VRPRO SERVICE

จัดการ Content ให้อยู่หมัดด้วย RouterOS!

Presented by Mana Kaewcharoen

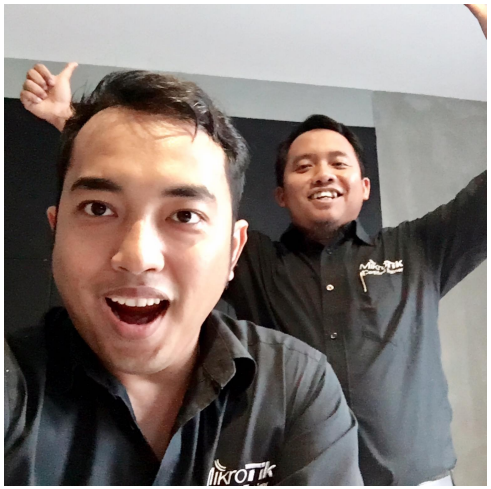
MUM Thailand 2018

ประวัติวิทยากร

Mana Kaewcharoen

MTCNA | MTCWE | MTCUME | MTCTCE

MTCRE | MTCINE | MTCIPv6E



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

ทำไมต้องจัดการ Content!

- Content หรือ “เนื้อหา” ในที่นี้หมายถึง เว็บไซต์ , วิดีโอ , ไฟล์ต่างๆ , อีเมล์ หรือข้อมูลต่างๆที่อยู่บนอินเทอร์เน็ต
- การจำกัดการเข้าถึง “เนื้อหา” ต่างๆอาจมีเหตุผลหลายประการเช่น
  - กฎระเบียบหรือข้อบังคับของหน่วยงาน
  - การควบคุมโดยผู้ปกครอง
  - คัดกรองจากหน่วยงานรัฐ
  - ประเด็นเรื่องกฎหมาย
  - ด้านความปลอดภัย
  - อื่นๆ

ตัวอย่าง: การจัดการเนื้อหา

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

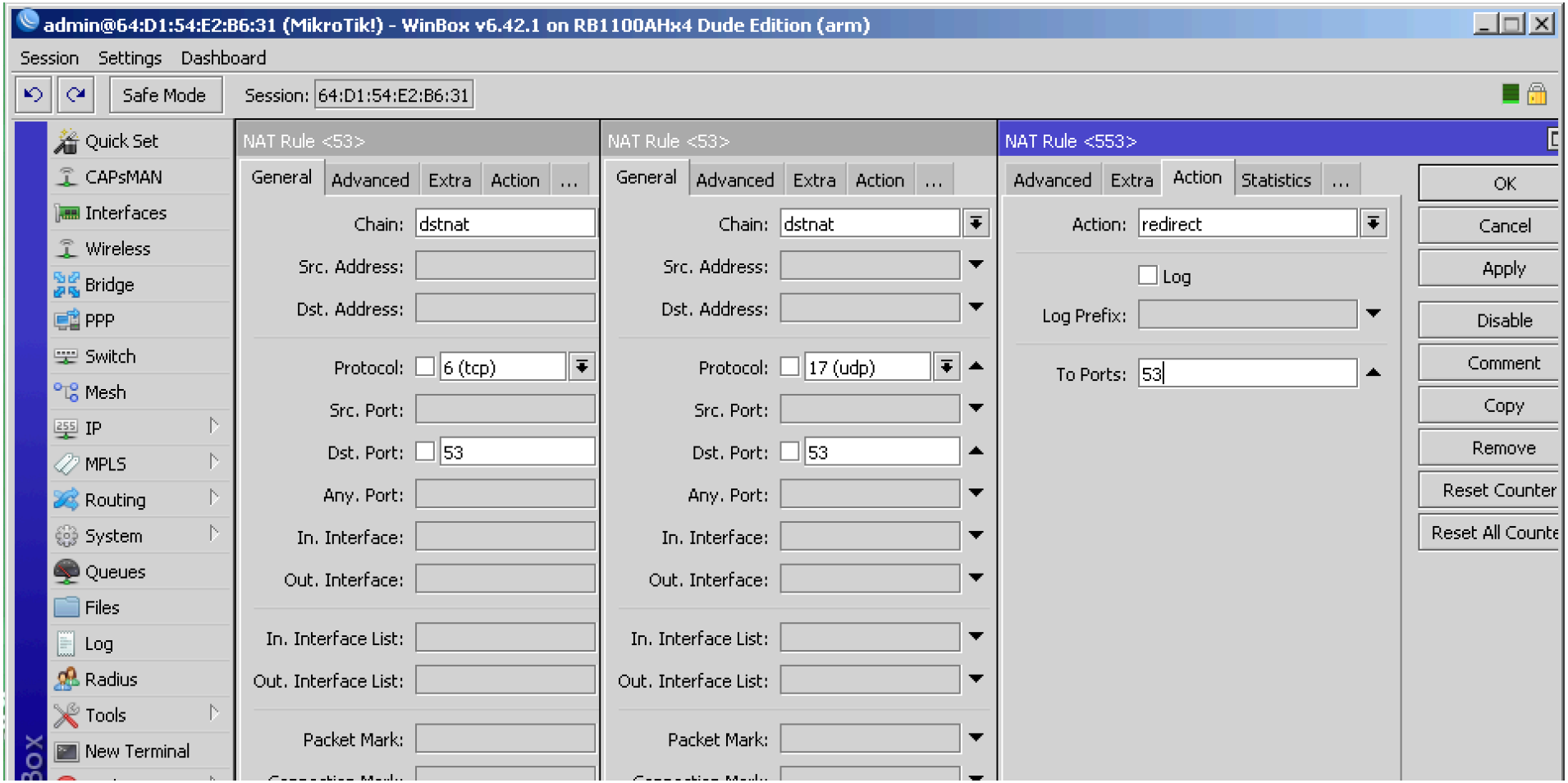
เนื้อหา	เครื่องมือจัดการ
HTTP	DNS, Protocol+Port, Content, Web Proxy
HTTPS	DNS, Procol+Port, TLS Host
Video, File	Layer 7 Protocols
Torrents	Layer 7 Protocols
Facebook	DNS, IP, Layer 7 Protocols, Routing
YouTube	DNS, TLS Host, Layer 7 Protocols
Line	IP, Routing, Layer 7 Protocols

DNS (Static DNS)

