

# 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

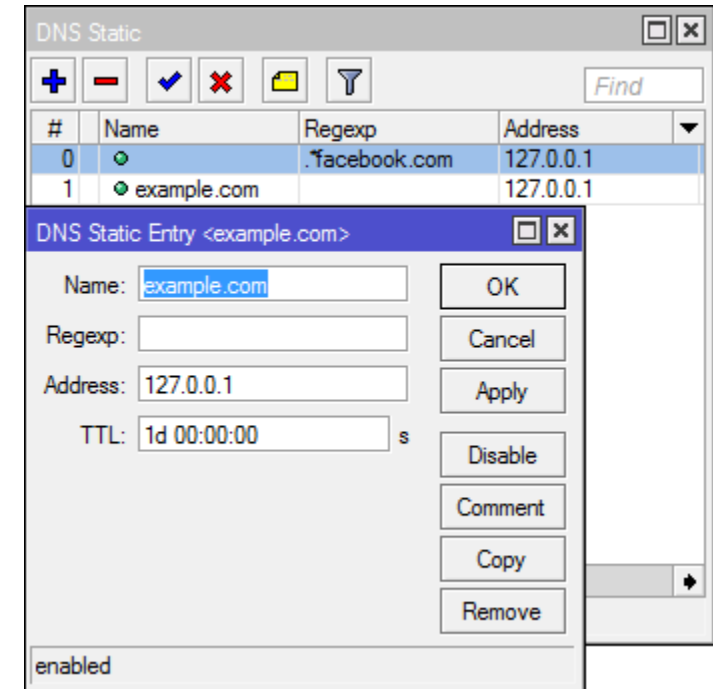
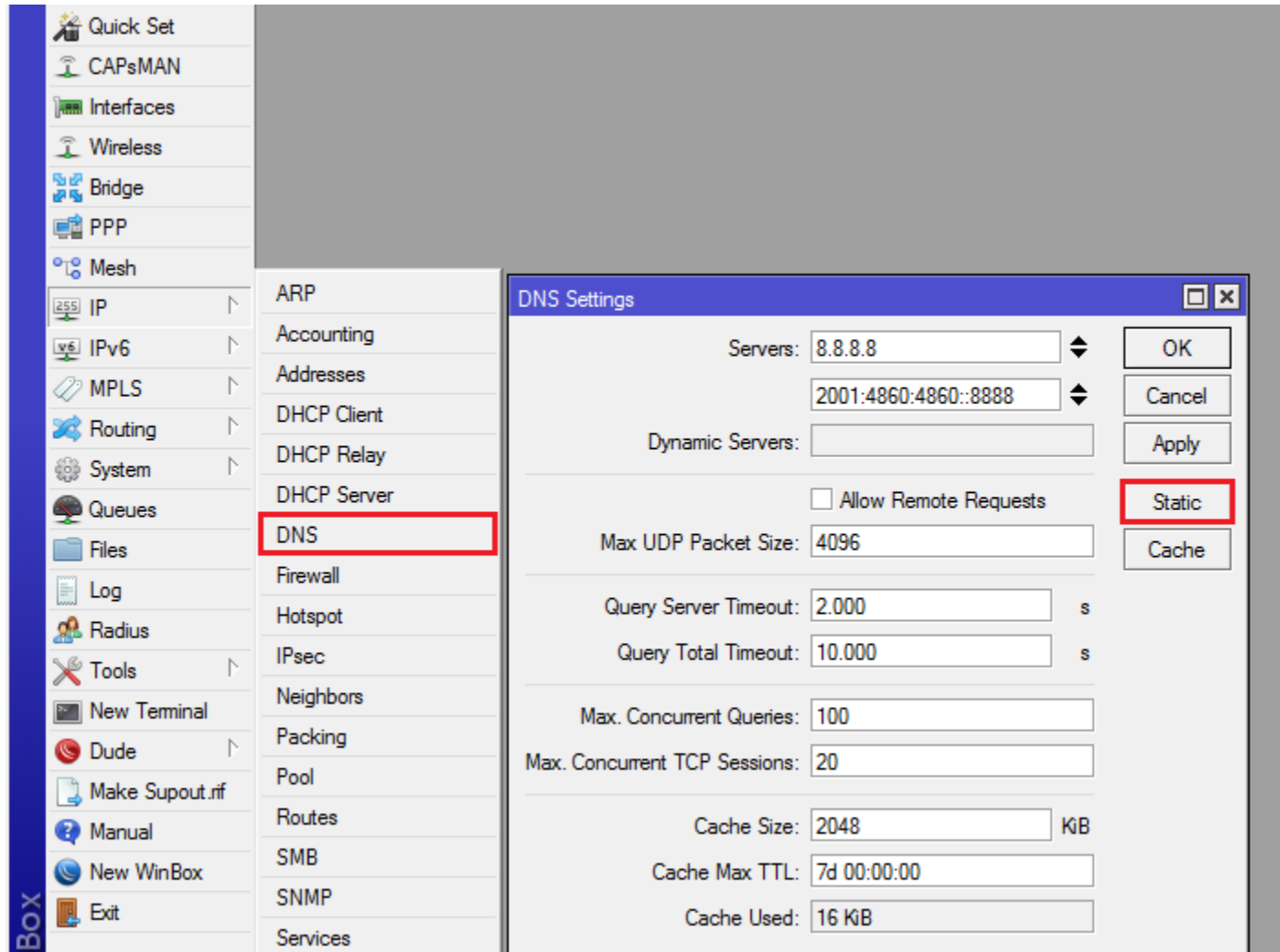
- Will change the IP Address from a domain
- Client DNS Request must be redirected to router
- Static DNS will replace the IP of Original Server with fake IP and make your client host can't access the actual server by domain

```
/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
```

