



จัดการ Content ให้อยู่หมัดด้วย RouterOS!

Presented by Mana Kaewcharoen
MUM Thailand 2018

ประวัติวิทยากร

Mana Kaewcharoen



- CEO VRProService Co.,Ltd.
- MikroTik Certified Trainer & Consultant
- MikroTik Academy Trainer



ทำไมต้องจัดการ Content!

- Content หรือ “เนื้อหา” ในที่นี้หมายถึง เว็บไซต์ , วิดีโอ , ไฟล์ต่างๆ , อีเมล หรือข้อมูลต่างๆที่อยู่บนอินเทอร์เน็ต
- การจำกัดการเข้าถึง “เนื้อหา” ต่างๆอาจมีเหตุผลหลายประการเช่น
 - กฎระเบียบหรือข้อบังคับของหน่วยงาน
 - การควบคุม โดยผู้ปกครอง
 - คัดกรองจากหน่วยงานรัฐ
 - ประเด็นเรื่องกฎหมาย
 - ด้านความปลอดภัย
 - อื่นๆ

ตัวอย่าง: การจัดการเนื้อหา



เว็บไซต์นี้มีเนื้อหาและข้อมูลที่ไม่เหมาะสม
ถูกระงับโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เครื่องมือจัดการ Content!

- DNS (/ip dns)
- IP, Protocol, Port, Address lists (/ip firewall)
- Content (/ip firewall)
- TLS Host (/ip firewall)
- Layer 7 protocols (/ip firewall)
- Routing (/ip route)
- Web Proxy (/ip proxy)



การเลือกเครื่องมือ

เนื้อหา	เครื่องมือจัดการ
HTTP	DNS, Protocol+Port, Content, Web Proxy
HTTPS	DNS, Procol+Port, TLS Host
Video, File	Layer 7 Protocols
Torrents	Layer 7 Protocols
Facebook	DNS, IP, Layer 7 Protocols, Routing
YouTube	DNS, TLS Host, Layer 7 Protocols
Line	IP, Routing, Layer 7 Protocols

DNS (Static DNS)

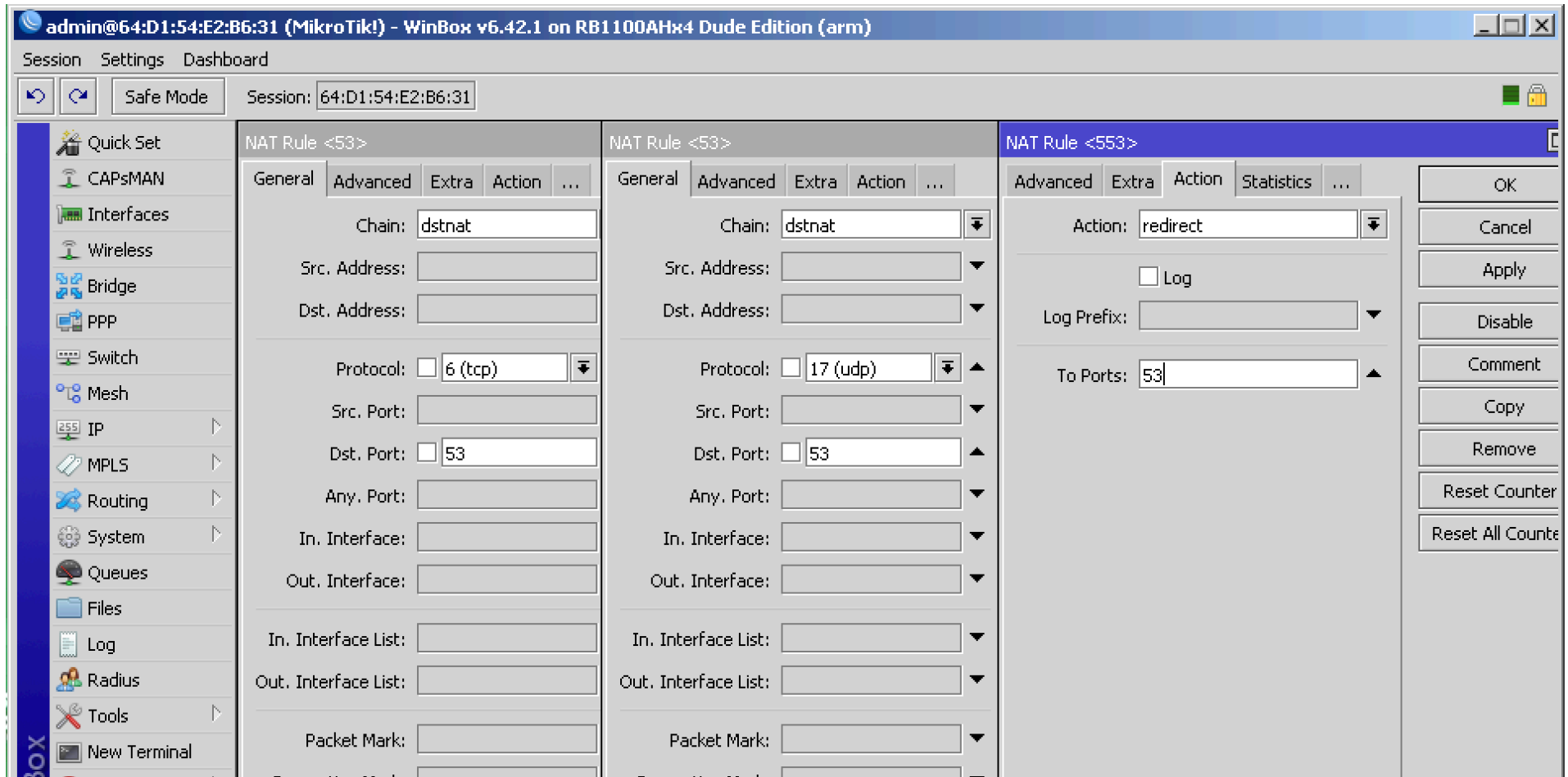
- การตั้งค่า Static DNS จะช่วยให้การเรียก DNS วิ่งมาหาที่ตัว Router เพื่อแปลงชื่อที่เรียกไปเป็นหมายเลข IP Address แต่จะต้องตั้งค่า Transparent DNS ตามตัวอย่างด้านล่างนี้

```
/ip firewall nat add action=redirect chain=dstnat dst-port=53 protocol=udp to-ports=53
```

```
/ip firewall nat add action=redirect chain=dstnat dst-port=53 protocol=tcp to-ports=53
```

```
/ip dns static add address=110.164.86.34 name=www.xxx.com
```

DNS (Static DNS)



ตัวอย่างการตั้งค่าใน /ip firewall nat

DNS (Static DNS)

The screenshot shows the Mikrotik WinBox interface. The top bar indicates the user is 'admin@64:D1:54:E2:B6:31 (MikroTik!)' on 'WinBox v6.42.1 on RB1100AHx4 Dude Edition (arm)'. The main menu includes 'Session', 'Settings', and 'Dashboard'. Below this, there are navigation buttons for 'Safe Mode' and 'Session: 64:D1:54:E2:B6:31'. The left sidebar contains various system settings categories: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, and Routing. The main window displays the 'DNS Static' configuration page. It features a table with columns for '#', 'Name', 'Regexp', 'Address', and 'TTL (s)'. A single entry is shown with '# 0', 'Name www.xxx.com', 'Regexp', 'Address 110.164.186.34', and 'TTL (s) 1d 00:00:00'. A 'Find' search box is located to the right of the table. Below the table, a 'DNS Static Entry <www.xxx.com>' dialog box is open, showing input fields for 'Name: www.xxx.com', 'Regexp:', 'Address: 110.164.186.34', and 'TTL: 1d 00:00:00 s'. The dialog also includes buttons for 'OK', 'Cancel', 'Apply', 'Disable', and 'Comment'.

