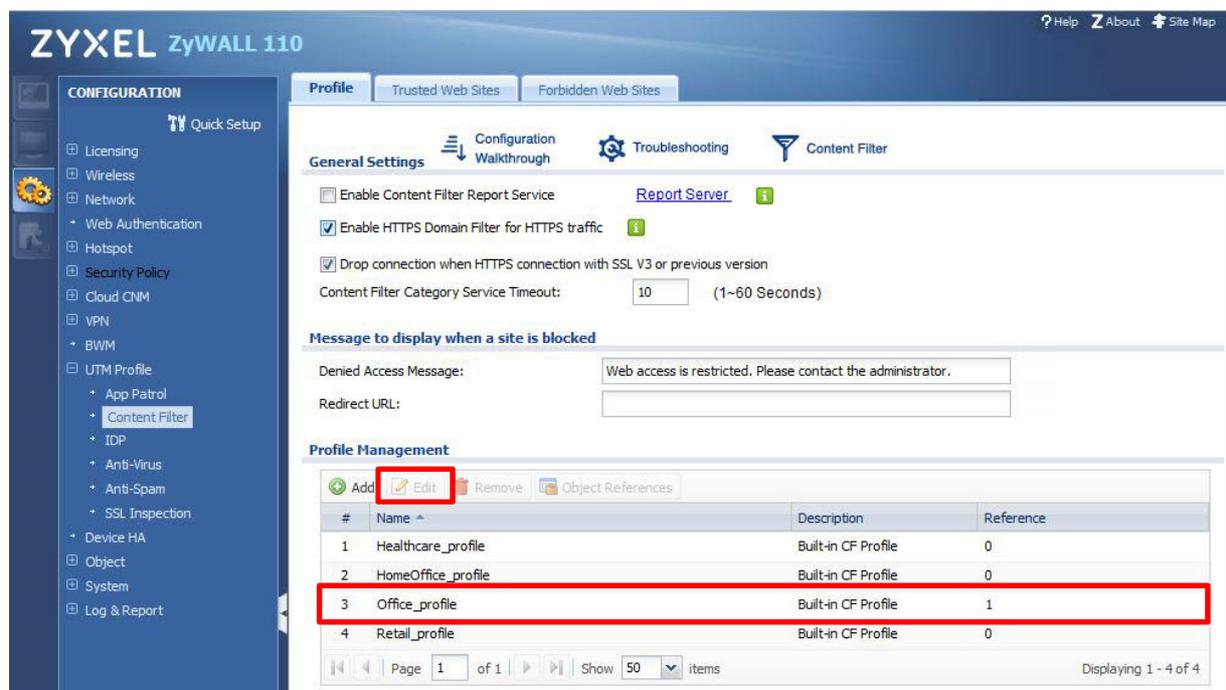
Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

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

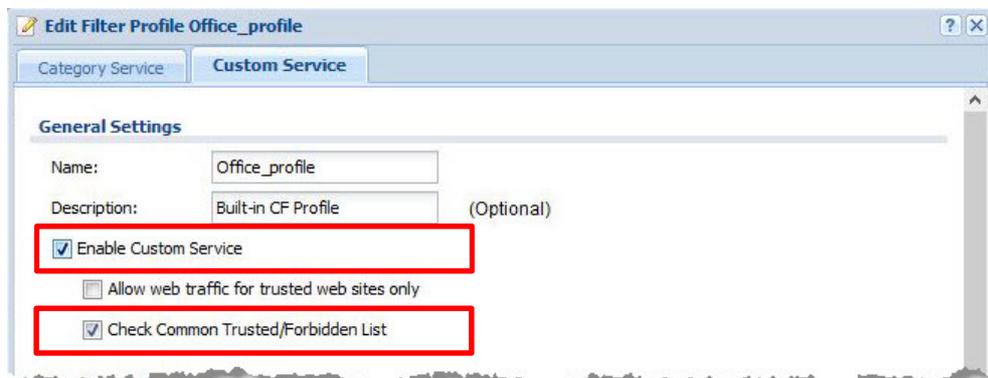
www.google.*



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**.

