

Blocking Facebook

By: Haydar Fadel



Blocking Facebook Introduction

- There is many ways and method to block facebook browsing downloading video Etc .
- Most implementation on MikroTik Routers by using Firewall facility and layer7 configuration .
- In this document we will block facebook via automated address list that base on MikroTik router DNS-Cache
- First create the script which will catch facebook.com from the DNS cache and will add it in **“facebook-dns-ips”** address list.
- Open Terminal and paste the following script.

Step 1 : Script

```
1# Script to add Facebook DNS IP addresses
2# Haydar Fadel / haider@satgate-Iraq.com
3# Script Source: N/A / GOOGLE : )
4
5:log warning "Script Started ... Adding Facebook DNS ip's to address list name  facebook-dns-ips"
6:foreach i in=[/ip dns cache find] do={
7:local bNew "true";
8:local cacheName [/ip dns cache all get $i name] ;
9:if ([:find $cacheName "facebook"] != 0) do={
10:local tmpAddress [/ip dns cache get $i address] ;
11:put $tmpAddress;
12:if ( [/ip firewall address-list find ] = "") do={
13:log info ("added entry: $[/ip dns cache get $i name] IP $tmpAddress");
14:ip firewall address-list add address=$tmpAddress list=facebook-dns-ips comment=$cacheName;
15} else={
16:foreach j in=[/ip firewall address-list find ] do={
17:if ( [/ip firewall address-list get $j address] = $tmpAddress ) do={
18:set bNew "false";
19}
20}
21:if ( $bNew = "true" ) do={
22:log info ("added entry: $[/ip dns cache get $i name] IP $tmpAddress");
23:ip firewall address-list add address=$tmpAddress list=facebook-dns-ips comment=$cacheName;
24}
25}
26}
27}
28# FB DNS IP ADD Script Ended ...
```

The screenshot shows the 'Script List' application window. The 'Scripts' tab is active, and a table lists the script 'facebook-list' with owner 'admin', last started 'Jul/14/2014 10:45:00', and run count '2'. A dialog box titled 'Script <facebook-list>' is open, showing the script's configuration. The 'Name' field is highlighted with a red box and contains 'facebook-list'. Other fields include 'Owner: admin', a 'Policy' section with checkboxes for 'reboot', 'write', 'test', 'sniff', 'read', 'policy', 'password', and 'sensitive', and a 'Source' field containing the script's source code. The 'Run Script' button is visible at the bottom right of the dialog.

Name	Owner	Last Time Started	Run Count
facebook-list	admin	Jul/14/2014 10:45:00	2

Script <facebook-list>

Name: facebook-list

Owner: admin

Policy

- reboot
- write
- test
- sniff
- read
- policy
- password
- sensitive

Last Time Started: Jul/14/2014 10:45:00

Run Count: 2

Source:

```
# Script to add Facebook DNS IP
addresses
# Haydar Fadel / haider@satgate-Iraq.com
# Script Source: N/A / GOOGLE :)

:log warning "Script Started ... Adding
Facebook DNS ip's to address list name
facebook-dns-ips"
foreach i in=[/ip dns cache find] do={
:local bNew "true";
```

Step 2 : Scheduler

- Schedule the script to run after every 5 minutes (or hourly basis)

```
/system scheduler
```

```
1add disabled=no interval=5m name=fb-script-run-schedule on-event=facebook-list
```

```
2policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api start-date=feb/11/2014 start-time=00:00:00
```

The screenshot displays the Windows Scheduler application. The main window shows a list of tasks with the following details:

Name	Start Date	Start Time	Interval	On Event	Owner	Run Count	Next Run
fb-script-run-s...	Feb/11/2014	00:00:00	00:05:00	facebook-list	admin	1	Jul/14/2014 ...

The task 'fb-script-run-schedule' is selected. A secondary window titled 'Schedule <fb-script-run-schedule>' is open, showing the configuration for this task:

- Name: fb-script-run-schedule
- Start Date: Feb/11/2014
- Start Time: 00:00:00
- Interval: 00:05:00
- On Event: facebook-list

The 'Name' field in the configuration window is highlighted with a red box. The 'On Event' list contains 'facebook-list'. The 'OK' button is also highlighted with a red box. The status bar at the bottom of the Scheduler window indicates '1 item (1 selected)'.