ตัวอย่างการตั้งค่าใน /ip dns static

DNS (Static DNS)

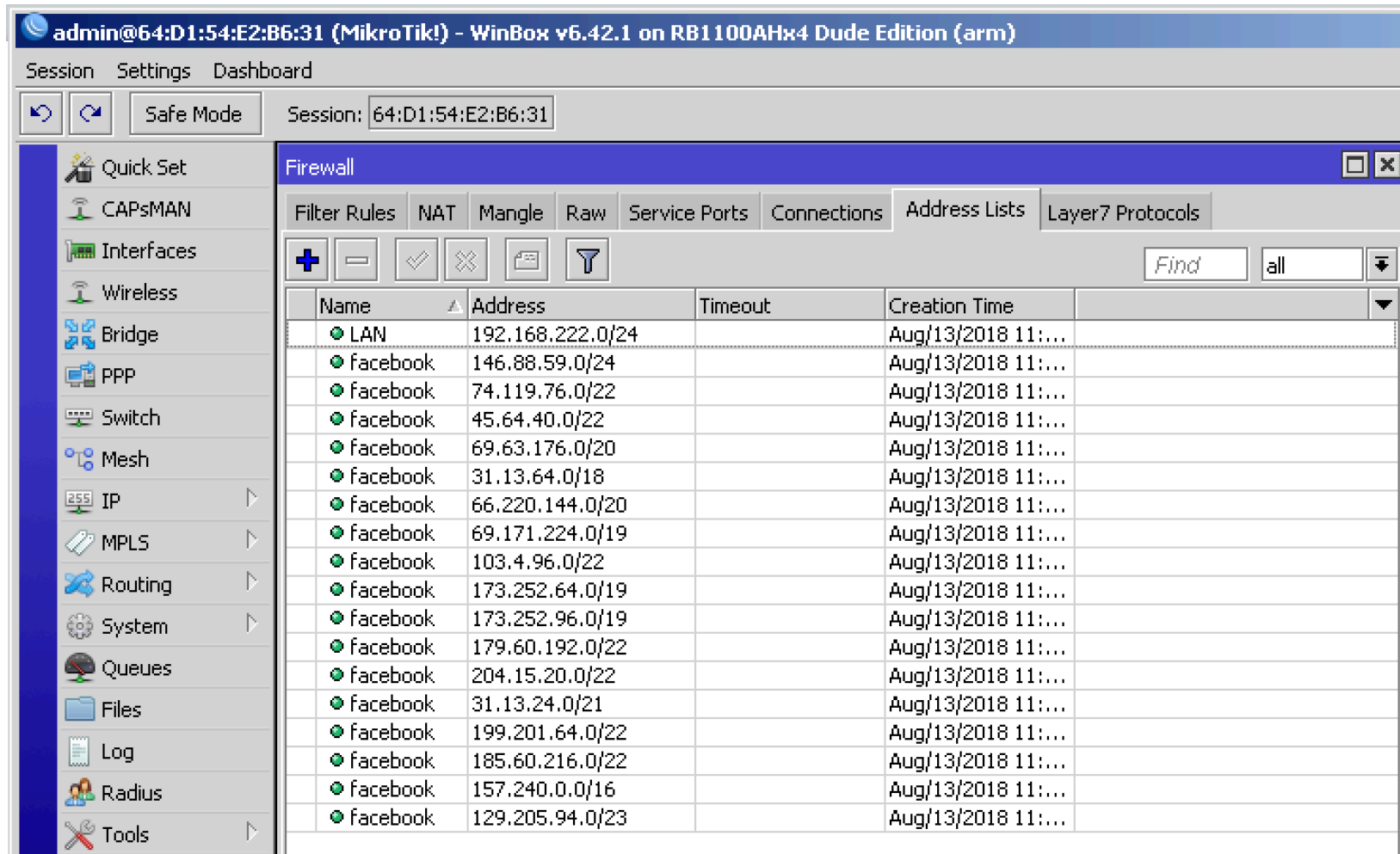


ตัวอย่างทดลองเข้าเว็บไซต์

IP, Protocol, Port, Address lists

- RouterOS มีฟีเจอร์มาตรฐานที่ติดมาด้วยคือ Firewall อยู่ในเมนู /ip firewall สามารถระบุได้ทั้ง IP , Protocol , Port
- นอกจากนี้เรายังสามารถสร้าง Address List ไว้ใช้งานแบบกลุ่มหรือชุด IP Address ได้ทั้งแบบ Dynamic และ Static
- Address List สามารถใส่ Domain แทนการใส่ IP Address ได้ ระบบจะไปทำการดึง IP Address มาใส่ในช่องให้เอง

IP, Protocol, Port, Address lists

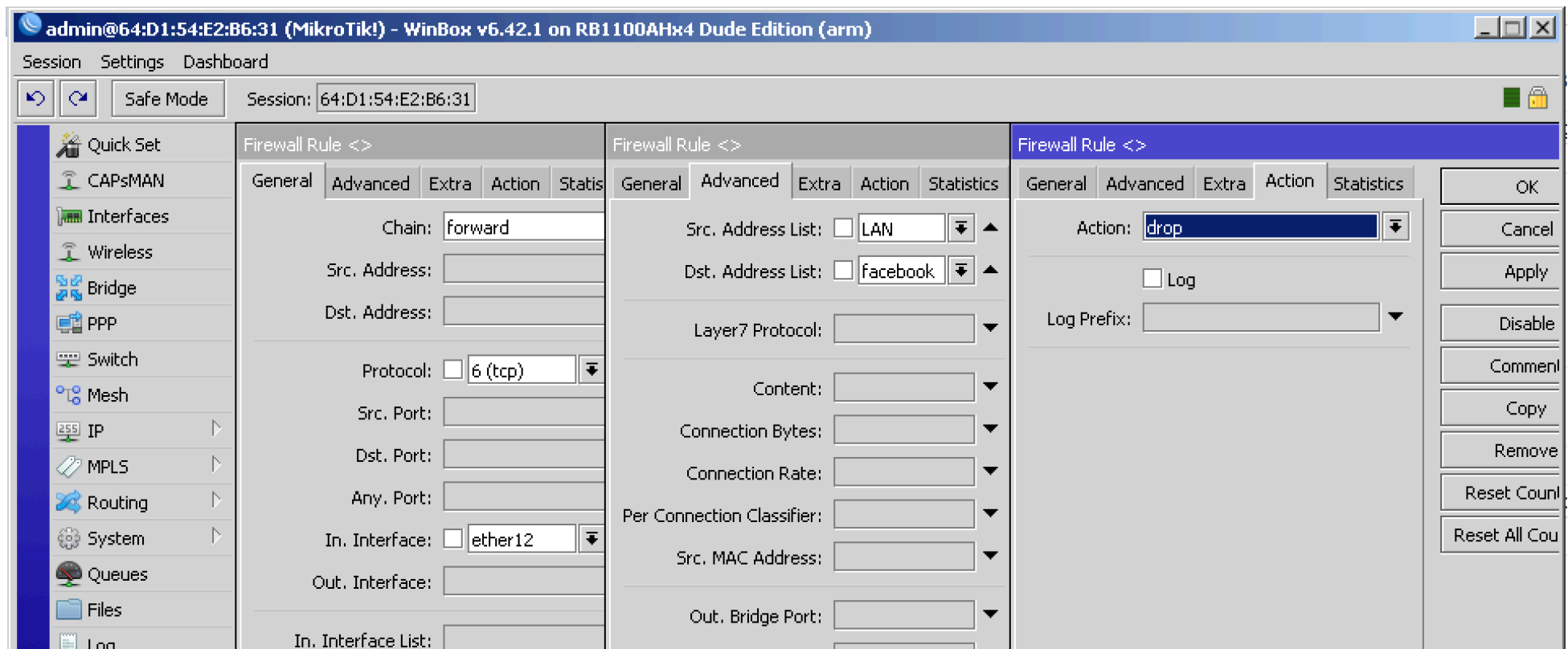


The screenshot shows the Mikrotik WinBox interface for configuring Firewall Address Lists. The left sidebar contains various system settings, and the main window displays the 'Address Lists' tab. A table lists the configured address lists, including their names, IP addresses, and creation times.