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

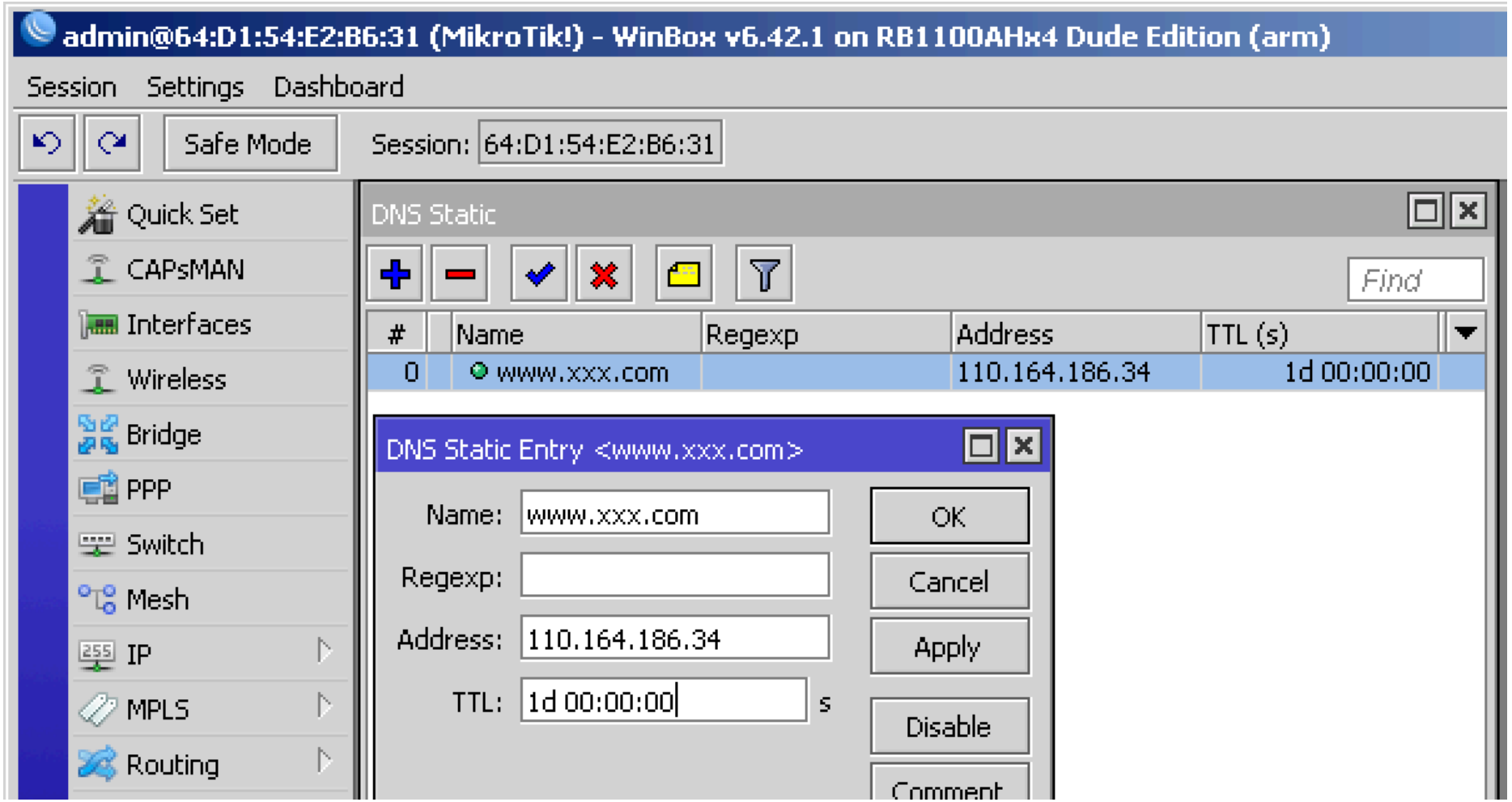
```
/ip firewall nat add action=redirect chain=dstnat dst-port=53 protocol=udp to-ports=53

/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)



ตัวอย่างการตั้งค่าใน /ip dns static

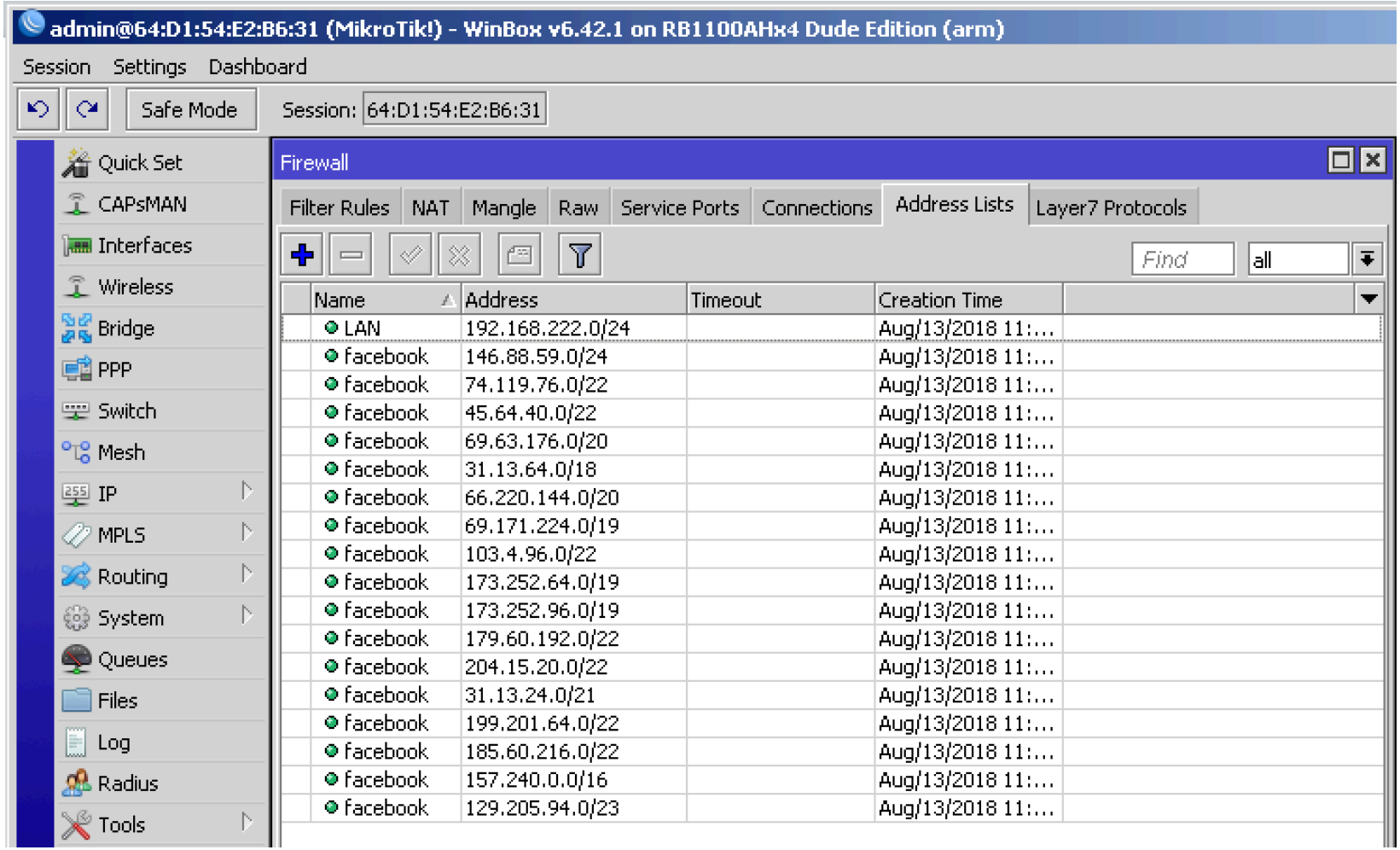
DNS (Static DNS)

ตัวอย่างทดลองเข้าเว็บไซต์

IP, Protocol, Port, Address lists

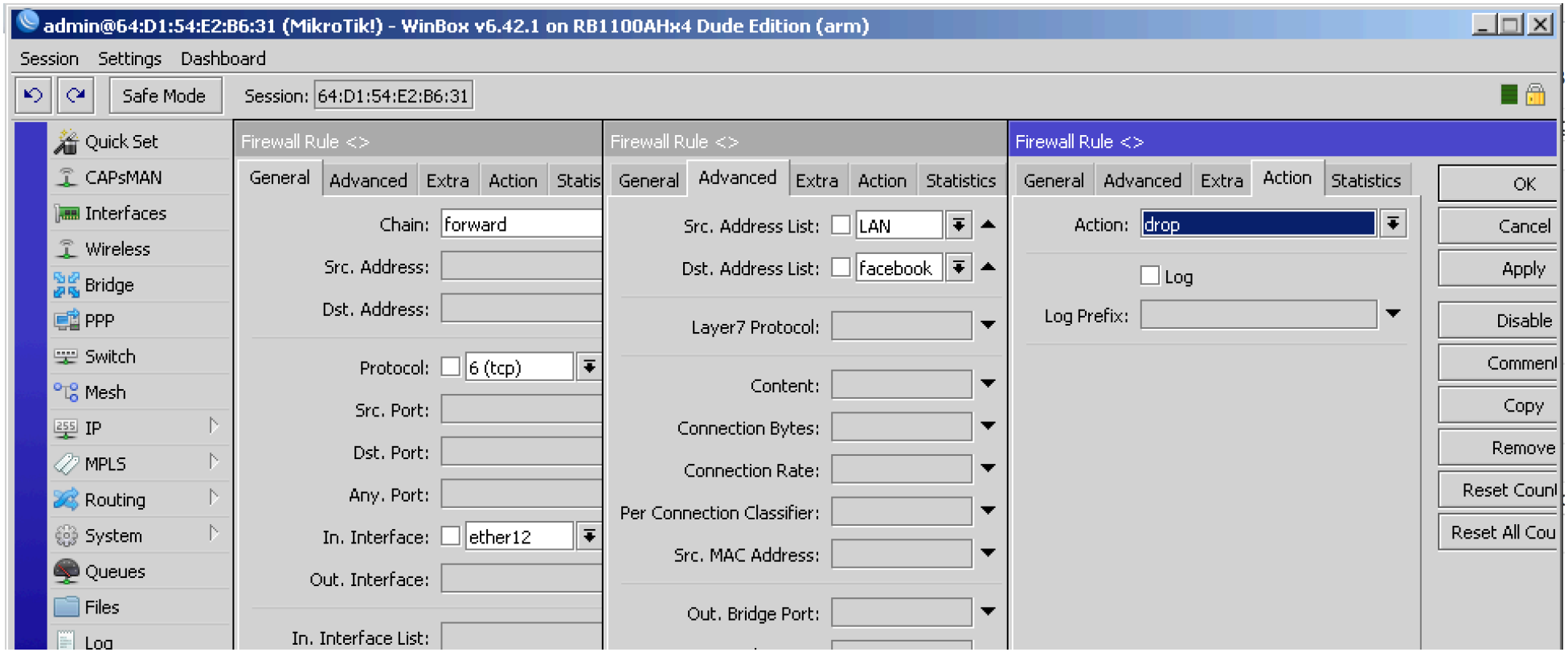
