



# BLOCK ADULT WEBSITES

By:Haydar Fadel



# Block Adult Websites

---

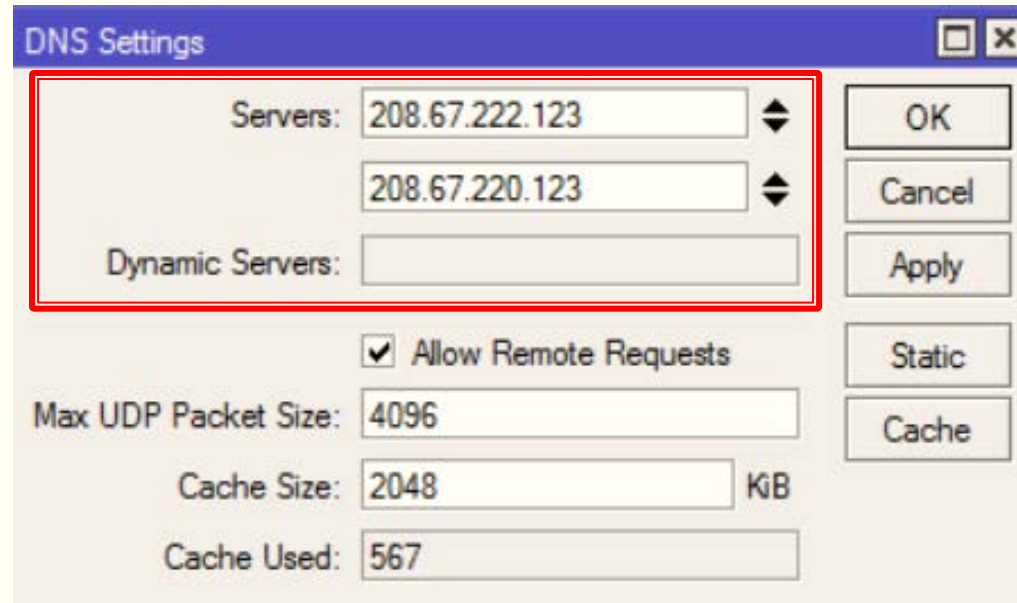
---

- The following is the free, neat and clean method to block about **80-90%** of porn web sites using **OpenDNS** server as your primary DNS server in your router/proxy or even desktop PC.
- Use the below DNS server as your primary DNS server in MikroTik/ ISA server / router or even a desktop.
- **208.67.222.123**
- **208.67.220.123**
  - A. If you are using MikroTik or other Server, make sure clients are using your server ip as there DNS server, because opendns will work only if the client / router is using there DNS server.
  - B. You can also force users to use your DNS server by adding redirect rule so every request for DNS should be redirected to your local server.