Name	Address	Timeout	Creation Time
LAN	192.168.222.0/24		Aug/13/2018 11:...
facebook	146.88.59.0/24		Aug/13/2018 11:...
facebook	74.119.76.0/22		Aug/13/2018 11:...
facebook	45.64.40.0/22		Aug/13/2018 11:...
facebook	69.63.176.0/20		Aug/13/2018 11:...
facebook	31.13.64.0/18		Aug/13/2018 11:...
facebook	66.220.144.0/20		Aug/13/2018 11:...
facebook	69.171.224.0/19		Aug/13/2018 11:...
facebook	103.4.96.0/22		Aug/13/2018 11:...
facebook	173.252.64.0/19		Aug/13/2018 11:...
facebook	173.252.96.0/19		Aug/13/2018 11:...
facebook	179.60.192.0/22		Aug/13/2018 11:...
facebook	204.15.20.0/22		Aug/13/2018 11:...
facebook	31.13.24.0/21		Aug/13/2018 11:...
facebook	199.201.64.0/22		Aug/13/2018 11:...
facebook	185.60.216.0/22		Aug/13/2018 11:...
facebook	157.240.0.0/16		Aug/13/2018 11:...
facebook	129.205.94.0/23		Aug/13/2018 11:...

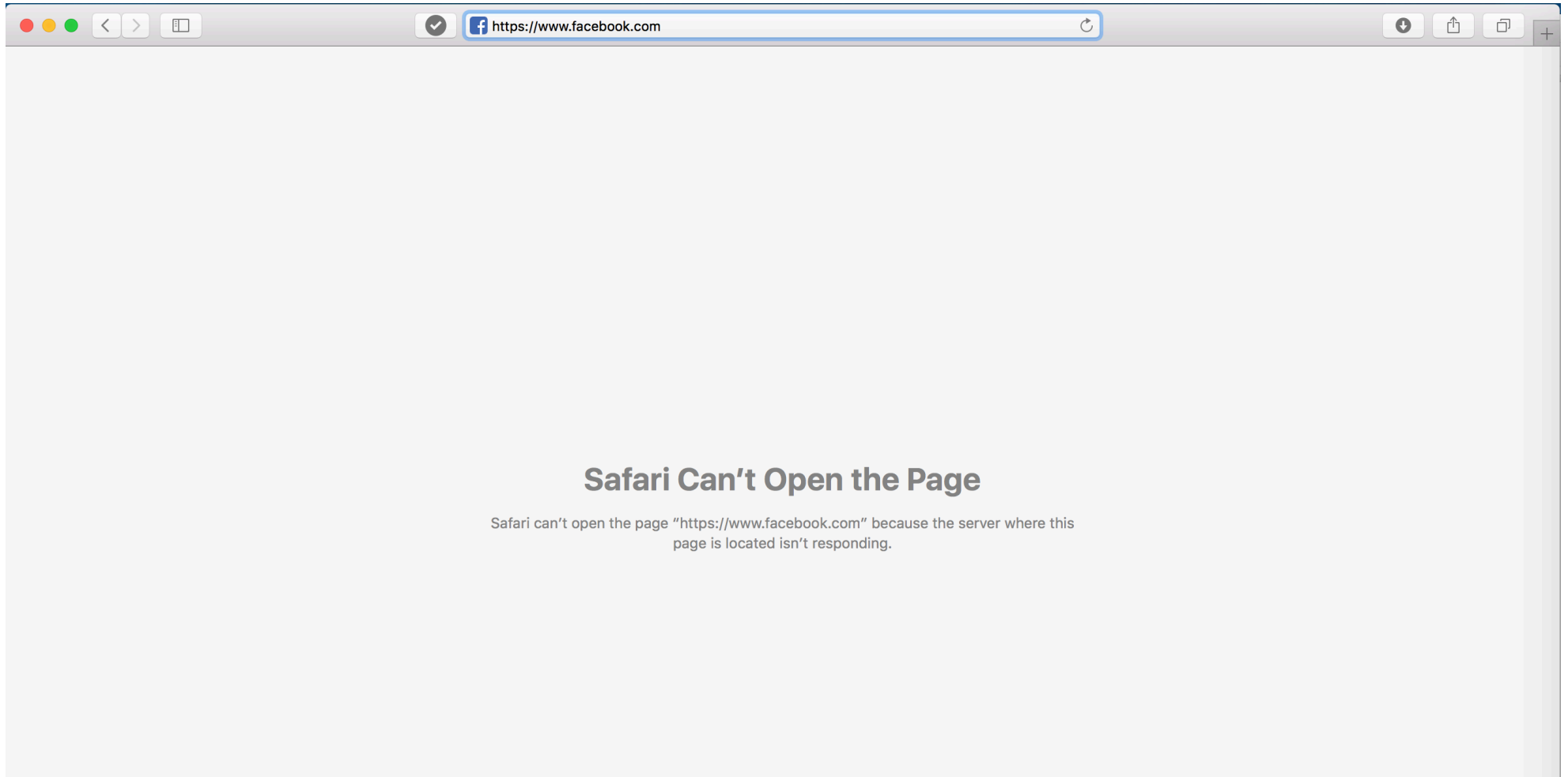
ตัวอย่างการตั้งค่าใน /ip firewall address-list