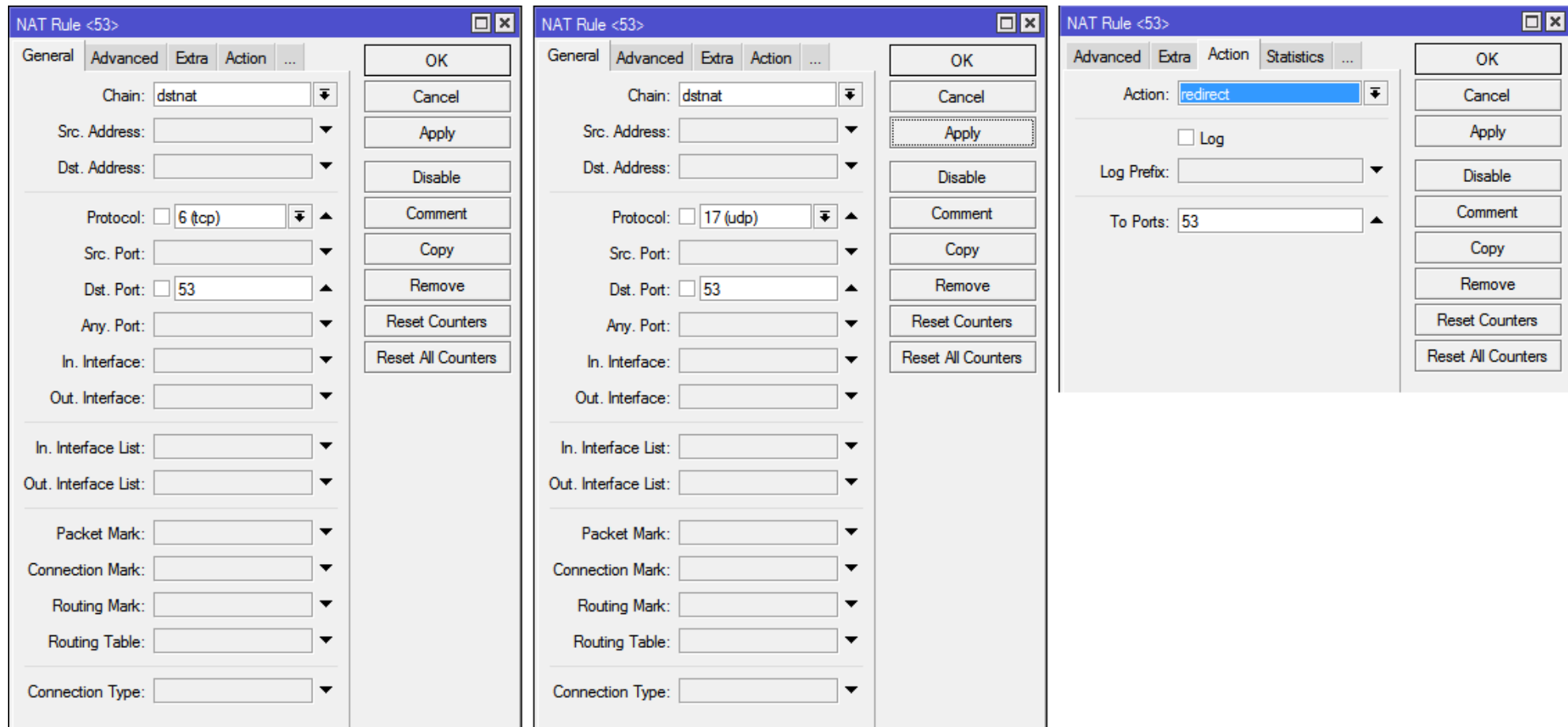
# 1. Static DNS – Applying



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

if you use name with [example.com](http://example.com),  
then [www.example.com](http://www.example.com) won't work

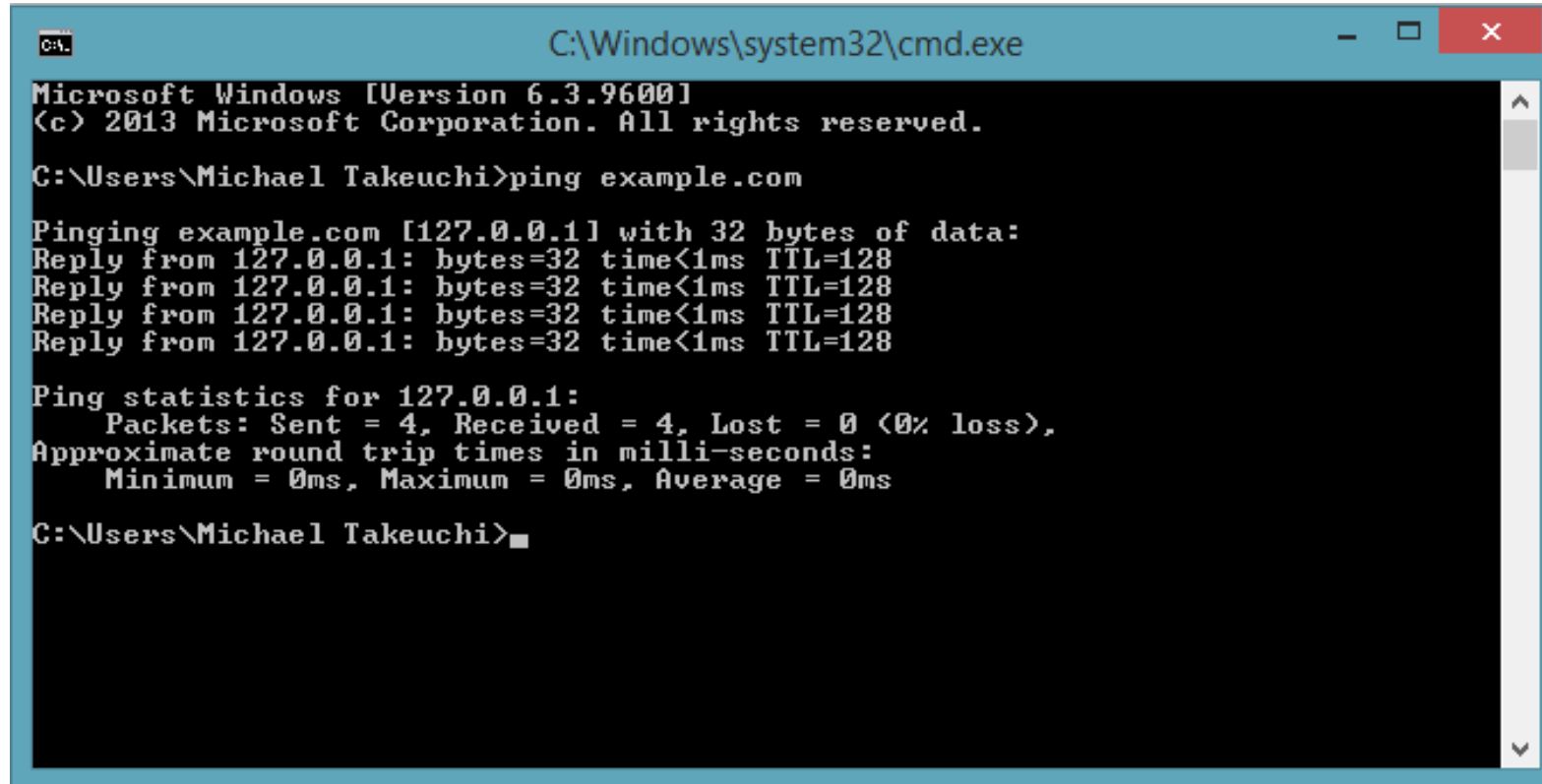
# 1. Static DNS – Transparent DNS (TCP & UDP)



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 !