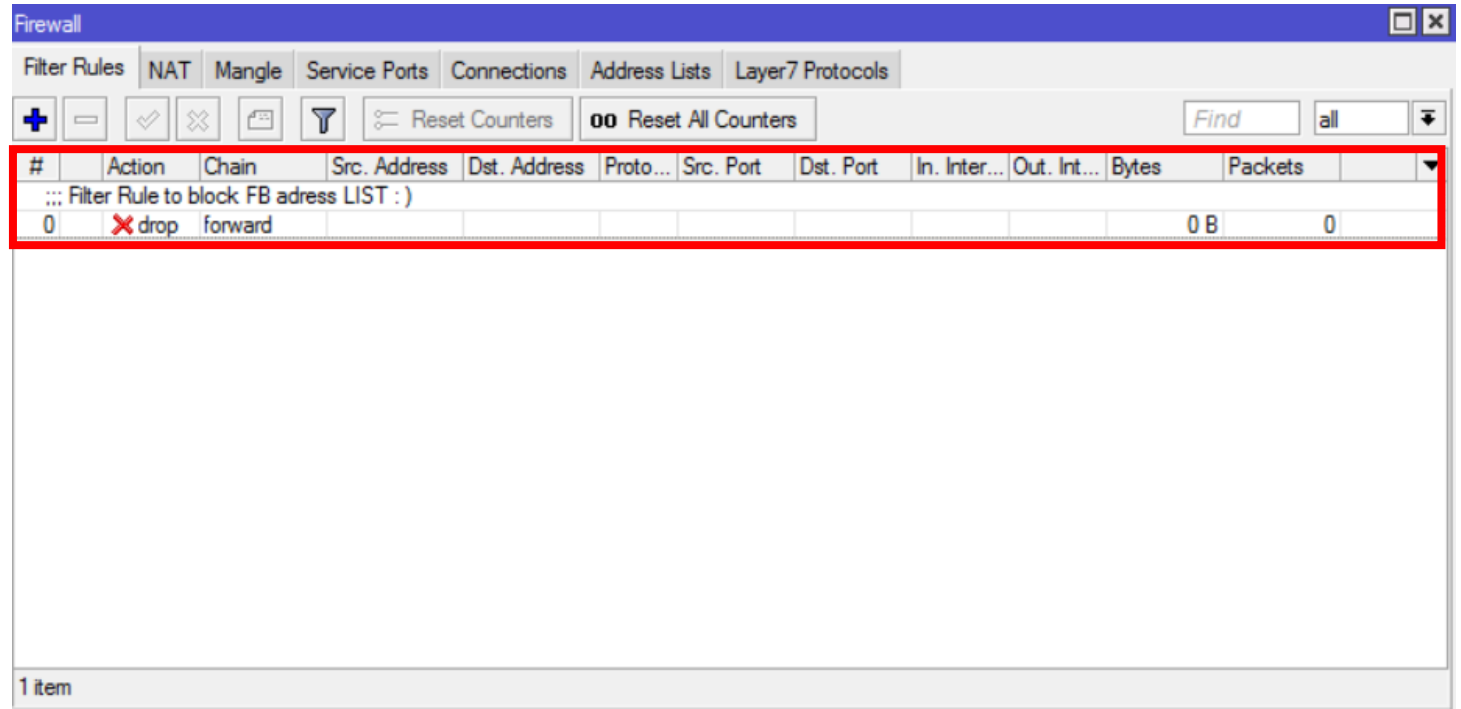
Step 3 : Filter Rule

- Now create a **FIREWALL FILTER** rule which will actually **DROP** the request going to **facebook-dns-ips** address list.
- [Make sure to move this rule on TOP , or before any general accept rule in Filter section)

1/ip firewall filter

2add action=drop chain=forward comment="Filter Rule to block FB adress LIST :)" disabled=no dst-address-list=facebook-dns-ips

- Now try to access the facebook, it will open as usual, but as soon as the script will run, a address list will be created with the FB ip address list, & its access will be blocked.
- *As showed in the image below ...*



Step 3 : Time Base Filter Rule

- You can also use this technique to block FB in some specific timings only. For example you want to block access to FB from 9am to 10:am then use the following filter rule.

```
1/ip firewall filter
```

```
2 add action=drop chain=forward comment="Filter Rule to block FB address LIST : )" disabled=no dst-address-list=facebook-dns-ips time=9h-10h,sun,mon,tue,wed,thu,fri,sat
```

Force / Redirect Users to Use Your DNS

1/ip firewall nat

2add chain=dstnat action=dst-nat to-addresses=192.168.1.1 to-ports=53 protocol=tcp dst-port=53

3add chain=dstnat action=dst-nat to-addresses=192.168.1.1 to-ports=53 protocol=udp dst-port=53

The screenshot shows the 'NAT Rule <53>' configuration window in Mikrotik WinBox. The 'General' tab is active. The 'Chain' dropdown is set to 'dstnat'. The 'Protocol' dropdown is set to '6 (tcp)'. The 'Dst. Port' field is set to '53'. The 'Src. Address', 'Dst. Address', 'Src. Port', 'Any. Port', 'In. Interface', 'Out. Interface', 'Packet Mark', 'Connection Mark', 'Routing Mark', 'Routing Table', and 'Connection Type' fields are empty. The 'Action' tab is visible but not selected. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters' are on the right.

The screenshot shows the 'NAT Rule <53>' configuration window in Mikrotik WinBox. The 'General' tab is active. The 'Action' dropdown is set to 'dst-nat'. The 'To Addresses' field is set to '192.168.1.1'. The 'To Ports' field is set to '53'. The 'Chain', 'Src. Address', 'Dst. Address', 'Protocol', 'Src. Port', 'Any. Port', 'In. Interface', 'Out. Interface', 'Packet Mark', 'Connection Mark', 'Routing Mark', 'Routing Table', and 'Connection Type' fields are empty. The 'Action' tab is selected. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters' are on the right.



The END

Source

<https://aacable.wordpress.com/2014/02/11/blocking-httphttps-facebook-via-automated-address-list/>