- RouterOS มีฟีเจอร์มาตรฐานที่ติดมาด้วยคือ Firewall อยู่ในเมนู /ip firewall สามารถระบุได้ทั้ง IP , Protocol , Port
- นอกจากนี้เรายังสามารถสร้าง Address List ไว้ใช้งานแบบกลุ่มหรือชุด IP Address ได้ทั้งแบบ Dynamic และ Static
- Address List สามารถใส่ Domain แทนการใส่ IP Address ได้ ระบบจะไปทำการดึง IP Address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

IP, Protocol, Port, Address lists



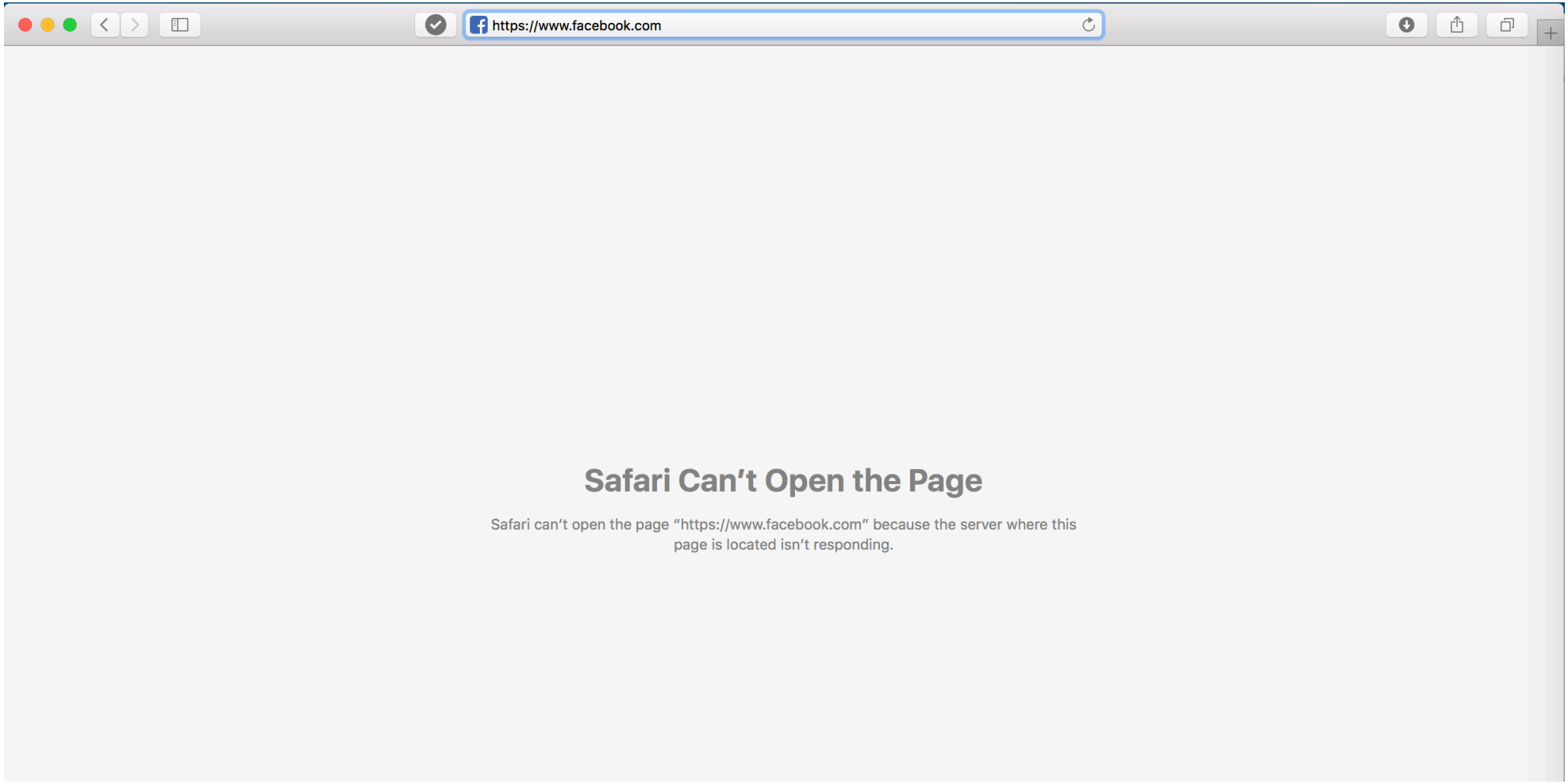