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Michael Takeuchi>ping example.com

Pinging example.com [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Michael Takeuchi>
```



## 2. Web Proxy

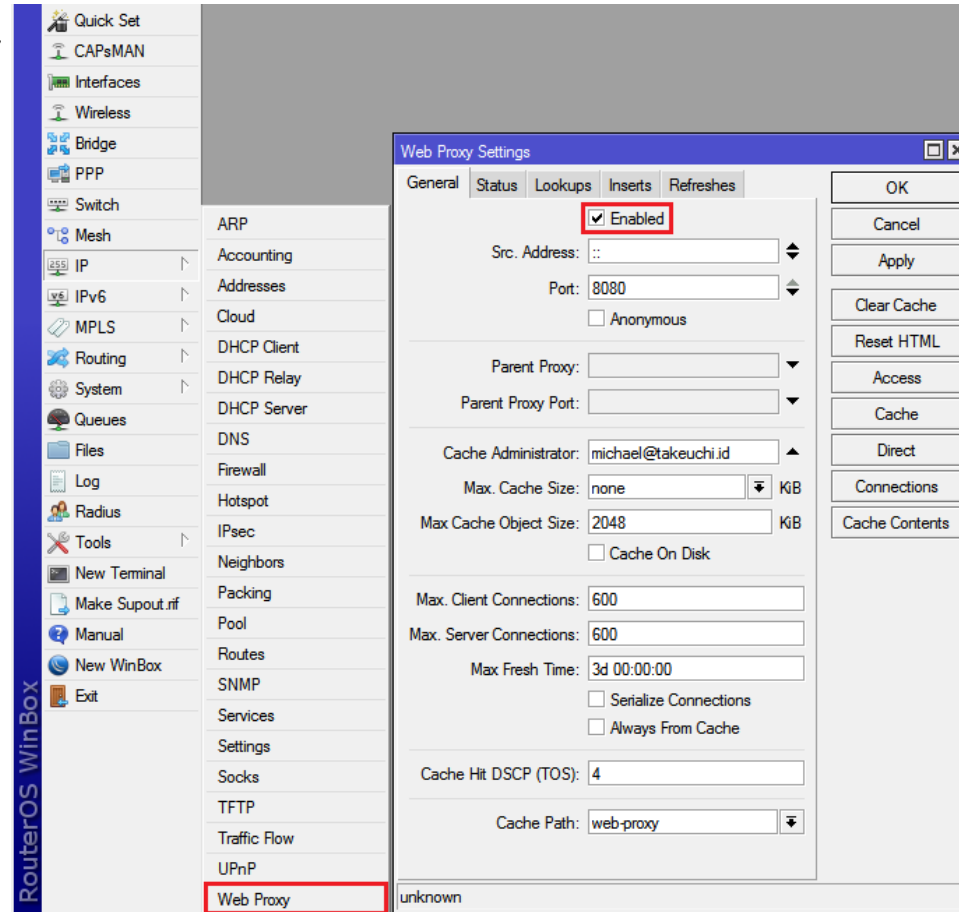
- Doesn't work at all with HTTPS traffic
- Work as Content Cache & Filter Server
- Router Storage Killer (we can set the limit)
- All of HTTP Traffic must be redirected to router
- Can be used to block HTTP website or redirect to a new website

```
/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

The screenshot shows the 'Web Proxy Access' configuration window. At the top, there are buttons for adding, removing, and applying rules, along with 'Reset Counters' and 'Reset All Counters' buttons. A table below lists the current rules:

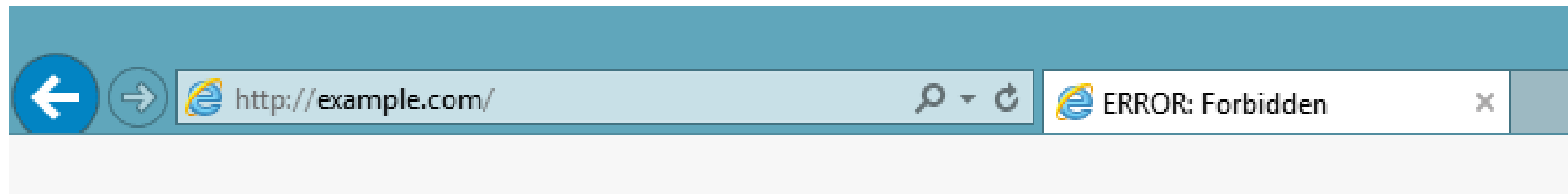
| # | Src. Address   | Dst. Address | Dst. Port | Dst. Host     | Path | Method | Action | Redirect To | Hits |
|---|----------------|--------------|-----------|---------------|------|--------|--------|-------------|------|
| 0 | 192.168.3.0/29 |              | 80        | *.example.com |      |        | deny   |             | 0    |

A 'Web Proxy Rule <192.168.3.0/29>' dialog box is open, showing the configuration for the selected rule:

- Src. Address: 192.168.3.0/29
- Dst. Address: (empty)
- Dst. Port: 80
- Local Port: (empty)
- Dst. Host: \*.example.com
- Path: (empty)
- Method: (empty)
- Action: deny
- Redirect To: (empty)
- Hits: 0

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters. The rule is currently 'enabled'.

## 2. Web Proxy – Result



### **ERROR: Forbidden**

---

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

- **Access Denied**

Your cache administrator is [michael@takeuchi.id](mailto:michael@takeuchi.id).

---

*Generated Wed, 08 Mar 2017 22:32:22 GMT by ::ffff:192.168.3.1 (Mikrotik HttpProxy)*

# 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

New Route

General Attributes

Dst. Address: 8.8.8.8

Gateway: 192.168.137.1

Check Gateway:

Type: blackhole

Distance:

Scope: 30

blackhole

prohibit

unicast

unreachable

OK

Cancel

Apply

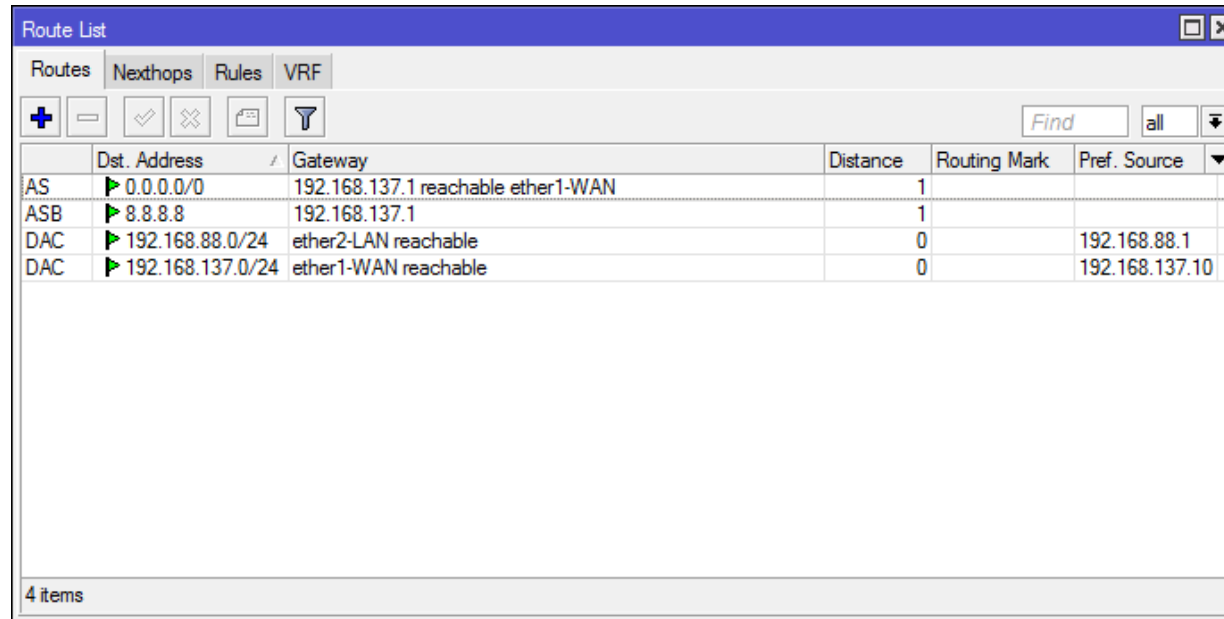
Disable

Comment

Copy

Remove

# 3. Route Policy –Testing



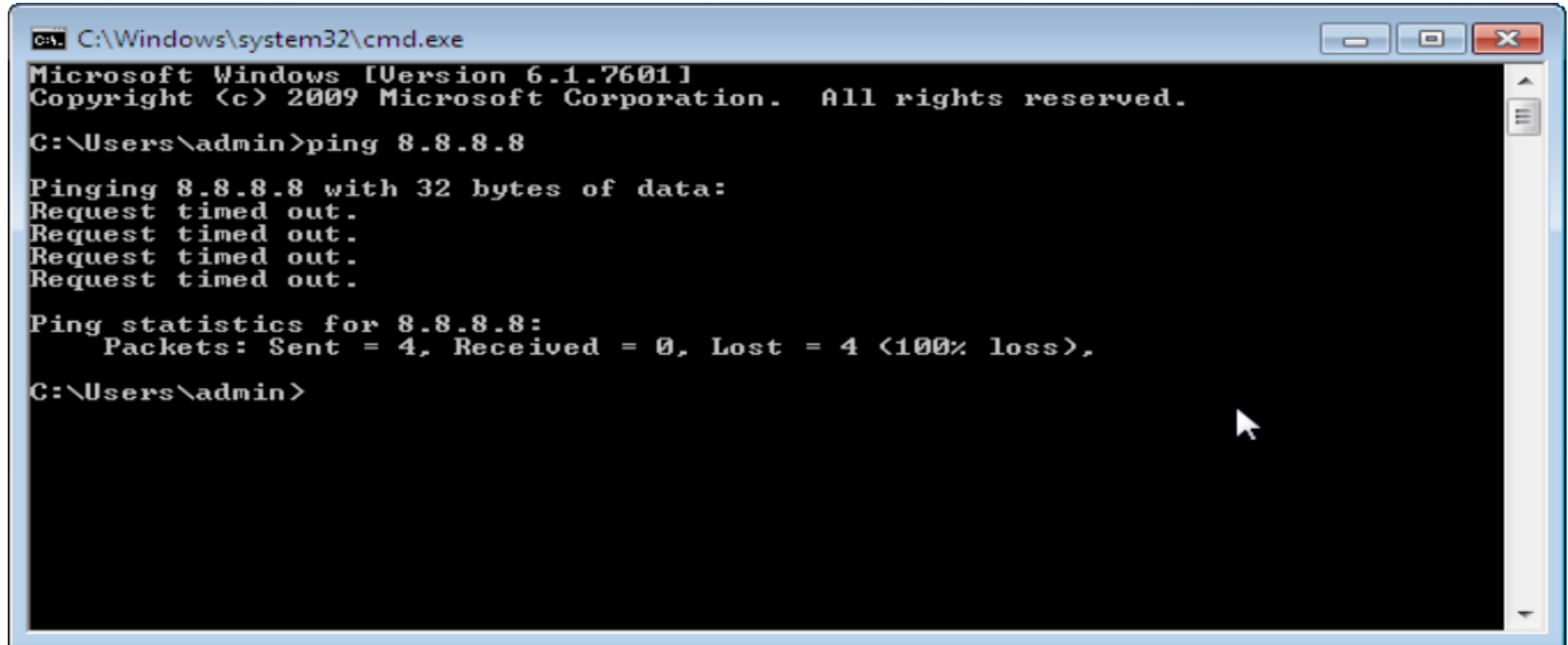
The screenshot shows the Mikrotik WinBox 'Route List' window. It has tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. Below the tabs are several icons: a plus sign, a minus sign, a checkmark, a cross, a document, and a funnel. A search bar labeled 'Find' is on the right. The main area contains a table with the following data:

|     | Dst. Address     | Gateway                            | Distance | Routing Mark | Pref. Source   |
|-----|------------------|------------------------------------|----------|--------------|----------------|
| AS  | 0.0.0.0/0        | 192.168.137.1 reachable ether1-WAN | 1        |              |                |
| ASB | 8.8.8.8          | 192.168.137.1                      | 1        |              |                |
| DAC | 192.168.88.0/24  | ether2-LAN reachable               | 0        |              | 192.168.88.1   |
| DAC | 192.168.137.0/24 | ether1-WAN reachable               | 0        |              | 192.168.137.10 |

At the bottom of the window, it says '4 items'.

```
[admin@MikroTik] > ping 8.8.8.8
SEQ HOST                SIZE TTL TIME STATUS
0
1
2
3
4
5
6
7
8
9
10
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>
```

The screenshot shows a Windows Command Prompt window with a blue title bar. The window title is "C:\Windows\system32\cmd.exe". The text inside the window shows the output of a ping command to 8.8.8.8. The output indicates that all four packets sent were lost, resulting in a 100% loss. The window has standard Windows window controls (minimize, maximize, close) in the top right corner and a scroll bar on the right side.



