

How to Block “Facebook” for Some Users with the Vigor2820 Router

This document applies to router models that use CSM with object-based settings: Vigor2110, Vigor2710, Vigor2820, VigorPro5300, VigorPro5500, VigorPro5510.

The steps below will allow you to block **facebook** web sites for some users by using the router URL content filter. This method show how to restrict access to facebook based on the LAN computers IP address, so you will need to assign static IP addresses for each PC on your network.

In our example all computers except those having an IP address with the range of 192.168.1.20 to 192.168.1.30 will be blocked from accessing facebook web sites.

Step 1 – Define Keyword Object

Go to **Object Settings>>Keyword Object** configuration menu.
Enter **facebook** in the **Contents** field as shown in the diagram below:

Objects Setting >> Keyword Object

Keyword Object Profiles: [Set to Factory Default](#)

Index	Name	Index	Name
1.	Facebook	17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> [Next](#) >>

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name:

Contents:

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

Step 2 – Set up URL Content Filter Profile

Go to **CSM>>URL Content Filter Profile** configuration menu

Select the first available profile and enter the settings as shown below.

If you wish to also prevent users from accessing facebook web sites by using the IP address of the web site then also tick the selection box "Prevent web access from IP address" in CSM>>URL Content Filter Profile

CSM >> URL Content Filter Profile

URL Content Filter Profile Table: [Set to Factory Default](#)

Profile	Name	Profile	Name
1.	Facebook	5.	
2.		6.	
3.		7.	
4.		8.	

Administration Message (Max 255 characters)

```
<body><center><div><p>The requested Web page has been blocked by URL Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:

Priority: Log:

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy File Extension Profile:

Object/Group Edit

<u>Keyword Object</u>	<input type="text" value="None"/>
or Keyword Object	<input type="text" value="None"/>
or Keyword Object	<input type="text" value="1.Facebook"/>
or Keyword Object	<input type="text" value="None"/>
or Keyword Object	<input type="text" value="None"/>
or Keyword Object	<input type="text" value="None"/>
or Keyword Object	<input type="text" value="None"/>
or Keyword Object	<input type="text" value="None"/>
or <u>Keyword Group</u>	<input type="text" value="None"/>
or Keyword Group	<input type="text" value="None"/>
or Keyword Group	<input type="text" value="None"/>
or Keyword Group	<input type="text" value="None"/>
or Keyword Group	<input type="text" value="None"/>
or Keyword Group	<input type="text" value="None"/>
or Keyword Group	<input type="text" value="None"/>
or Keyword Group	<input type="text" value="None"/>

Select the keyword defined in step 1

Step 3 – Configure Firewall

Refer to the diagram and follow the steps below:

1. Go to **Firewall>>Filter Setup** configuration menu.
2. Select Default Data Filter.
3. In Default Data Filter configuration menu select the next filter rule. We have selected Filter Rule 2.
4. Select "Check to enable the Filter Rule" and add a comment in the comment field.
5. Select "LAN to WAN" for the direction
6. Click on Edit to enter the required range of IP addresses to be allowed access to facebook and select "Invert Selection"
7. In "**URL Content Filter**" pull down menu select the "Facebook" profile in the pull down list. This profile was defined in step 2.
8. Save all your settings

Firewall >> Filter Setup

Filter Setup | Set to Factory Default

Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	Firewall >> Filter Setup >> Edit Filter Set
3.		9.	
4.		10.	
5.		11.	Filter Set 2
6.		12.	

Filter Set 2
Comments: Default Data Filter

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	xNetBios -> DNS
2	<input checked="" type="checkbox"/>	Block facebook
3	<input type="checkbox"/>	

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments: Block facebook

Index(1-15) in Schedule Setup: [] [] [] []

Direction: LAN -> WAN

Source IP: !(192.168.1.20~192.168.1.30) [Edit]

Destination IP: Any [Edit]

Service Type: Any [Edit]

Fragments: Don't Care

Application Filter: [None] [Edit]

Branch to Other Filter Set: [None]

IMP2P Filter: [None]

URL Content Filter: **1-Facebook** [Edit]

Web Content Filter: [None]

Advance Setting [Edit]

[OK] [Clear] [Cancel]

Select Facebook profile for URL Content Filter

Enter IP address range for PC's to be allowed access to Facebook and click on "Invert Selection"

IP Address Edit

Address Type: Range Address

Start IP Address: 192.168.1.20

End IP Address: 192.168.1.30

Subnet Mask: 0.0.0.0

Invert Selection:

IP Group: [None]

or IP Object: [None]

or IP Object: [None]

or IP Object: [None]

[OK] [Close]

Now all users on the LAN except for computers having an IP address within the range of 192.168.1.20 to 192.168.1.30 will not be able to access "facebook" web sites by using either the web address or IP address. If they try to access facebook, they will be greeted by the following message:

The requested Web page has been blocked by URL Content Filter.
Please contact your system administrator for further information.

This message can be customised in **CSM>>URL Content Filter Profile** configuration menu.