IP, Protocol, Port, Address lists



ตัวอย่างการตั้งค่าใน /ip firewall filter

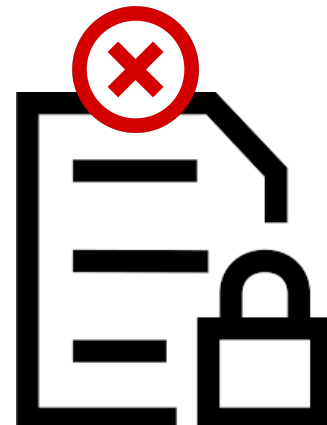
IP, Protocol, Port, Address lists



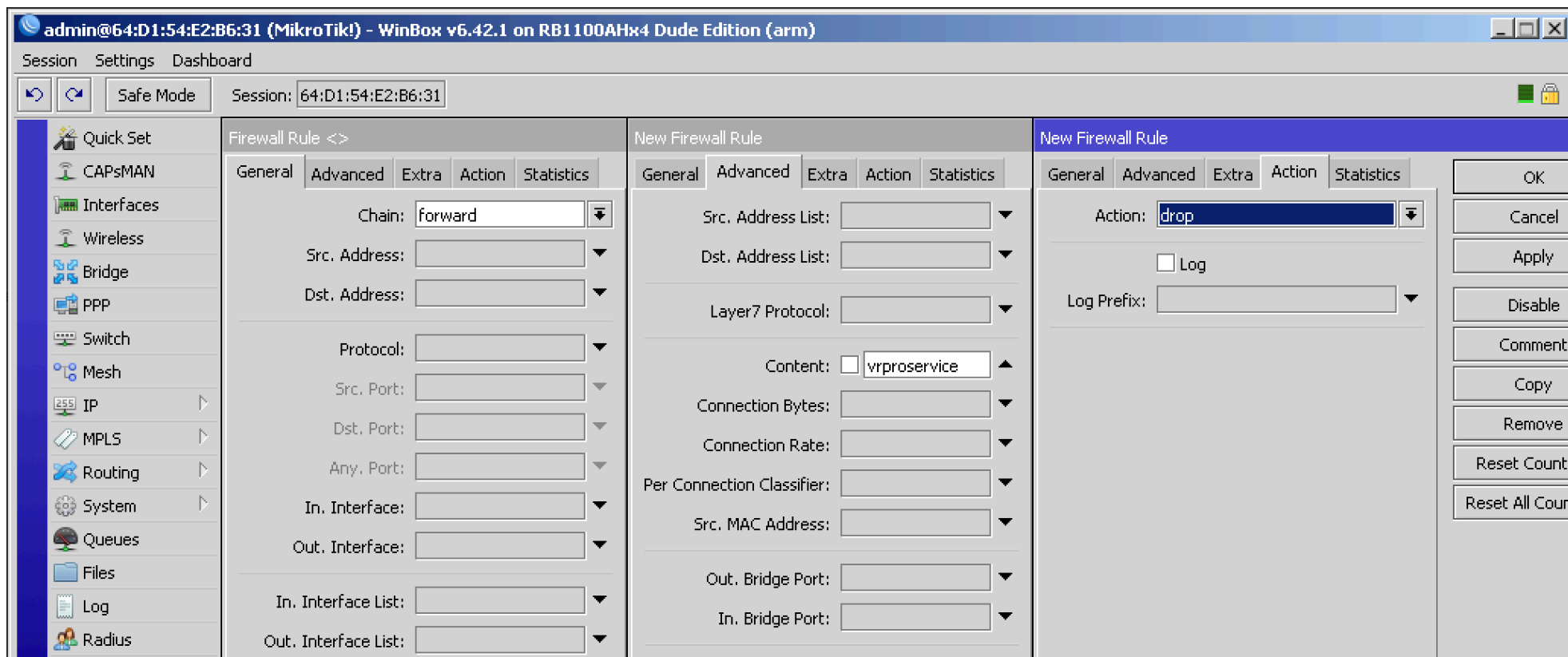
ตัวอย่างทดลองเข้าเว็บไซต์

Content

- เมนู Content ใน /ip firewall ตรงแท็บ Advanced จะมีให้เราสามารถใส่คำที่เราต้องการ หรือเรียกง่ายๆว่า Keyword
- ใช้ได้กับคำที่ไม่มีการเข้ารหัสเท่านั้น หรือที่เราเรียกกันว่า plain text และไม่สามารถใช้กับ Packet ที่มีการเข้ารหัส(encrypted) ได้

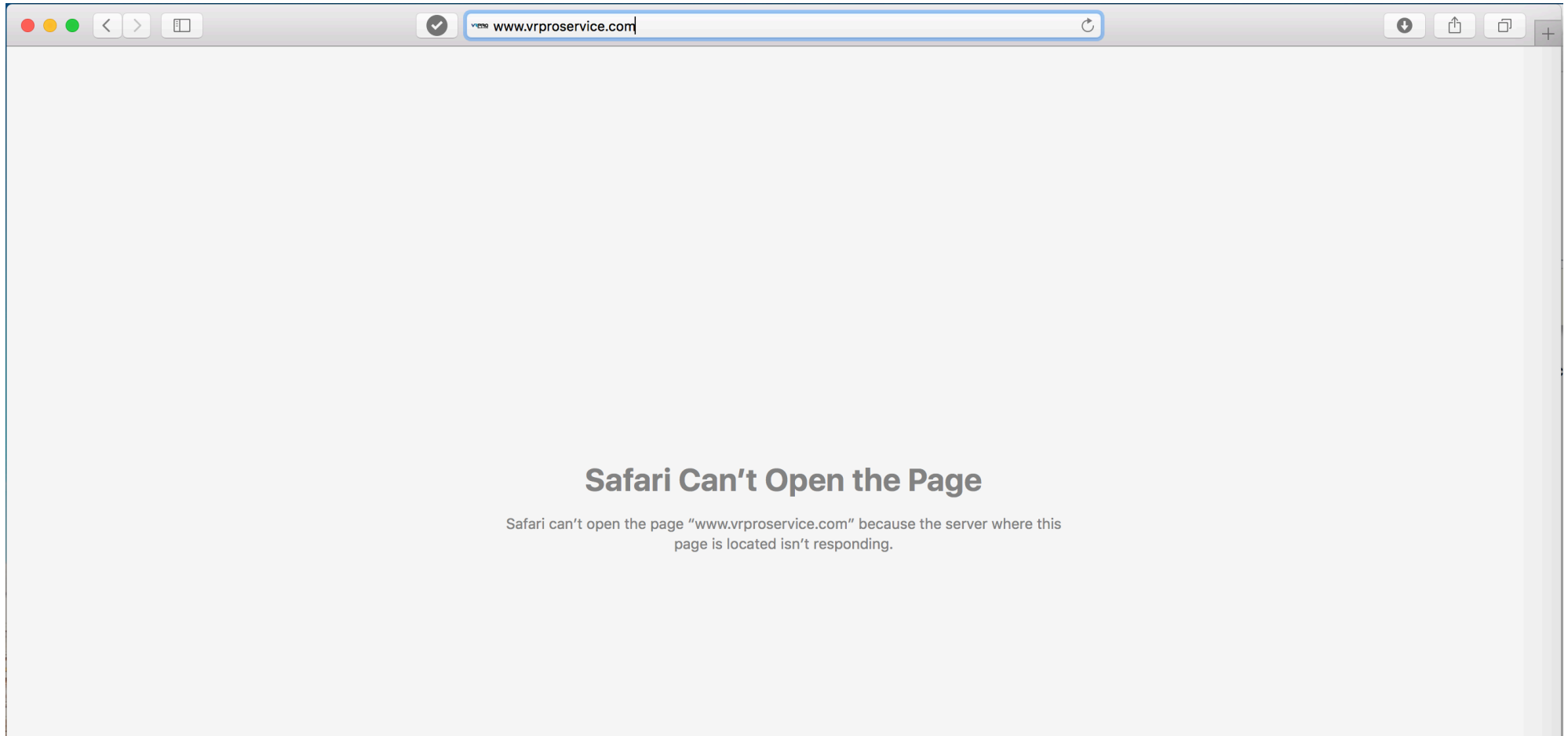


Content



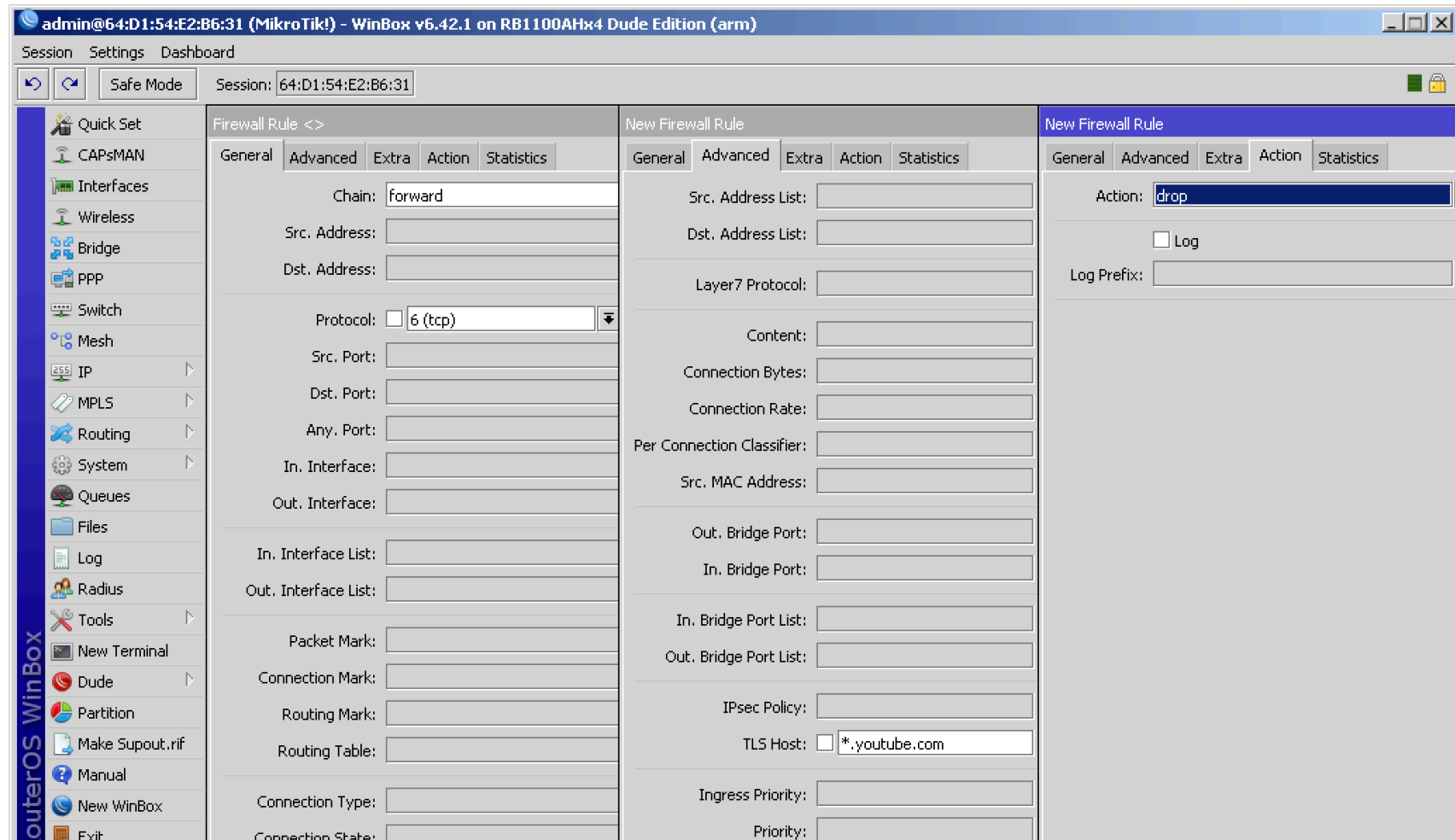
ตัวอย่างการตั้งค่าใน /ip firewall filter