ตัวอย่างการตั้งค่าใน /ip firewall address-list

IP, Protocol, Port, Address lists



ตัวอย่างการตั้งค่าใน /ip firewall filter

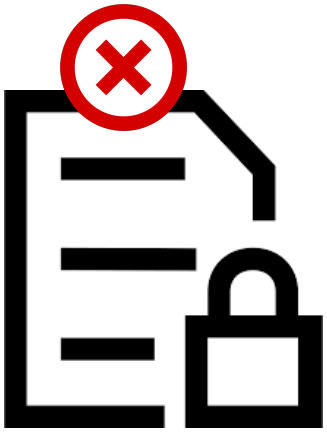
IP, Protocol, Port, Address lists



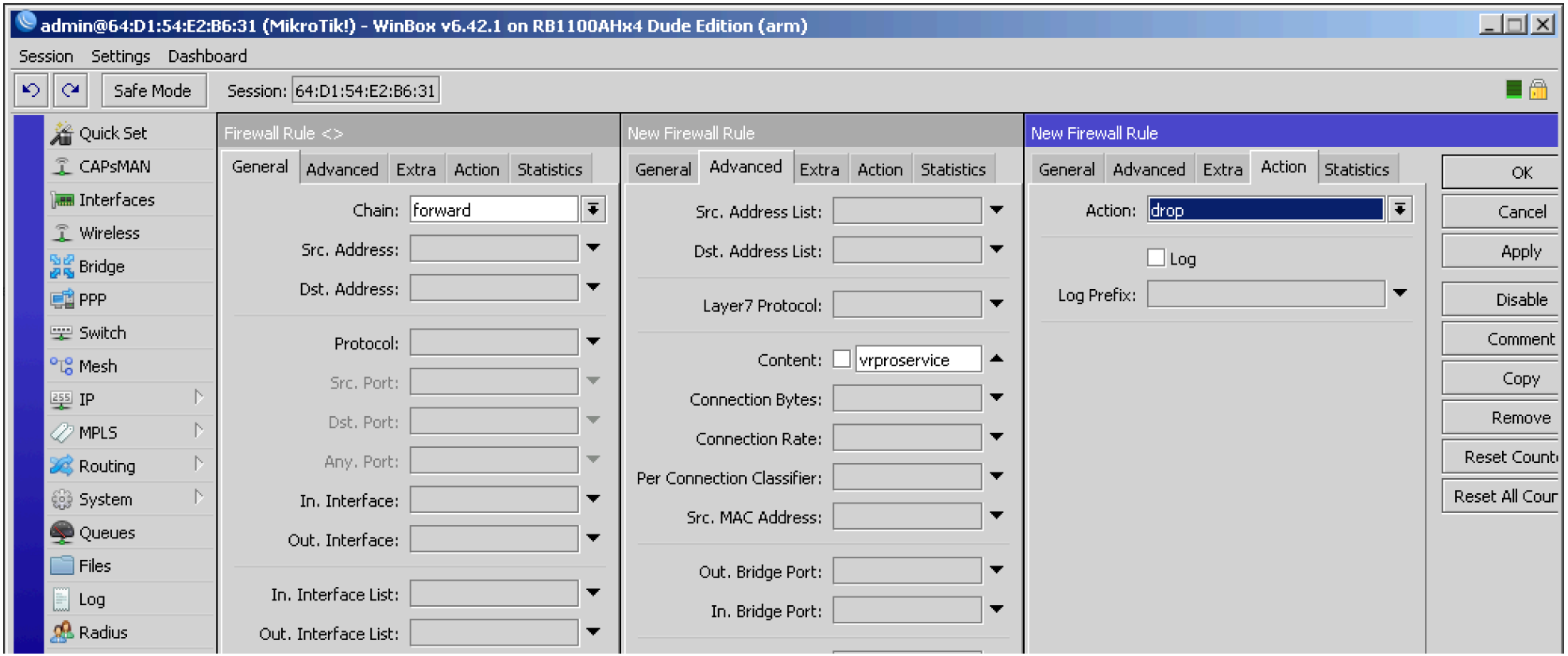
ตัวอย่างทดลองเข้าเว็บไซต์

Content

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

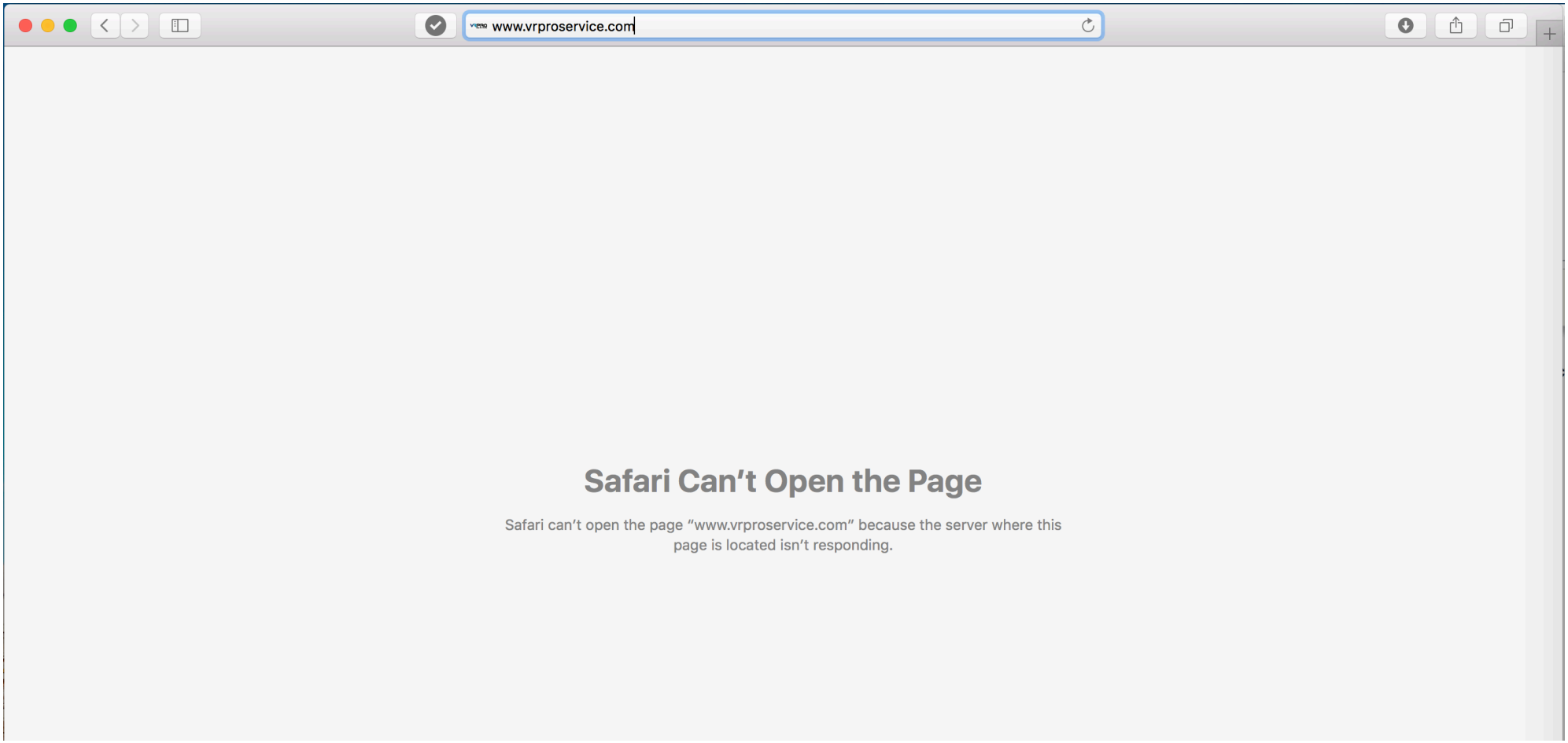


Content



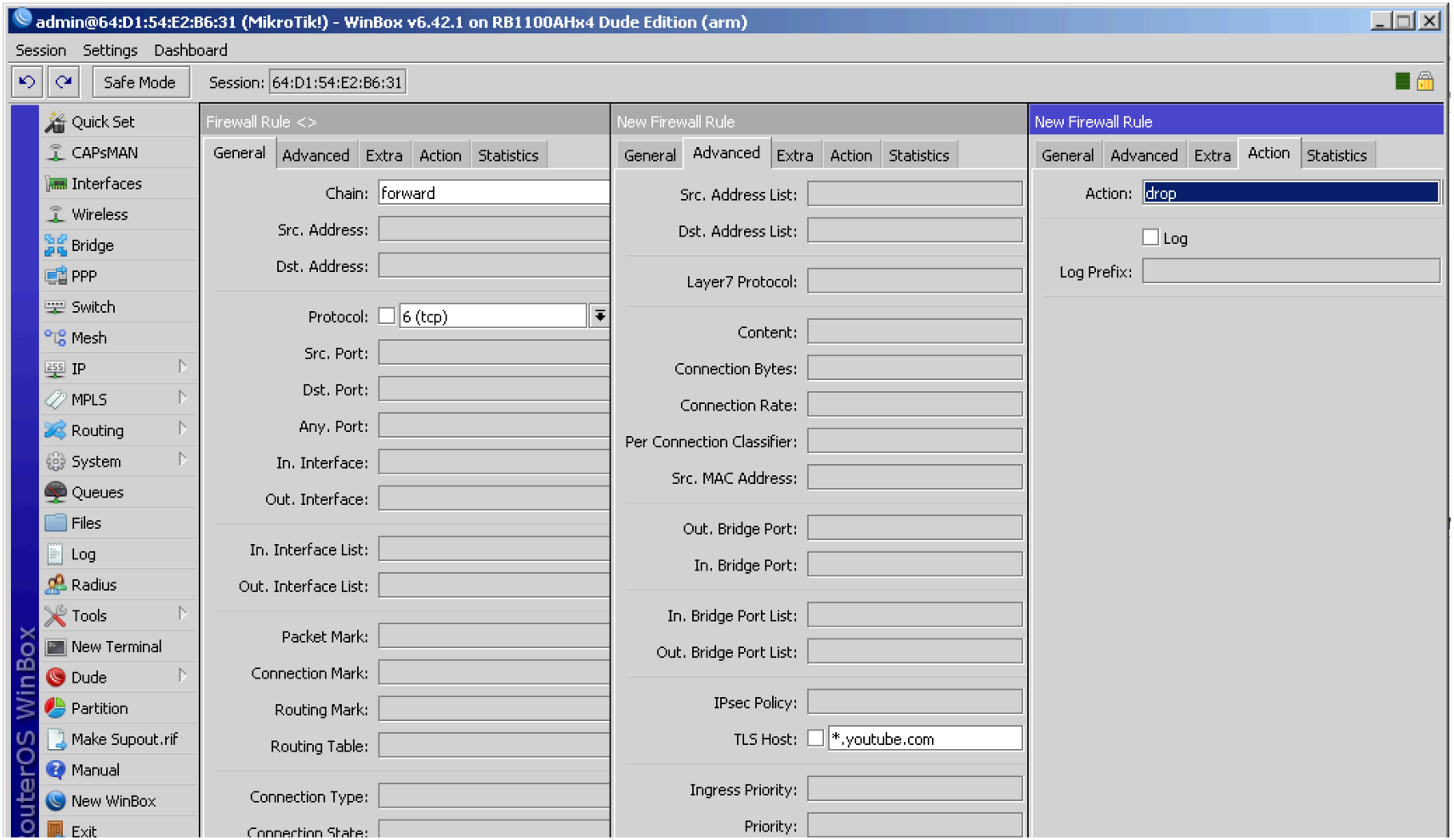
ตัวอย่างการตั้งค่าใน /ip firewall filter

