Website Blocking Policy
With MikroTik RouterOS

Presented by Michael Takeuchi
MikroTik User Meeting, 24 April 2017 – Ho Chi Minh City (Vietnam)
About Michael Takeuchi

• Using MikroTik RouterOS (v5.20) Since 14 December 2014
  • RouterOS x86 at PC
• Was MikroTik Certified on MTCNA, MTCRE, MTCINE, MTCUME, MTCWE, MTCTCE, MTCIPv6E
• Student of Vocational High School Taruna Bhakti Depok
• MikroTik Certified Consultant
Website Blocking? Policy?

• Many employee in office accessing social media or entertainment website when working hours and make they work not focus

• Many student in school or university accessing social media or entertainment website when the teacher explaining the lesson and make the student not focus to study

• So MikroTik Come with solution to block and control the traffic 😊
The Technique; Ninja Said This is The Jutsu joke

• Static DNS
• Web Proxy
• Route Policy
• Content Filter
• Layer 7 Firewall
• Destination IP Address/Port Block
1. Static DNS

- Will change the IP Address from a domain
- Client DNS Request must be redirected to router
- Static DNS will replace the IP of Original Server with fake IP and make your client host can’t access the actual server by domain

/ip dns static add name=example.com address=127.0.0.1
/ip firewall nat add chain=dstnat dst-port=53 action=redirect to-ports=53 protocol=tcp
/ip firewall nat add chain=dstnat dst-port=53 action=redirect to-ports=53 protocol=udp
1. Static DNS – Applying

You can use regex or name (only one).
But in this case I will try to use name

if you use name with example.com,
then www.example.com won't work
1. Static DNS – Transparent DNS (TCP & UDP)

Setup new rule with same action, port and chain, but has different protocol.
This rule will redirect all of DNS Request to router.
1. Static DNS – Result

- The IP of example.com changed!
2. Web Proxy

• Doesn't work at all with HTTPS traffic
• Work as Content Cache & Filter Server
• Router Storage Killer (we can set the limit)
• All of HTTP Traffic must be redirected to router
• Can be used to block HTTP website or redirect to a new website

/ip proxy set enabled=yes cache-administrator=michael@takeuchi.id
/ip firewall nat add chain=dstnat dst-port=80 action=redirect to-ports=8080 protocol=tcp
2. Web Proxy – Enabling

• Enable Web Proxy
2. Web Proxy – Blocking

• Go to Access Menu on The Left
2. Web Proxy – Result

ERROR: Forbidden

While trying to retrieve the URL http://example.com/:

- Access Denied

Your cache administrator is michael@takeuchi.id.

3. Route Policy

• Doesn’t Support by Domain
• Can be combined with route mark
• Will block all traffic with specified IP, not protocol or port (except you combine it with route mark)

/ip route add dst-address=8.8.8.8 type=blackhole
3. Route Policy – Applying
3. Route Policy – Testing

![Route List](image)

```
un An[admin@MicroTlK] > ping 8.8.8.8
SEQ HOST SIZE TTL TIME STATUS
 0 8.8.8.8 no route to host
 1 8.8.8.8 no route to host
 2 8.8.8.8 no route to host
 3 8.8.8.8 no route to host
 4 8.8.8.8 no route to host
 5 8.8.8.8 no route to host
 6 8.8.8.8 no route to host
 7 8.8.8.8 no route to host
 8 8.8.8.8 no route to host
 9 8.8.8.8 no route to host
10 8.8.8.8 no route to host

sent=11 received=0 packet-loss=100%
```
3. Route Policy – Result