Content



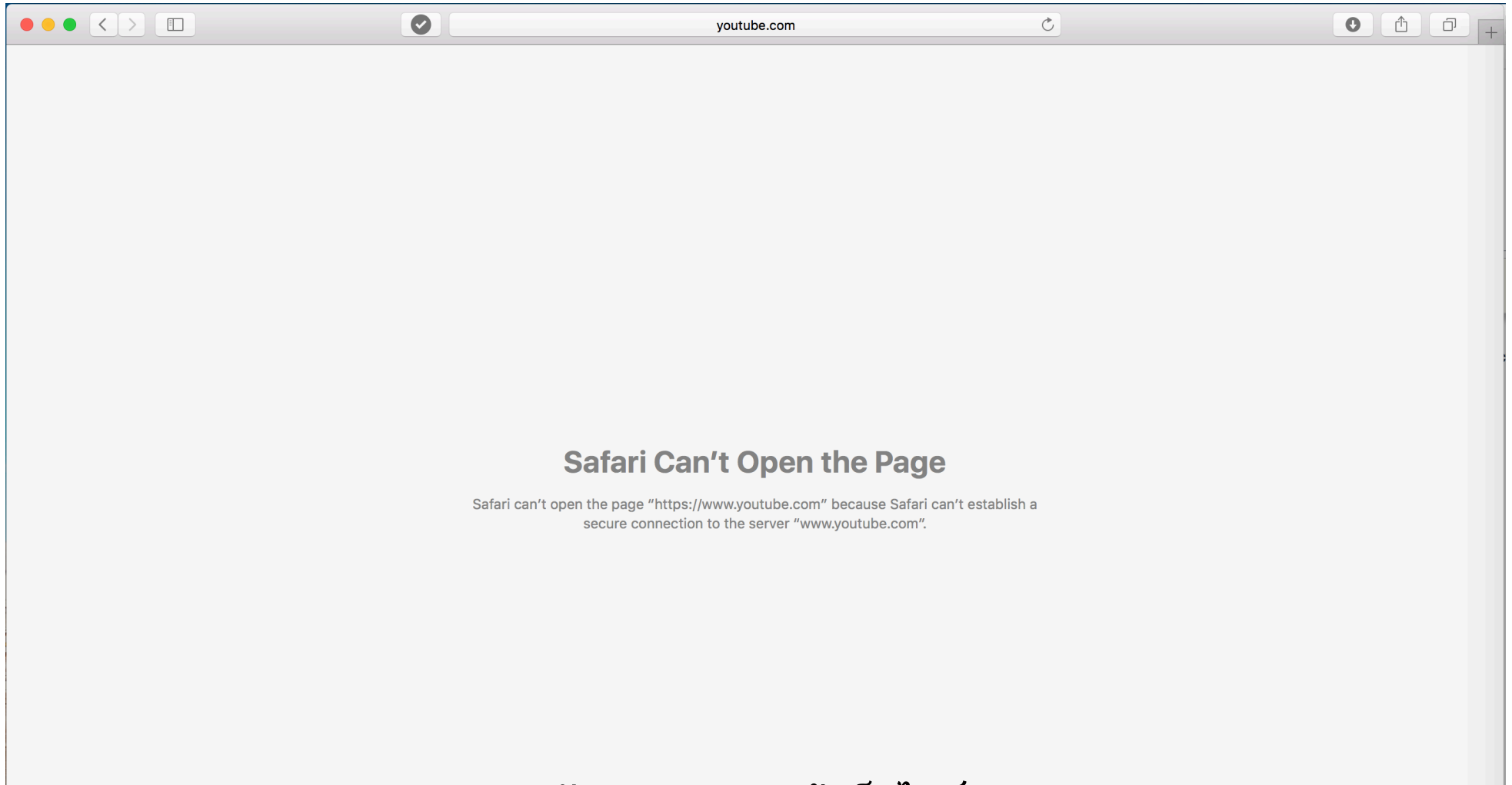
ตัวอย่างทดลองเข้าเว็บไซต์

TLS Host



ตัวอย่างการตั้งค่าใน /ip firewall filter

TLS Host



ตัวอย่างทดลองเข้าเว็บไซต์

Layer 7 Protocols

- Layer 7 Protocols จะค้นหาข้อมูลในรูปแบบ ICMP/TCP/UDP streams
- Layer 7 Protocols จะทำการค้นหา 10 Packets แรกของ Connection หรือ 2KB แรกของ Connection ที่ตรงกับ Pattern ของข้อมูลที่มี
- หากไม่พบข้อมูลที่ตรงกัน Layer 7 Protocols จะถือว่าไม่เข้ากฎหรือไม่ตรงตาม Pattern ที่มี
- ข้อควรระวังในการใช้งาน Layer 7 Protocols จะมีการเรียกใช้ CPU จำนวนมาก