Content



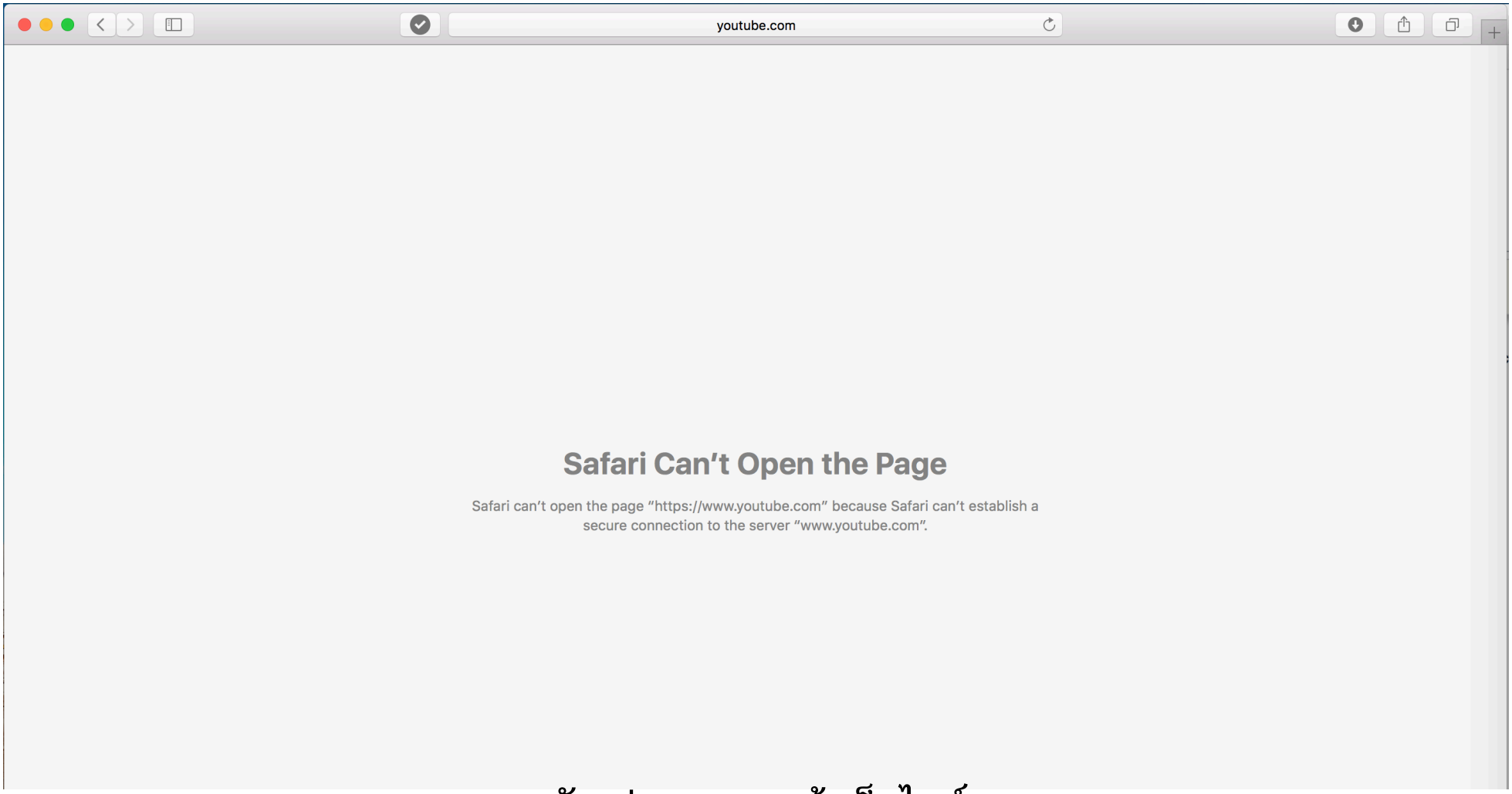
ตัวอย่างทดลองเข้าเว็บไซต์

TLS Host



ตัวอย่างการตั้งค่าใน /ip firewall filter

TLS Host



ตัวอย่างทดลองเข้าเว็บไซต์

Layer 7 Protocols

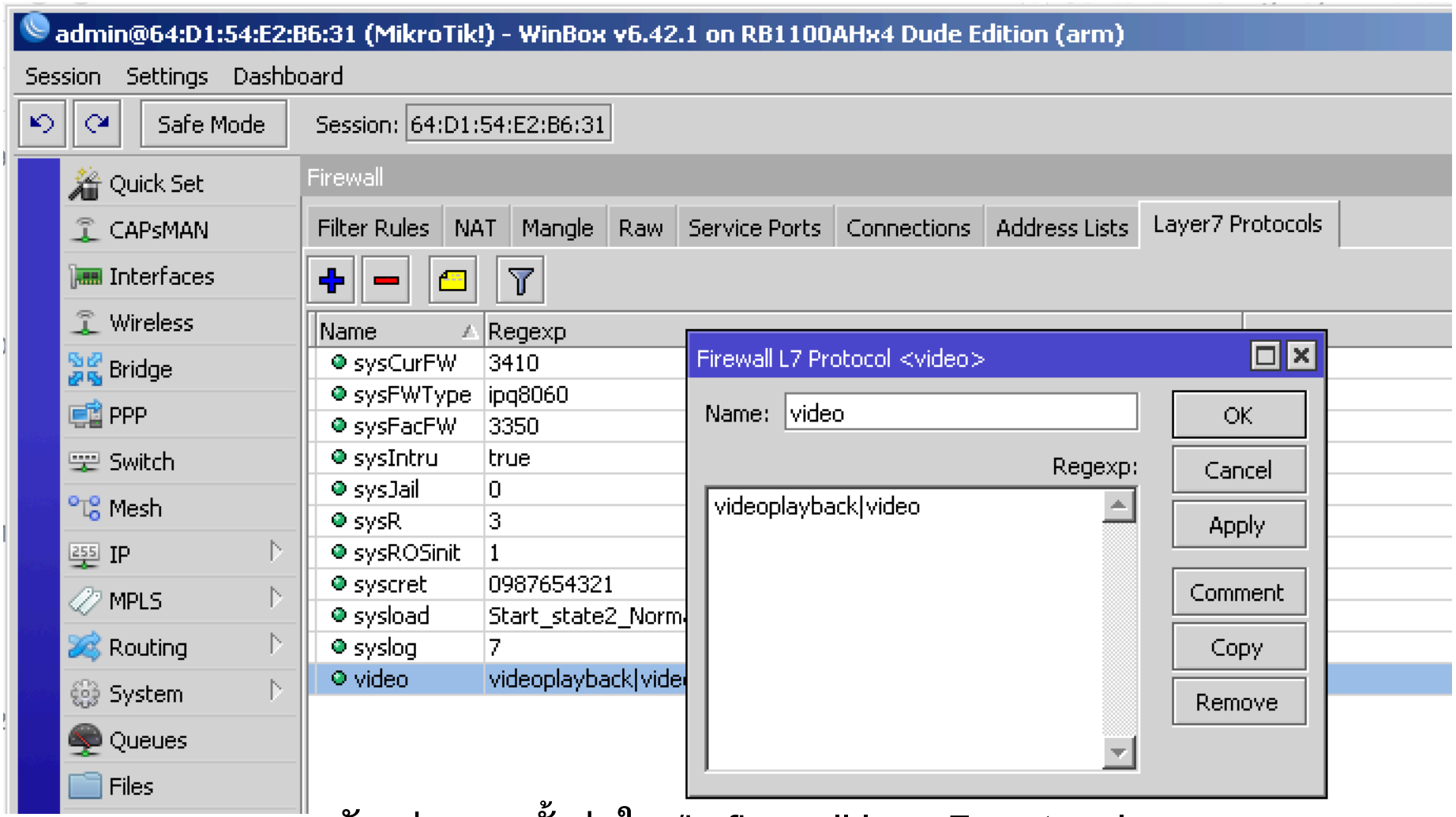
- Layer 7 Protocols จะค้นหาข้อมูลในรูปแบบ ICMP/TCP/UDP streams
- Layer 7 Protocols จะทำการค้นหา 10 Packets แรกของ Connection หรือ 2KB แรกของ Connection ที่ตรงกับ Pattern ของข้อมูลที่มี