# 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.

[https://wiki.mikrotik.com/wiki/Manual:IP/Route#Route\\_flags](https://wiki.mikrotik.com/wiki/Manual:IP/Route#Route_flags)

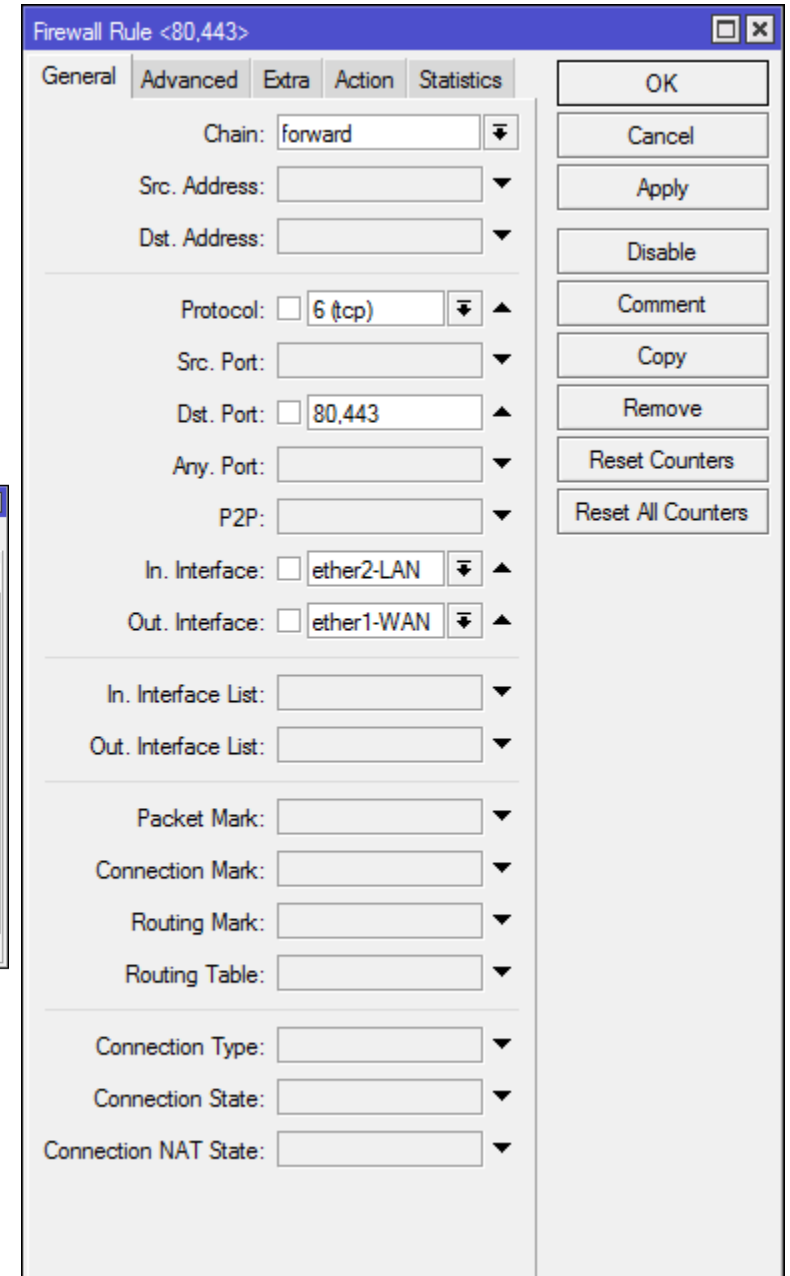
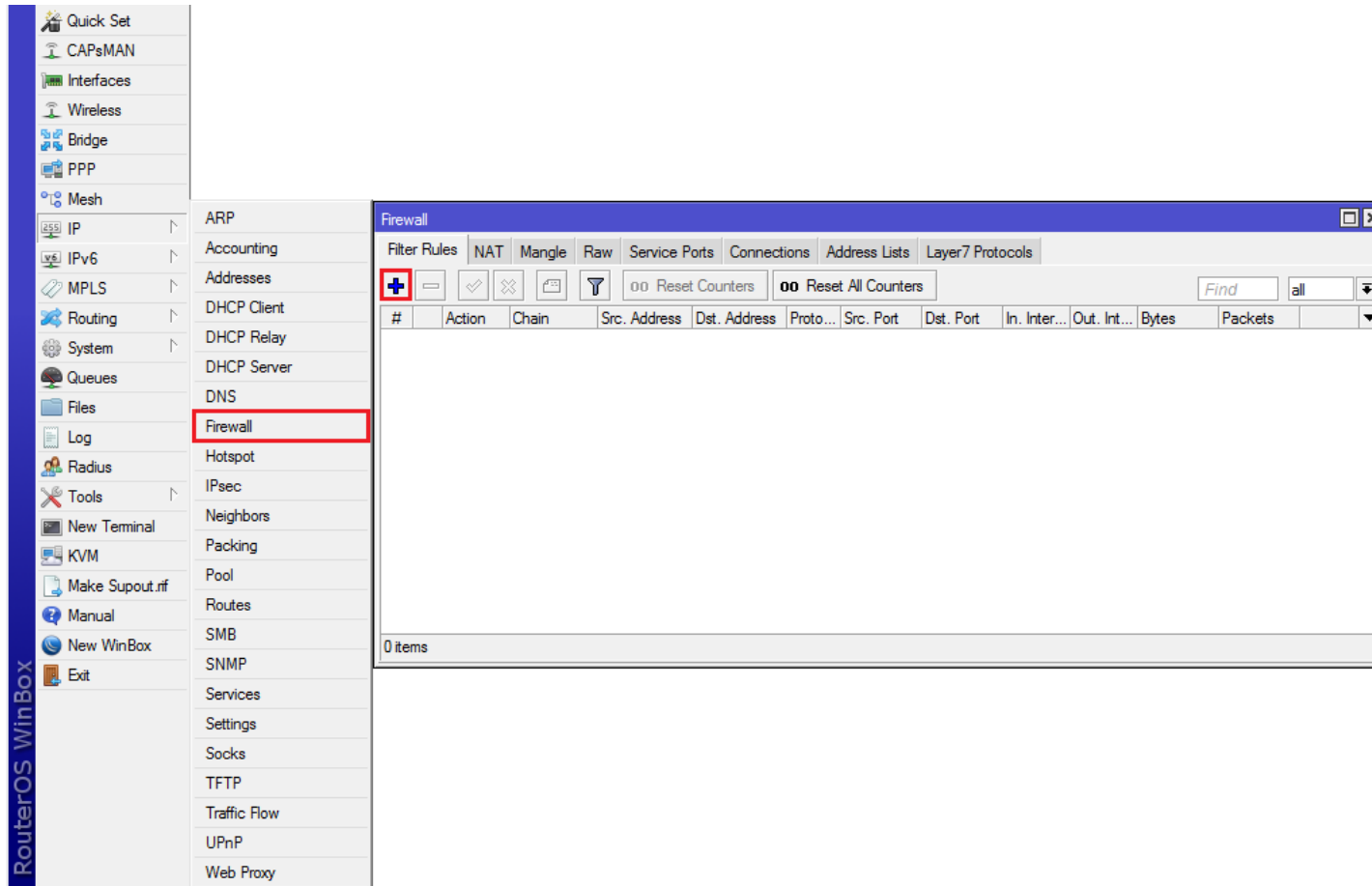
## 4. Content Filter