การอ่านค่า regular expression

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

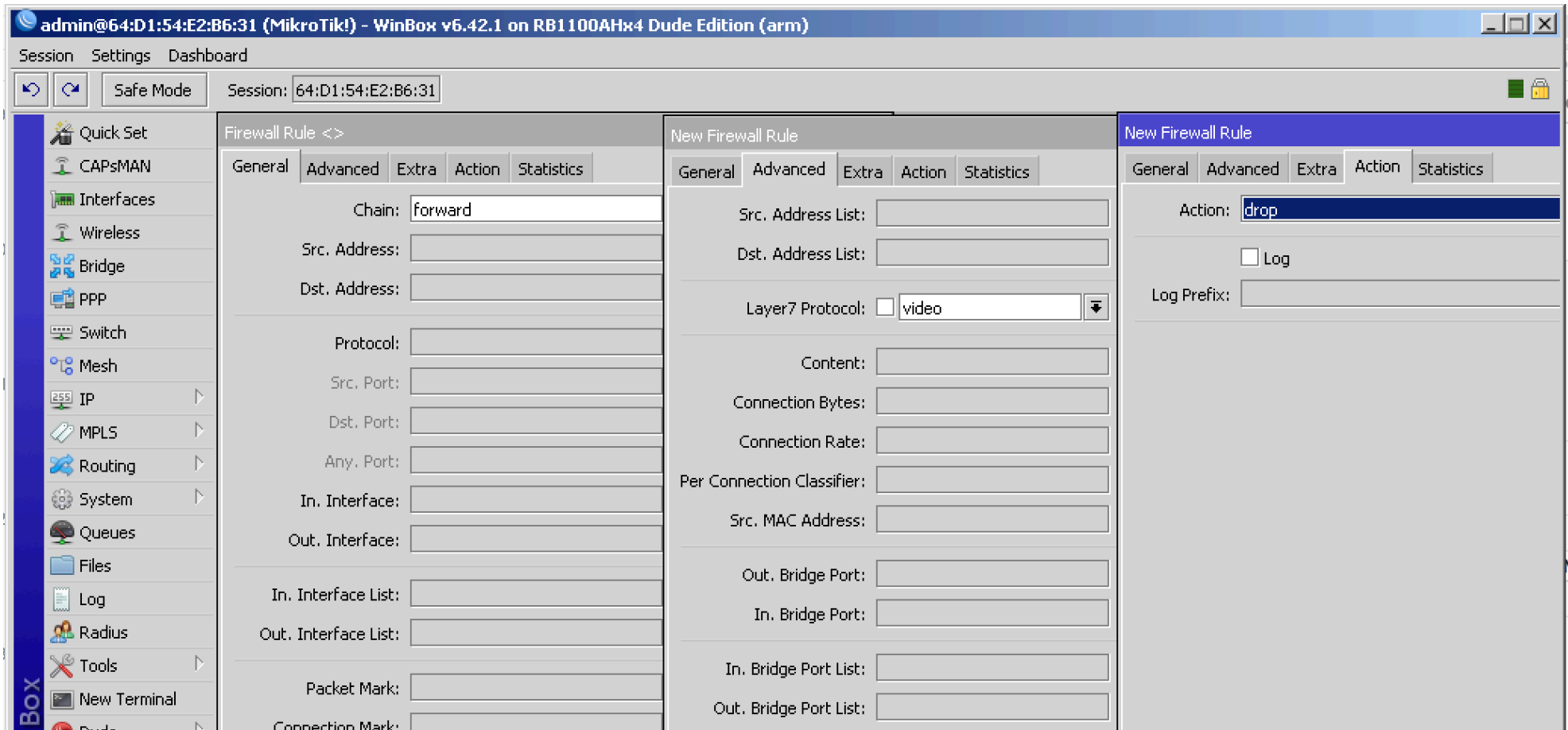
Layer 7 Protocols

The screenshot shows the Mikrotik WinBox interface for configuring Layer 7 Protocols. The 'video' protocol is selected in the list, and its configuration dialog is open. The dialog shows the name 'video' and the Regexp 'videoplayback|video'. The Regexp field is a text area with a scrollbar.

Name	Regexp
sysCurFW	3410
sysFWType	ipq8060
sysFacFW	3350
sysIntru	true
sysJail	0
sysR	3
sysROSinit	1
syscret	0987654321
sysload	Start_state2_Norm
syslog	7
video	videoplayback video

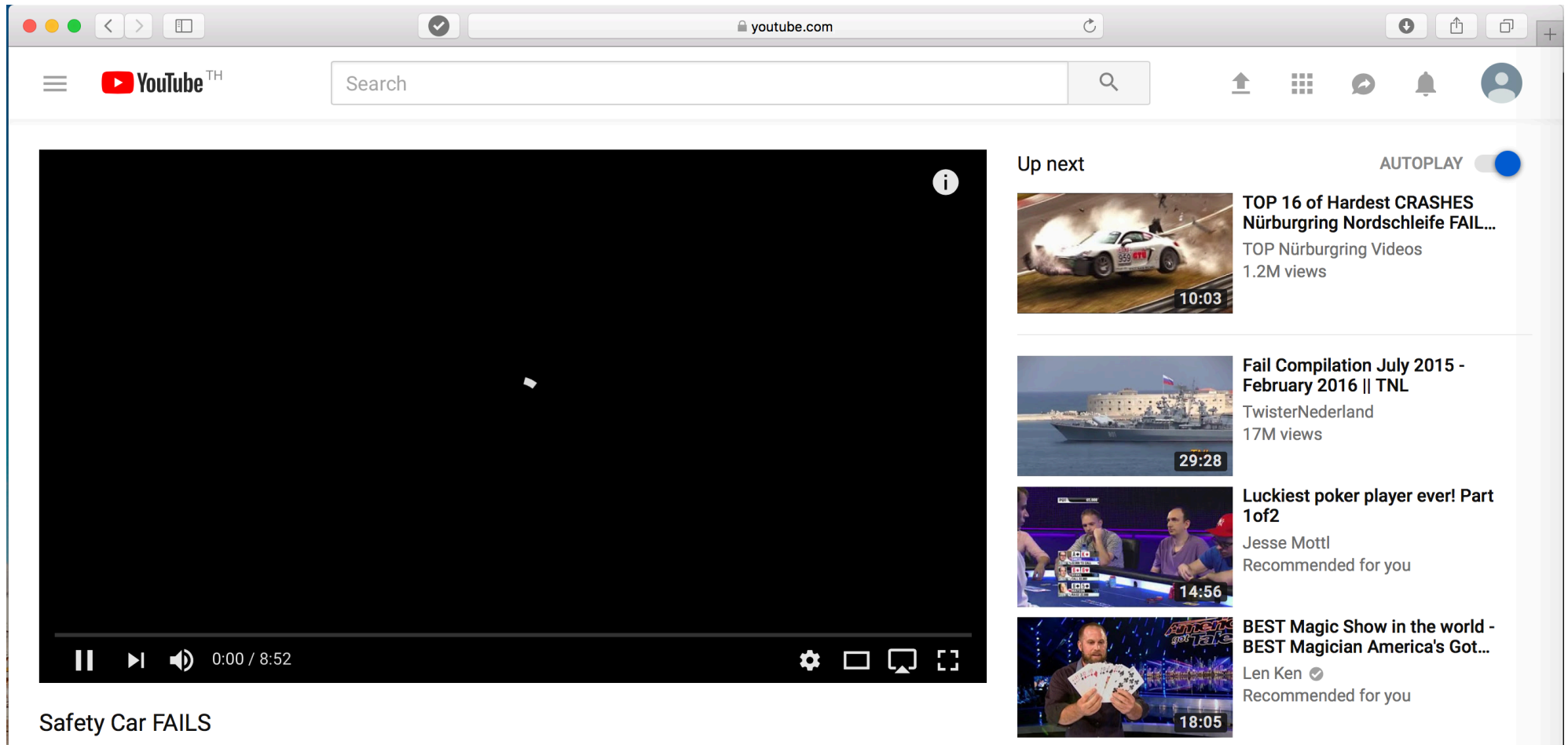
ตัวอย่างการตั้งค่าใน /ip firewall layer7-protocol

Layer 7 Protocols



ตัวอย่างการตั้งค่าใน /ip firewall filter

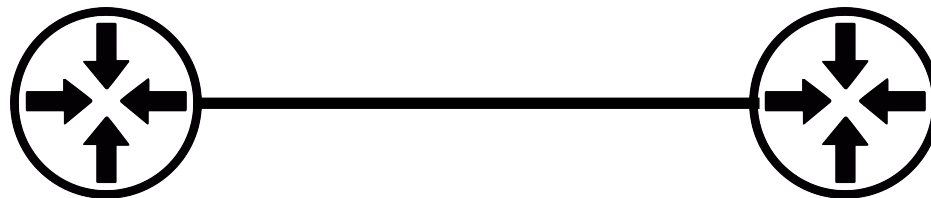
Layer 7 Protocols



ตัวอย่างทดลองเข้าเว็บไซต์

Routing

- ทำงานบน OSI Layer 3
- ไม่รองรับ โดเมนเนม
- สามารถใช้งานร่วมกับ Routing Mark ได้
- ใช้ได้กับ IP เท่านั้น (ยกเว้นใช้งานร่วมกับ Routing Mark จึงสามารถใช้อื่นๆได้เช่น Protocol, Port, Layer 7)



Routing Type

- Blackhole
 - Silently discard packet forwarded by this route
- Prohibit
 - Discard packet forwarded by this route. Notify sender with ICMP communication administratively prohibited (type 3 code 13) message
- Unreachable
 - Discard packet forwarded by this route. Notify sender with ICMP host unreachable (type 3 code 1) message

Routing

The screenshot shows the Mikrotik WinBox interface. The main window displays the 'Route List' for the selected router. A modal window titled 'Route <103.2.28.0/24>' is open, showing the configuration for a static route. The configuration is as follows:

Field	Value
Dst. Address	103.2.28.0/24
Gateway	
Check Gateway	ping
Type	blackhole
Distance	1
Scope	30
Target Scope	10
Routing Mark	
Pref. Source	

At the bottom of the modal window, the route status is shown as: enabled, active, static, blackhole.