- หากไม่พบข้อมูลที่ตรงกัน Layer 7 Protocols จะถือว่าไม่เข้ากฎหรือไม่ตรงตาม Pattern ที่มี
- ข้อควรระวังในการใช้งาน Layer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

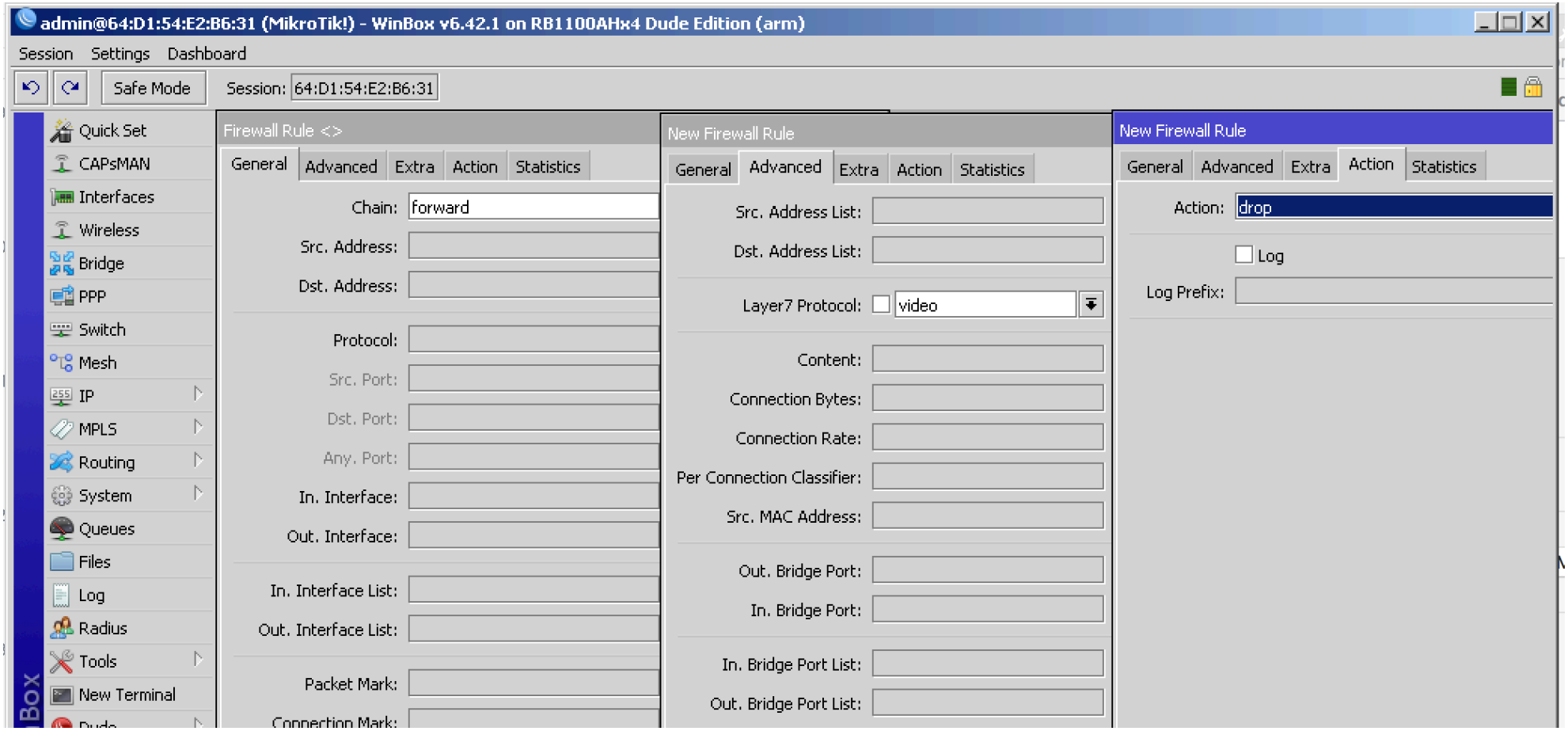
options: i case insensitive m make dot match newlines x ignore whitespace in regex o perform #{...} substitutions only once

Layer 7 Protocols



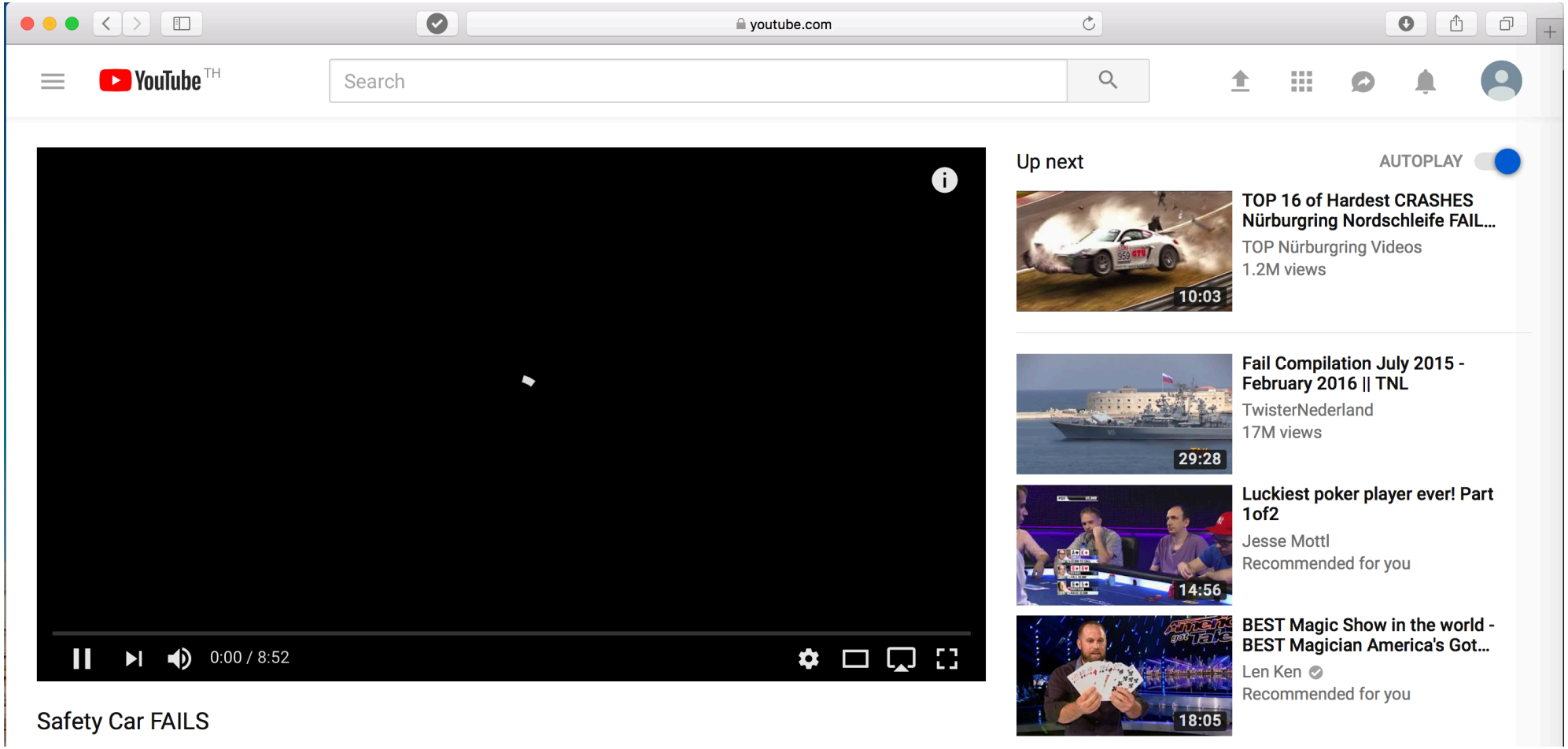
ตัวอย่างการตั้งค่าใน /ip firewall layer7-protocol

Layer 7 Protocols