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

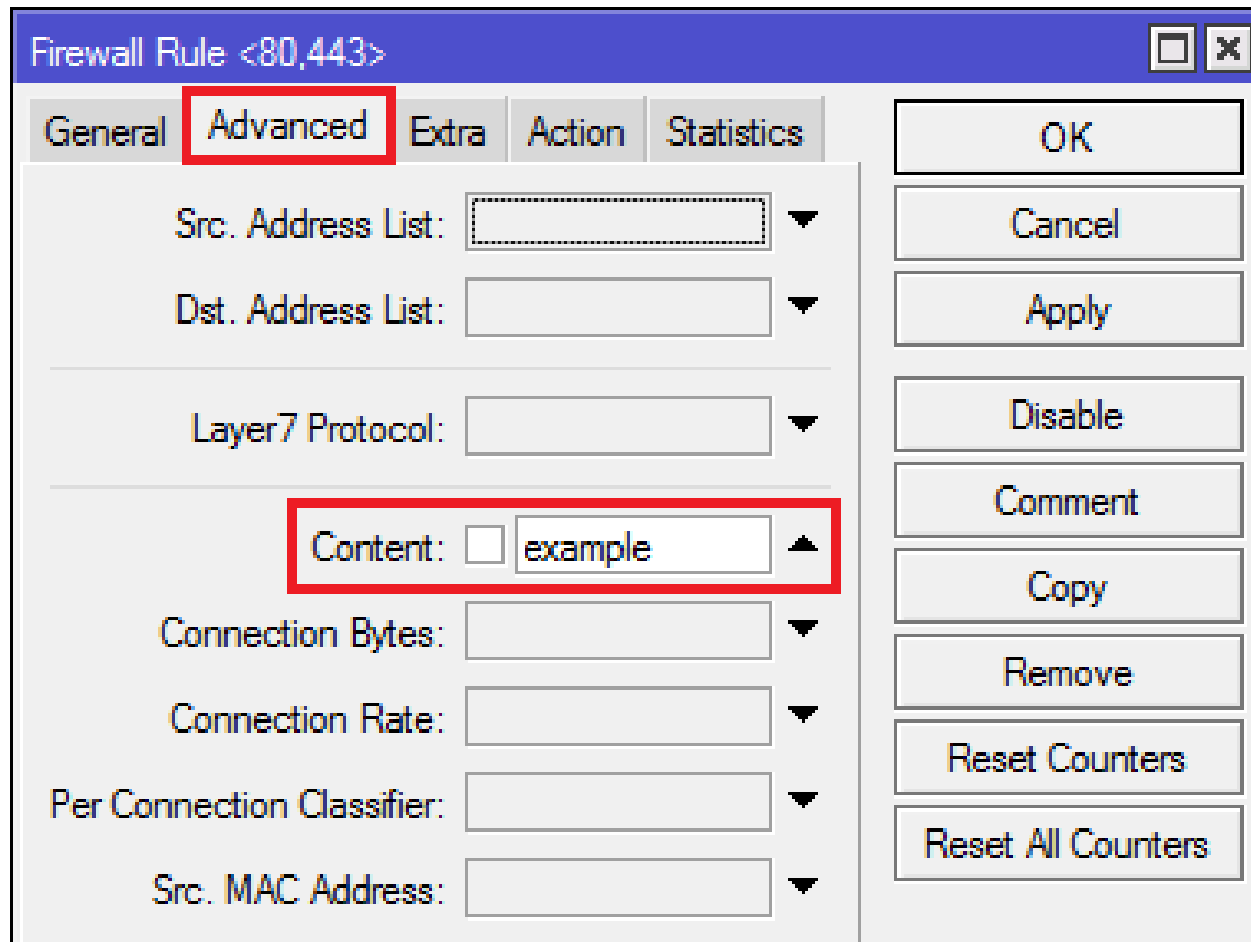
- We will try to block packet which contain **example**

```
/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

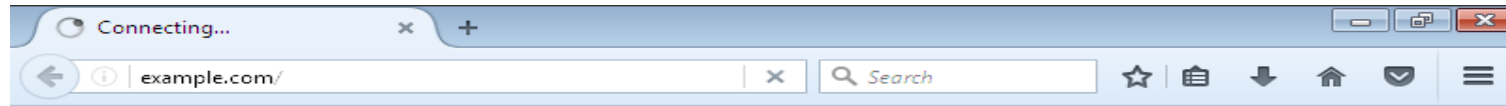


## 4. Content Filter – Applying



# 4. Content Filter – Result

- We can't access example.com with TCP/80 and TCP/443



# 4. Content Filter – Result

The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active. The rule list contains one rule with the following details:

| # | Action | Chain   | Src. Address | Dst. Address | Protocol | Src. Port | Dst. Port | In. Interface | Out. Interface | Layer7 Protocol | Content | Bytes   | Packets |
|---|--------|---------|--------------|--------------|----------|-----------|-----------|---------------|----------------|-----------------|---------|---------|---------|
| 0 | ✖ drop | forward |              |              | 6 (tcp)  |           | 80,443    | ether2-LAN    | ether1-WAN     |                 | example | 7.5 KiB | 22      |

## 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)+.*`

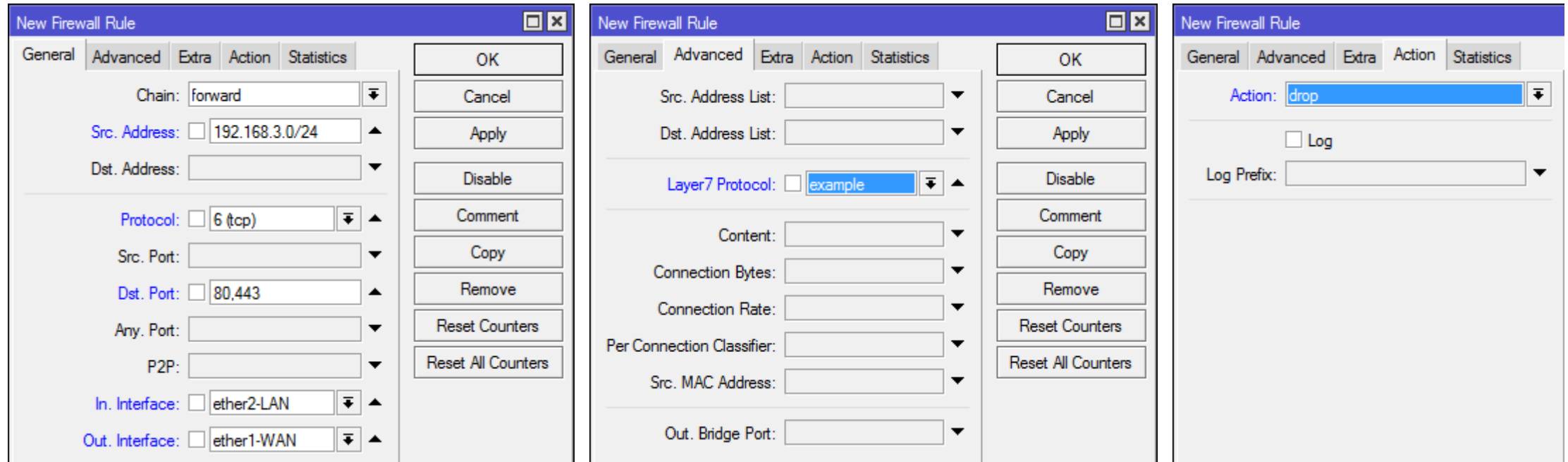
|                       |  |                 |   |                     |                             |
|-----------------------|--|-----------------|---|---------------------|-----------------------------|
| <code>[abc]</code>    | A single character of: a, b, or c            | <code>.</code>  | Any single character                            | <code>(...)</code>  | Capture everything enclosed |
| <code>[^abc]</code>   | Any single character except: a, b, or c      | <code>\s</code> | Any whitespace character                        | <code>(a b)</code>  | a or b                      |
| <code>[a-z]</code>    | Any single character in the range a-z        | <code>\S</code> | Any non-whitespace character                    | <code>a?</code>     | Zero or one of a            |
| <code>[a-zA-Z]</code> | Any single character in the range a-z or A-Z | <code>\d</code> | Any digit                                       | <code>a*</code>     | Zero or more of a           |
| <code>^</code>        | Start of line                                | <code>\D</code> | Any non-digit                                   | <code>a+</code>     | One or more of a            |
| <code>\$</code>       | End of line                                  | <code>\w</code> | Any word character (letter, number, underscore) | <code>a{3}</code>   | Exactly 3 of a              |
| <code>\A</code>       | Start of string                              | <code>\W</code> | Any non-word character                          | <code>a{3,}</code>  | 3 or more of a              |
| <code>\z</code>       | End of string                                | <code>\b</code> | Any word boundary                               | <code>a{3,6}</code> | Between 3 and 6 of a        |

options: `i` case insensitive   `m` make dot match newlines   `x` ignore whitespace in regex   `o` perform `#{...}` substitutions only once