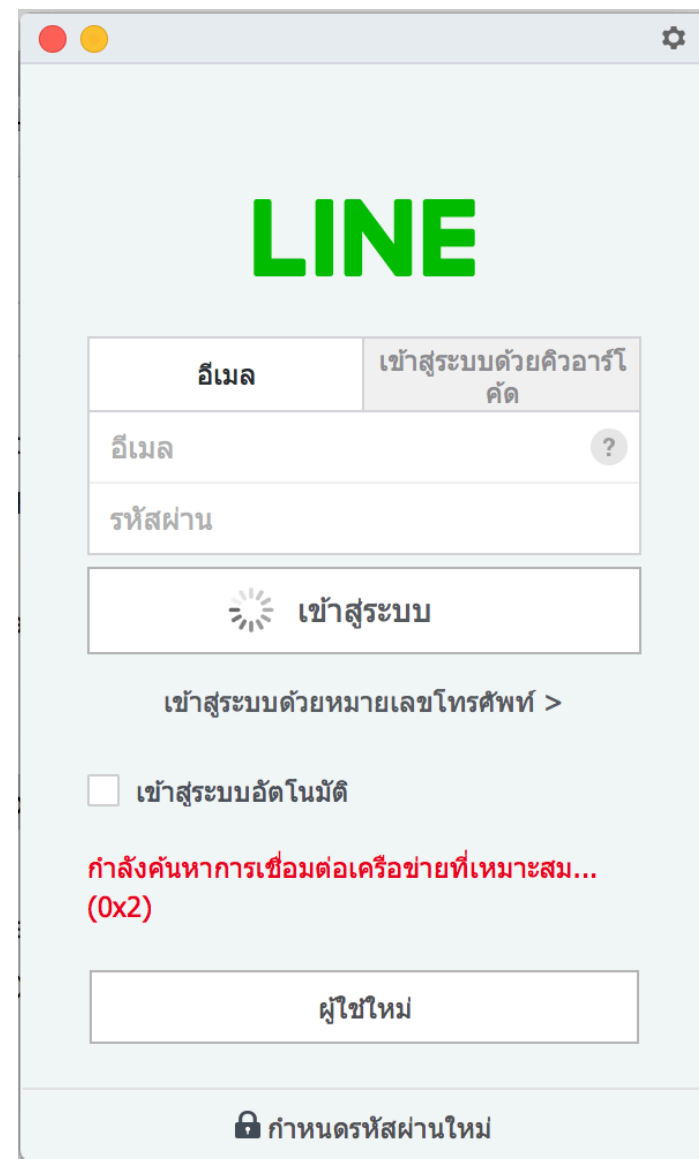
The background 'Route List' table shows the following entries:

Router	Dst. Address
DAS	0.0.0.0/0
ASB	103.2.28.0/24
ASB	103.2.30.0/23
ASB	119.235.224.0/24
ASB	119.235.232.0/24
ASB	119.235.235.0/24
ASB	119.235.236.0/23
ASB	125.6.150.0/24
DAC	192.168.1.0/24
DAC	192.168.222.0/24
ASB	203.104.128.0/20
ASB	203.104.144.0/21
ASB	203.104.152.0/22
ASB	203.104.156.0/23
ASB	203.104.158.0/24
ASB	203.104.160.0/23
ASB	203.104.160.0/24
ASB	203.104.161.0/24
ASB	203.104.163.0/24
ASB	203.104.164.0/23
ASB	203.104.164.0/24
ASB	203.104.165.0/24
ASB	203.104.166.0/23
ASB	203.104.166.0/24
ASB	203.104.167.0/24
ASB	203.104.168.0/23
ASB	203.104.168.0/24
ASB	203.104.169.0/24
ASB	203.104.170.0/23

ตัวอย่างการตั้งค่าใน /ip route

Routing

```
mai — ping 203.104.144.1 — 80x24
Last login: Mon Aug 13 11:57:44 on console
Mais-MacBook-Pro:~ mai$ ping 203.104.144.1
PING 203.104.144.1 (203.104.144.1): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
Request timeout for icmp_seq 12
```



ตัวอย่างทดลองใช้งานLINE

Web Proxy

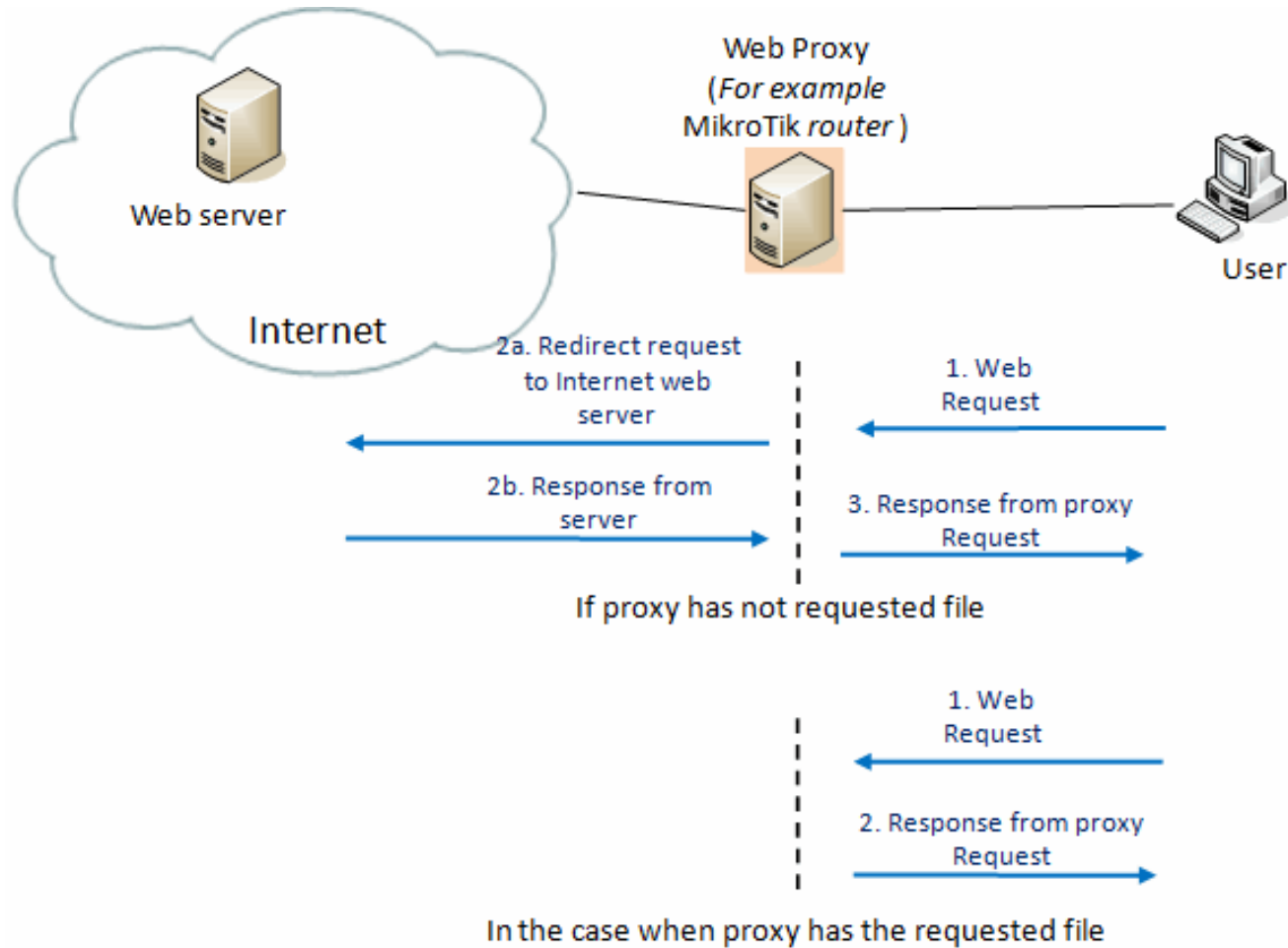
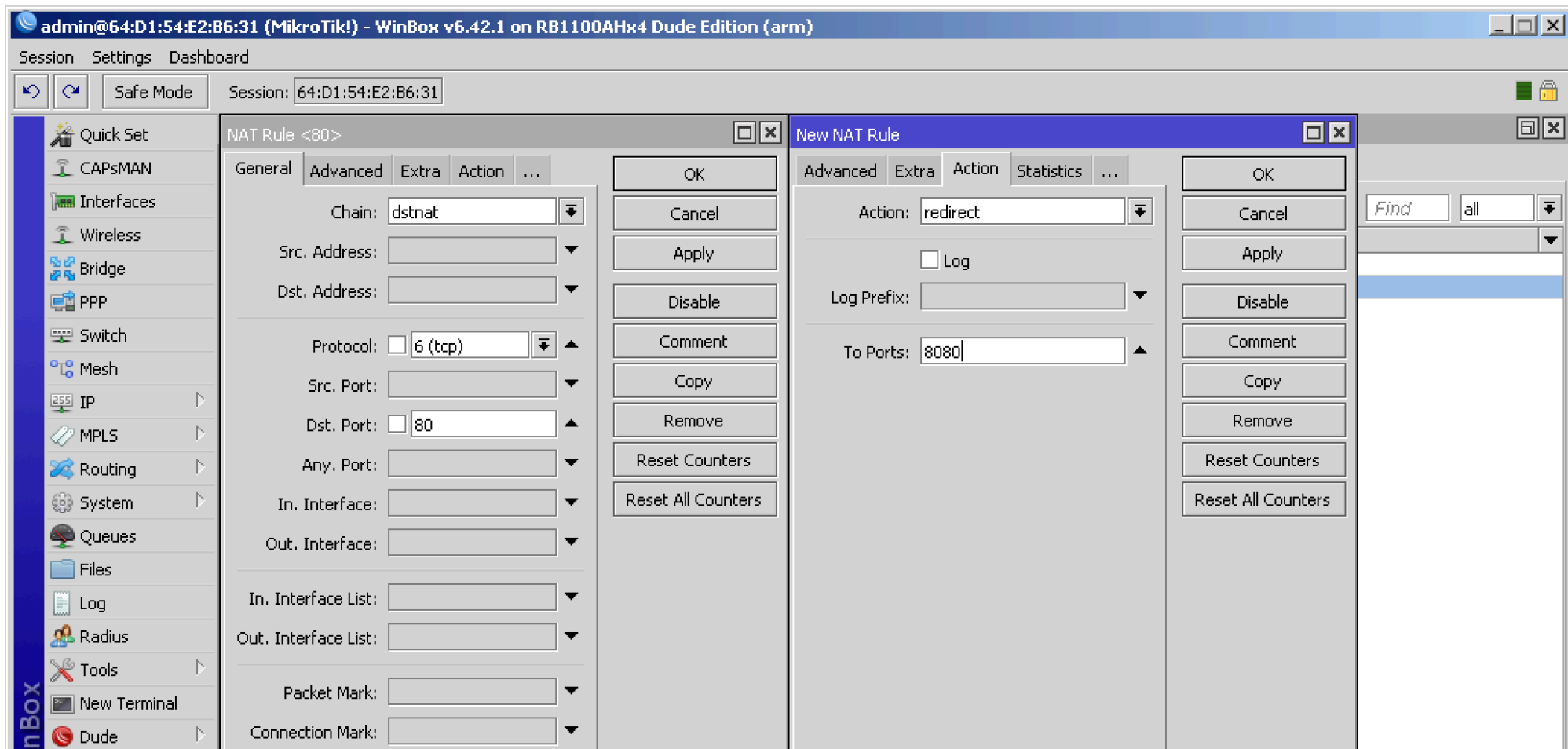