ตัวอย่างการตั้งค่าใน /ip firewall filter

Layer 7 Protocols



ตัวอย่างทดลองเข้าเว็บไซต์

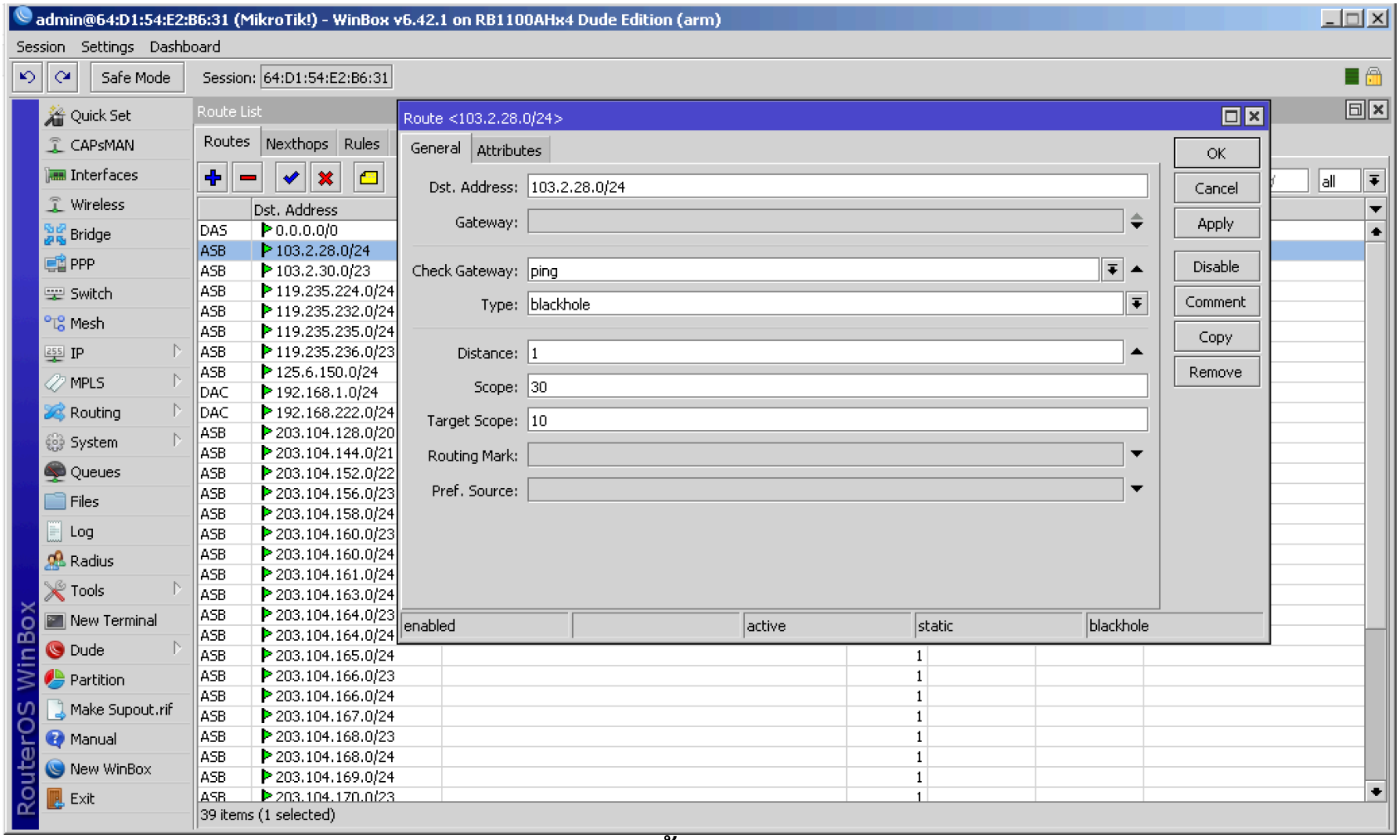
Routing

- ทำงานบน OSI Layer 3
- ไม่รองรับโดเมนเนม
- สามารถใช้งานร่วมกับ Routing Mark ได้
- ใช้ได้กับ IP เท่านั้น (ยกเว้นใช้งานร่วมกับ Routing Mark จึงสามารถใช้ร่วมกับอื่นๆได้เช่น Protocol, Port, Layer 7)

Routing Type

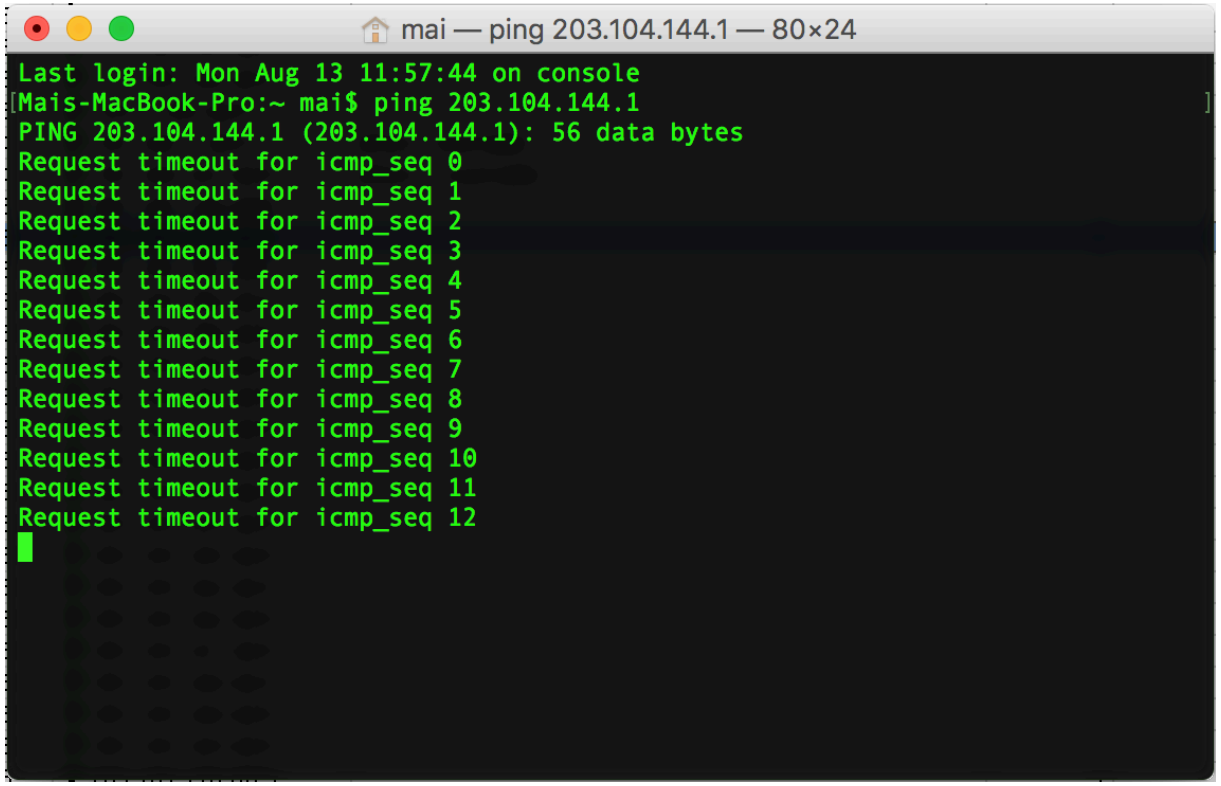
- Blackhole
  - Silently discard packet forwarded by this route