```
/ip firewall layer7-protocol add name=example regexp=".*(example)+.*"
```



# 5. Layer 7 Firewall – Applying

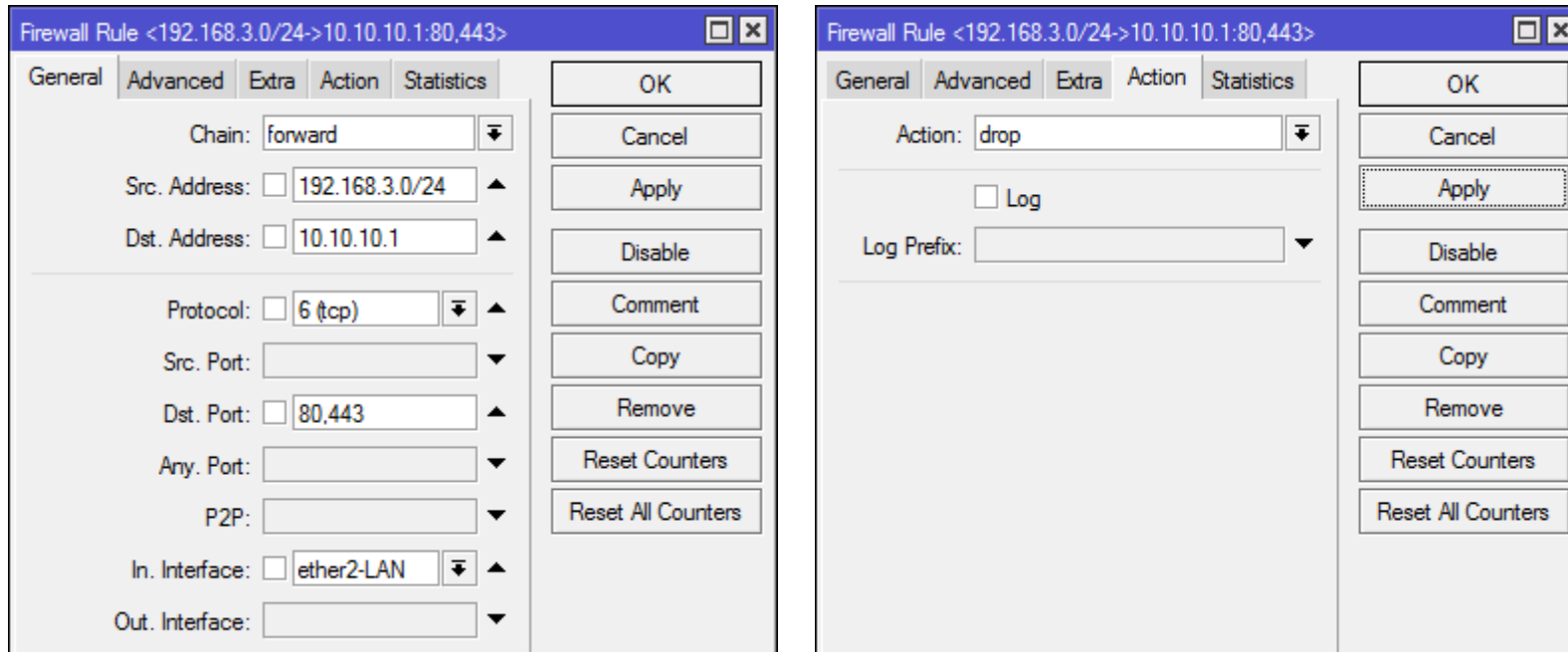


We are try to block or drop on filter rule with Layer 7 regex too, we can do more creation with it, just be creative 😊

## 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)

## 6. Dst. IP Address/Port Block – Applying (1)



We are try to a local website

```
/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)

The image displays four screenshots from Mikrotik WinBox illustrating the configuration of a firewall rule to block traffic to specific IP addresses and ports.