Figure 10.1. Web proxy basic operation scheme

Web Proxy

- สามารถเก็บ Cache และจำกัดการเข้าถึง HTTP ได้
- ไม่สามารถใช้งานกับ HTTPS ได้
- ต้อง Redirect HTTP จาก Router มาด้วย
- สามารถป้องกันการเข้าถึงและ Redirect ไปยังเว็บไซต์ใหม่ที่ต้องการได้
- สามารถเรียกไปยัง Web Proxy ตัวอื่นๆได้เพื่อใช้งาน Cache ในกรณีที่ขนาด HDD ไม่พอจัดเก็บข้อมูล

Web Proxy



ตัวอย่างการตั้งค่าใน /ip firewall nat

Web Proxy

The screenshot displays the WinBox interface for configuring a Web Proxy. The main window is titled "admin@64:D1:54:E2:B6:31 (MikroTik!) - WinBox v6.42.1 on RB1100AHx4 Dude Edition (arm)". The interface is divided into several sections:

- Web Proxy Settings (General):**
 - Enabled:
 - Src. Address: ::
 - Port: 8080
 - Anonymous:
 - Parent Proxy: (empty)
 - Parent Proxy Port: (empty)
 - Cache Administrator: webmaster
 - Max. Cache Size: unlimited KIB
 - Max Cache Object Size: 204800000 KIB
 - Cache On Disk:
 - Max. Client Connections: 6000
 - Max. Server Connections: 6000
 - Max Fresh Time: 3d 00:00:00
 - Serialize Connections:
 - Always From Cache:
 - Cache Hit DSCP (TOS): 4
 - Cache Path: disk1/webpro
- Web Proxy Access:**
 - Buttons: +, -, ✓, ✗, 📁, 🗑️, 📊, 📄
 - Counters: 00 Reset Counters, 00 Reset All Counters
 - Table:

#	Src. Address	Dst. Host	Action	Redirect To	Hits
0		*.otiknetwork.com	deny	www.vrproservice.com	2
- Web Proxy Rule <>:**
 - Src. Address: (empty)
 - Dst. Address: (empty)
 - Dst. Port: (empty)
 - Local Port: (empty)
 - Dst. Host: *.otiknetwork.com
 - Path: (empty)
 - Method: (empty)
 - Action: deny
 - Redirect To: www.vrproservice.com
 - Hits: 2
 - Status: enabled

ตัวอย่างการตั้งค่าใน /ip proxy

Web Proxy

The screenshot shows the VRproService website interface. At the top, there are navigation links for 'vrproservice' and 'vrchannel', along with 'ระบบจัดการCloud', 'ตัวอย่างผลงานเรา', and 'ติดต่อเรา'. The main header features the VRPRO SERVICE logo and contact information: 'ติดต่อวางระบบโทร 096-659-1415 | 096-659-1951'. A blue navigation bar contains links for 'หน้าแรก', 'ตารางอบรม', 'DOWNLOAD', 'ROUTEROS', and 'UNIFI', along with a search bar and a 'ค้นหา' button. A sidebar menu titled 'บริการของเรา' lists various services such as 'ติดตั้งระบบ Internet Hotspot', 'ติดตั้งระบบ WiFi ความเร็วสูง', 'ติดตั้งระบบ Network ภายในองค์กร', 'จัดเก็บ Log file ตามพรบ.คอมฯ', 'ติดตั้งระบบ Load balance', 'ติดตั้งระบบ Firewall, DMZ', 'ติดตั้งระบบ VPN Server เชื่อมสาขา', 'ติดตั้งระบบ Network Monitoring', 'ศูนย์อบรม MikroTik Training Center', and 'ระบบจัดการผู้ใช้งาน Internet'. The main content area features a large banner for 'MIKROTIK USER MEETING THAILAND 2018' in Bangkok, August 14, at the Asia Airport Hotel. Below the banner are four service categories: 'WiFi ความเร็วสูง รับวางระบบ WiFi', 'Internet Apartment รับติดตั้งเน็ตหอพัก', 'MikroTik Training ศูนย์อบรมไมโครติค', and 'Log Management ระบบจัดเก็บการใช้งาน'.

ตัวอย่างทดลองเข้าเว็บไซต์

ข้อมูลเพิ่มเติม

- Presentation & Script
 - <http://www.vrproservice.com/mumthailand2018.zip>
- ช่องทางการติดต่อ
 - <http://www.vrproservice.com>
 - <http://fb.me/vrproservices>
 - Line: @vrproservice

THANK YOU

Don't forget "GOOD FIREWALL"

https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router