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\admin>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\admin>
```
Route Type Comparison

- **blackhole (B)** = Silently discard packet forwarded by this route.

- **unreachable (U)** = Discard packet forwarded by this route. Notify sender with ICMP host unreachable (type 3 code 1) message.

- **prohibit (P)** = Discard packet forwarded by this route. Notify sender with ICMP communication administratively prohibited (type 3 code 13) message.

4. Content Filter

• Will filter the packet by specified plain text on packet
• Doesn’t work if the packet content encrypted
• Available on ip firewall -> advance tab

• We will try to block packet which contain **example**

/ip firewall filter add chain=forward protocol=tcp dst-port=80,443 in-interface=ether2-LAN out-interface=ether1-WAN action=drop **content=example**
4. Content Filter – Applying
4. Content Filter – Applying
4. Content Filter – Result

- We can’t access example.com with TCP/80 and TCP/443
4. Content Filter – Result

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>forward</td>
<td>6 (tcp)</td>
<td>80, 443</td>
<td>ether2-LAN</td>
<td>ether1-WAN</td>
<td>example</td>
<td>7.5 KB</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Layer 7 Firewall

- Layer 7 Firewall will search the packet patterns in ICMP/TCP/UDP Streams with the first 10 packets and 2KB packets.
- If the pattern is not found in the collected data, the matcher stops inspecting further.
- High CPU Load, because router need to search the packet patterns.
- The Regular Expression (regex) is sensitive case.
5. Layer 7 Firewall – Regular Expressions

.*(example)+.*

/ip firewall layer7-protocol add name=example regexp=".*(example)+.*"
5. Layer 7 Firewall – Applying

We are try to block or drop on filter rule with Layer 7 regex too, we can do more creation with it, just be creative 😊
6. Dst. IP Address/Port Block

- Will block by specified IP address, port, protocol, content, regexp and many more (defined on /ip firewall filter)
- We can create address-list manually
- We can create address-list dynamically (see below)
We are trying to access a local website using:

```
/ip firewall filter add action=drop chain=forward dst-address=10.10.10.1 dst-port=80,443 in-interface=ether2-LAN protocol=tcp src-address=192.168.3.0/24
```
6. Dst. IP Address/Port Block – Applying (2)

We are try to block using address-list:
:for x from=1 to=15 \
do={/ip firewall address-list add address="10.10.10.$"x"0" list=local-website}

/ip firewall filter add action=drop chain=forward dst-address-list=local-website dst-port=80,443 in-interface=ether1 protocol=tcp src-address=192.168.3.0/24
6. Dst. IP Address/Port Block – Applying (3)

We are trying to block using dynamic address-list, create the address-list first:

/ip firewall address-list add list=blocked-web address=facebook.com
/ip firewall address-list add list=blocked-web address=youtube.com

Then block with /ip firewall filter:
/ip firewall filter add chain=forward action=drop dst-address-list=blocked-web
6. Dst. IP Address/Port Block – Applying (3)

We are trying to block using dynamic address-list we made before.
/ip firewall filter add chain=forward action=drop dst-address-list=blocked-web
which one the best?
depends on your network and what you block 😊
are we finish? NO!
we need to see the main problem 😊
The Main Problem (VPN/Tunnel)

• Someone who using tunnel, we need to block the tunnel too
• How we block tunnel? We need to learn the packet pattern
• Learn how tunnel is on http://rickfreyconsulting.com/mikrotik-vpns/
• For the example we will block PPTP (TCP/1723) & L2TP (UDP/1701)

/ip firewall filter
add action=drop chain=forward dst-port=1723 in-interface=ether2-LAN out-interface=ether1-WAN protocol=tcp
add action=drop chain=forward dst-port=1701 in-interface=ether2-LAN out-interface=ether1-WAN protocol=udp
Another Solution

• **Block All, Accept Few**

• For the example, we will try to allow ping only

/ip firewall filter

add chain=forward dst-address=8.8.8.8 protocol=icmp src-address=192.168.3.0/24

add action=drop chain=forward dst-address=0.0.0.0/0 src-address=192.168.3.0/24
Question & Answer
& don’t feel so hard to contact or consult with me
I am available on michael[at]takeuchi[dot]id
and listed in MikroTik Certified Consultant