- Firewall Filter Rules:** A list of 15 rules, all named 'local-website', with destination addresses ranging from 10.10.10.10 to 10.10.10.150.
- Firewall Rule <192.168.3.0/24->80,443> (General):** Chain: forward; Src. Address: 192.168.3.0/24; Dst. Address: (empty); Protocol: 6 (tcp); Src. Port: (empty); Dst. Port: 80,443; In. Interface: ether2-LAN; Out. Interface: (empty).
- Firewall Rule <192.168.3.0/24->80,443> (Advanced):** Src. Address List: (empty); Dst. Address List: local-website; Layer7 Protocol: (empty); Content: (empty); Connection Bytes: (empty); Connection Rate: (empty); Per Connection Classifier: (empty); Src. MAC Address: (empty); Out. Bridge Port: (empty).
- Firewall Rule <192.168.3.0/24->80,443> (Action):** Action: drop; Log: (unchecked); Log Prefix: (empty).

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)

| Name             | Address        | Creation Time        |
|------------------|----------------|----------------------|
| blocked-web      | facebook.com   | Mar/25/2017 08:57:19 |
| ::: facebook.com |                |                      |
| D blocked-web    | 31.13.78.35    | Mar/25/2017 09:02:48 |
| blocked-web      | youtube.com    | Mar/25/2017 09:03:02 |
| ::: youtube.com  |                |                      |
| D blocked-web    | 74.125.200.190 | Mar/25/2017 09:03:02 |
| ::: youtube.com  |                |                      |
| D blocked-web    | 74.125.200.136 | Mar/25/2017 09:03:02 |
| ::: youtube.com  |                |                      |
| D blocked-web    | 74.125.200.93  | Mar/25/2017 09:03:02 |
| ::: youtube.com  |                |                      |
| D blocked-web    | 74.125.200.91  | Mar/25/2017 09:03:02 |

| Name        | Address      | Timeout | Creation Time        |
|-------------|--------------|---------|----------------------|
| blocked-web | facebook.com |         | Mar/25/2017 08:57:19 |

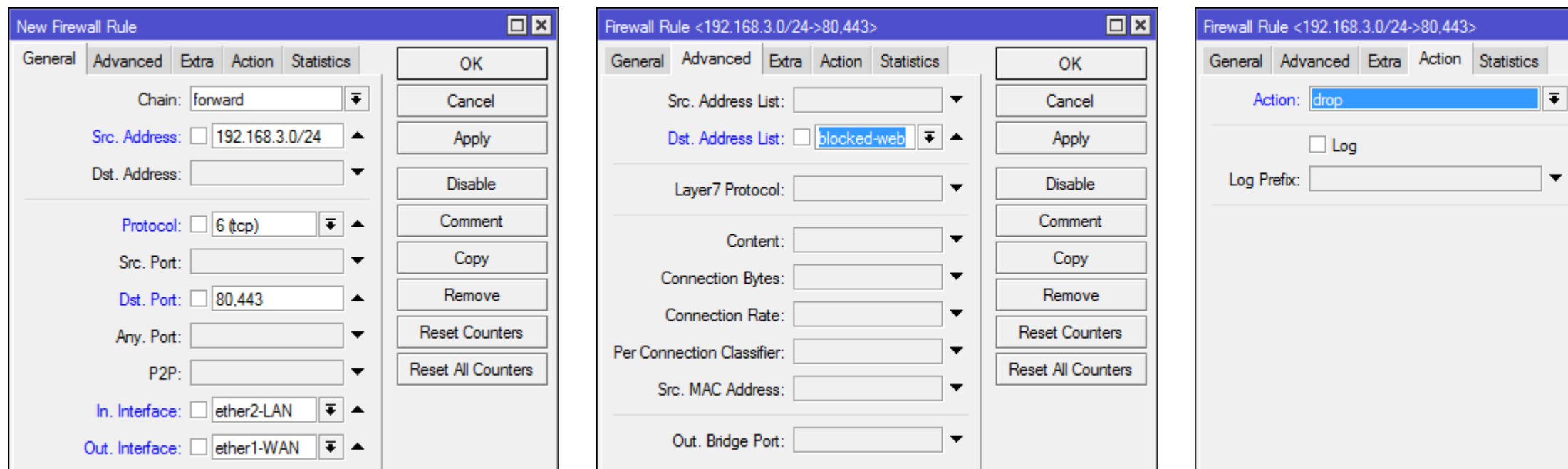
We are try to block using dynamic address-list, create the address-list first  
`/ip firewall address-list add list=blocked-web address=facebook.com`

`/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 try 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
```

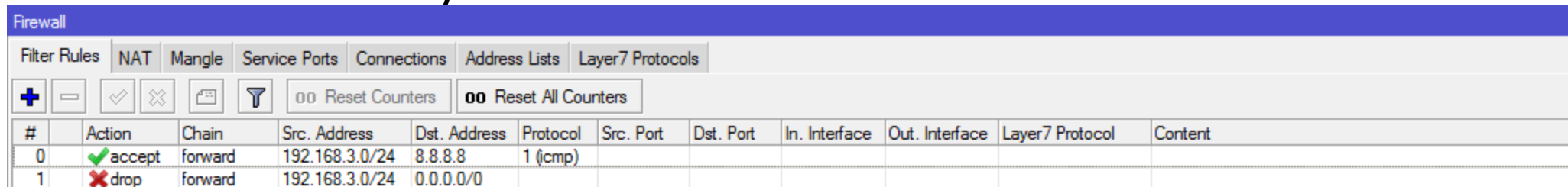
```
add action=drop chain=forward dst-port=1701 in-interface=ether2-LAN out-interface=ether1-WAN protocol=udp
```

# 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
```



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active. The table below shows two rules:

| # | Action   | Chain   | Src. Address   | Dst. Address | Protocol | Src. Port | Dst. Port | In. Interface | Out. Interface | Layer7 Protocol | Content |
|---|----------|---------|----------------|--------------|----------|-----------|-----------|---------------|----------------|-----------------|---------|
| 0 | ✓ accept | forward | 192.168.3.0/24 | 8.8.8.8      | 1 (icmp) |           |           |               |                |                 |         |
| 1 | ✗ drop   | forward | 192.168.3.0/24 | 0.0.0.0/0    |          |           |           |               |                |                 |         |

Question & Answer



Question  
&  
Answer



& don't feel so hard to contact or consult with me  
I am available on [michael\[at\]takeuchi\[dot\]id](mailto:michael@takeuchi.id)  
and listed in **MikroTik Certified Consultant**