# Block Adult Websites

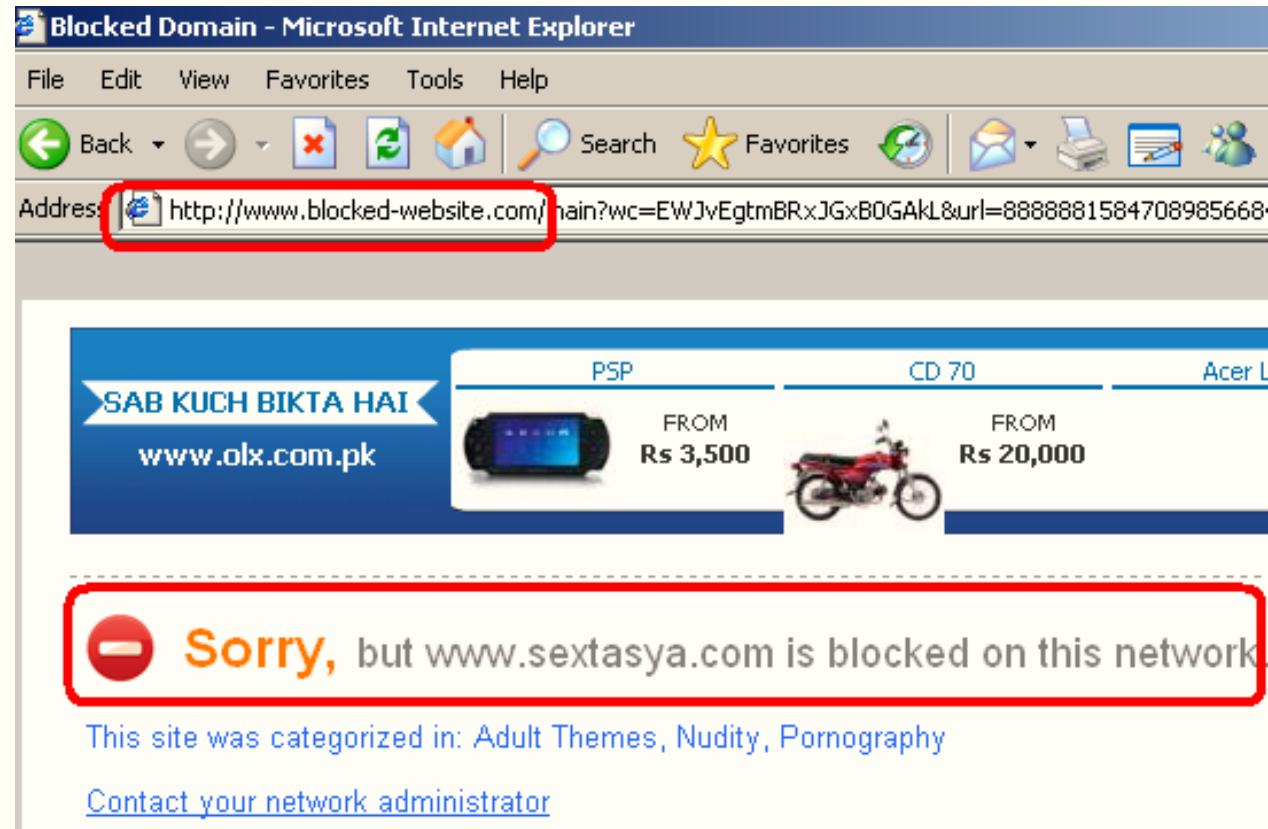
---

- If you are using MikroTik server, then it would look alike something below image . . .



# Block Adult Websites

- Now if you will try to open any adult web site , it wont open and will give you the default browser 'Could not open' error, or the request will be redirected to **OpenDNS** block page informing you that your request was blocked by **OpenDNS**.
- *As showed in the image below . . .*



# Redirect Open DNS Error to Local Page

---

- You can also show your own page explaining that Adult web sites are blocked and with your Advertisement.
- For this purpose, you have to enable web.proxy and redirect user traffic to local proxy, then in proxy access, block the **<http://www.blocked-website.com>** and redirect it to local web server page.
- Replace the **101.11.11.240** and the full path with your local web server.

# Redirect Open DNS Error to Local Page

The screenshot shows the 'Web Proxy Settings' dialog box with the 'General' tab selected. The 'Enabled' checkbox is checked and highlighted with a red box. The 'Cache On Disk' checkbox is also checked and highlighted with a red box. Other settings include Src. Address: ::, Port: 8080, Anonymous: unchecked, Parent Proxy: empty, Parent Proxy Port: empty, Cache Administrator: webmaster, Max. Cache Size: unlimited, Max Cache Object Size: 2048, Max. Client Connections: 600, Max. Server Connections: 600, Max Fresh Time: 3d 00:00:00, Cache Hit DSCP (TOS): 4, and Cache Drive: system.

The screenshot shows the 'New Web Proxy Rule' dialog box. The 'Dst. Host' field is set to 'www.blocked-website.com' and is highlighted with a red box. The 'Action' is set to 'deny'. The 'Redirect To' field is set to '101.11.11.240' and is highlighted with a red box. The 'Hits' field is set to 0. The status at the bottom is 'enabled'.

**How to Enable Web Proxy in Mikrotik and redirect opens error page to local error page.**

# Redirect All Users Traffic to Local Proxy

New NAT Rule

General Advanced Extra Action Statistics

Chain: dstnat

Src. Address:

Dst. Address:

Protocol:  6 (tcp)

Src. Port:

Dst. Port:  80

Any. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

enabled

New NAT Rule

General Advanced Extra Action Statistics

Action: redirect

To Ports: 8080

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Redirect all traffic to local proxy

enabled



# Redirect All Users Traffic to Local Proxy

New NAT Rule

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:  208.67.216.135

Protocol:  6 (tcp)

Src. Port:

Dst. Port:  80

Any. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

enabled

New NAT Rule

General Advanced Extra Action Statistics

Action:

To Ports:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

enabled

Redirect traffic for only specific webpage or IP to local proxy



# Redirect Open DNS Error to Local Page

The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration. The 'DNS-Redirect-UDP' rule is highlighted with a red box. The table below shows the configuration for the highlighted rule and other rules in the list.

| # | Action   | Chain  | Src. Address | Dst. Address | Proto... | Src. Port | Dst. Port | In. Inter... | Out. Int... | Bytes    | Packets |
|---|----------|--------|--------------|--------------|----------|-----------|-----------|--------------|-------------|----------|---------|
| 0 | srcnat   | srcnat |              |              |          |           |           |              |             | 69.8 KiB | 925     |
| 1 | redir... | dstnat |              |              | 17 (u... |           | 53        |              |             | 29.4 KiB | 457     |
| 2 | redir... | dstnat |              |              | 6 (tcp)  |           | 53        |              |             | 0 B      | 0       |

3 items

# Redirect Open DNS Error to Local Page

NAT Rule <53>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:  17 (udp)

Src. Port:

Dst. Port:  53

Any. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Reset Counters  
Reset All Counters

enabled

NAT Rule <53>

General Advanced Extra Action Statistics

Action:

To Ports:

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Reset Counters  
Reset All Counters

enabled

**force users to use specific DNS Server**



# THE END

Source :  
<https://aacable.wordpress.com/2012/11/22/howto-block-adult-websites-using-opendns-for-free/>