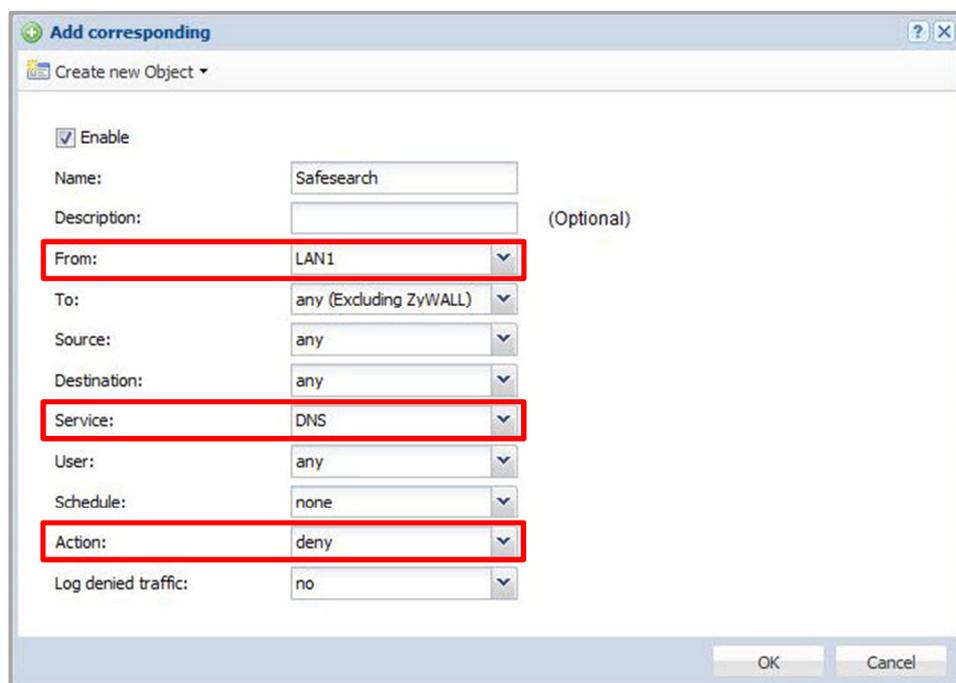


Unter **Custom Service** muss nun die die Option **Enable Custom Service** und **Check Common Trusted/Forbidden List** aktiviert werden



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**).

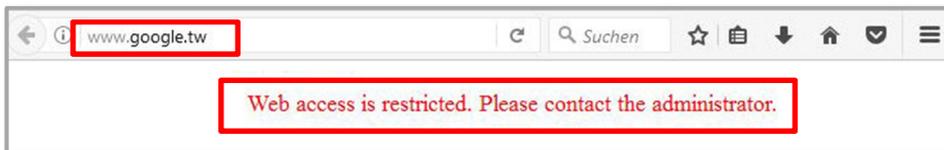
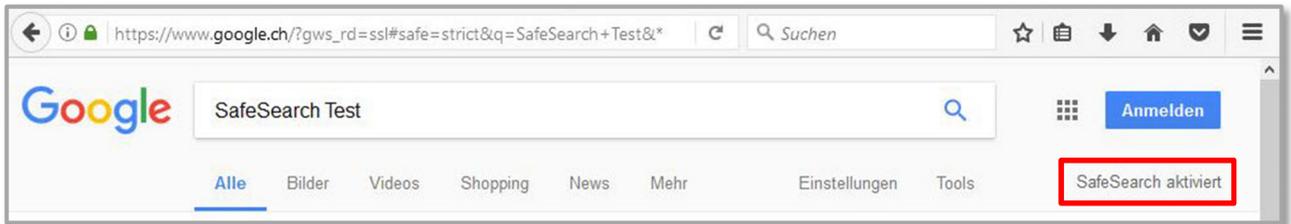
The screenshot shows the ZyXEL ZyWALL 110 web interface. The left sidebar contains a 'CONFIGURATION' menu with options like Licensing, Wireless, Network, Hotspot, Web Authentication, Security Policy, Policy Control, ADP, Session Control, Cloud CNM, VPN, BWM, UTM Profile, Device HA, Object, System, and Log & Report. The main area is titled 'Policy' and shows 'General Settings' with 'Enable Policy Control' checked. Below is the 'IPv4 Configuration' section with a table of rules. The rule 'LAN1_Outgoing' is highlighted with a red box.

Priority	Status	Name	From	To	IPv4 Source	IPv4 Destination	Service	User	Schedule	Action	Log	UTM Profile
1	🟡	Safesearch	LAN1	any (Excluding Zy...	any	any	DNS	any	none	deny	no	
2	🟡	LAN1_Outgoing	LAN1	any (Excluding Zy...	any	any	any	any	none	allow	no	
3	🟡	LAN2_Outgoing	LAN2	any (Excluding Zy...	any	any	any	any	none	allow	no	
4	🟡	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no	
5	🟡	IPSec_VPN_Outgoing	IPSec_VPN	any (Excluding Zy...	any	any	any	any	none	allow	no	
6	🟡	SSL_VPN_Outgoing	SSL_VPN	any (Excluding Zy...	any	any	any	any	none	allow	no	
7	🟡	TUNNEL_Outgoing	TUNNEL	any (Excluding Zy...	any	any	any	any	none	allow	no	
8	🟡	LAN1_to_Device	LAN1	ZyWALL	any	any	any	any	none	allow	no	
9	🟡	LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	none	allow	no	
10	🟡	DMZ_to_Device	DMZ	ZyWALL	any	any	Default_Allow_D...	any	none	allow	no	
11	🟡	WAN_to_Device	WAN	ZyWALL	any	any	Default_Allow_W...	any	none	allow	no	
12	🟡	IPSec_VPN_to_Device	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	no	
13	🟡	SSL_VPN_to_Device	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no	
14	🟡	TUNNEL_to_Device	TUNNEL	ZyWALL	any	any	any	any	none	allow	no	
Default			any	any	any	any	any	any	none	deny	log	

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

The screenshot shows the 'Edit Policy2' dialog box. The 'Enable' checkbox is checked. The 'Name' field is 'LAN1_Outgoing'. The 'From' field is 'LAN1' and the 'To' field is 'any (Excluding ZyWALL)'. The 'Service' field is 'any' and the 'Action' field is 'allow'. The 'Log matched traffic' field is 'no'. In the 'UTM Profile' section, the 'Content Filter' checkbox is checked and the profile is set to 'Office_profile'. Other UTM Profile options like 'Application Patrol', 'IDP', 'Anti-Virus', 'Anti-Spam', and 'SSL Inspection' are all set to 'none'.

Google SafeSearch ist nun auf der USG aktiviert und nicht eingetragenen 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