- Prohibit
  - Discard packet forwarded by this route. Notify sender with ICMP communication administratively prohibited (type 3 code 13) message
- Unreachable
  - Discard packet forwarded by this route. Notify sender with ICMP host unreachable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

Routing



ตัวอย่างการตั้งค่าใน /ip route

Routing



ตัวอย่างทดลองเข้าใช้งานLINE

Web Proxy

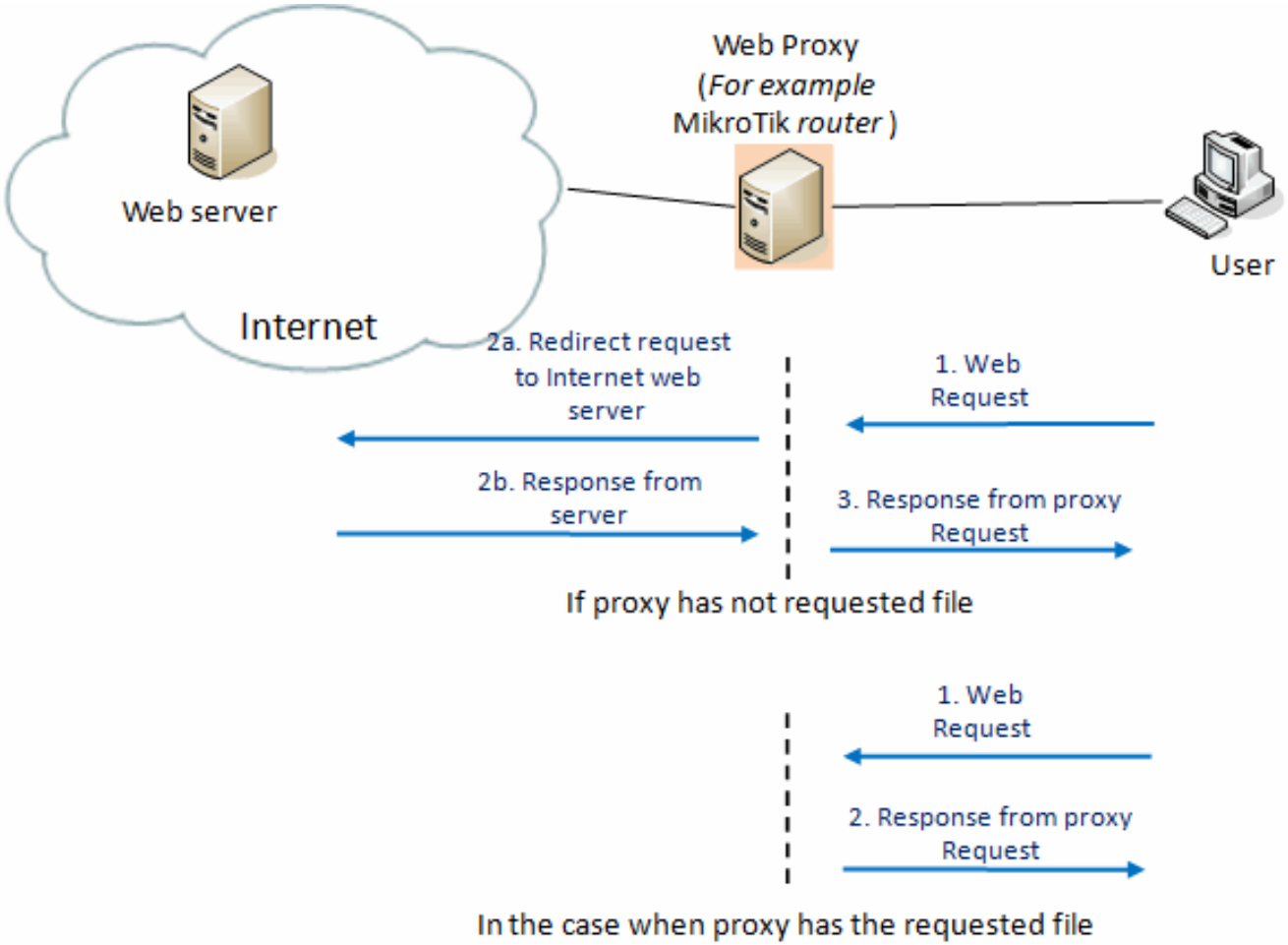
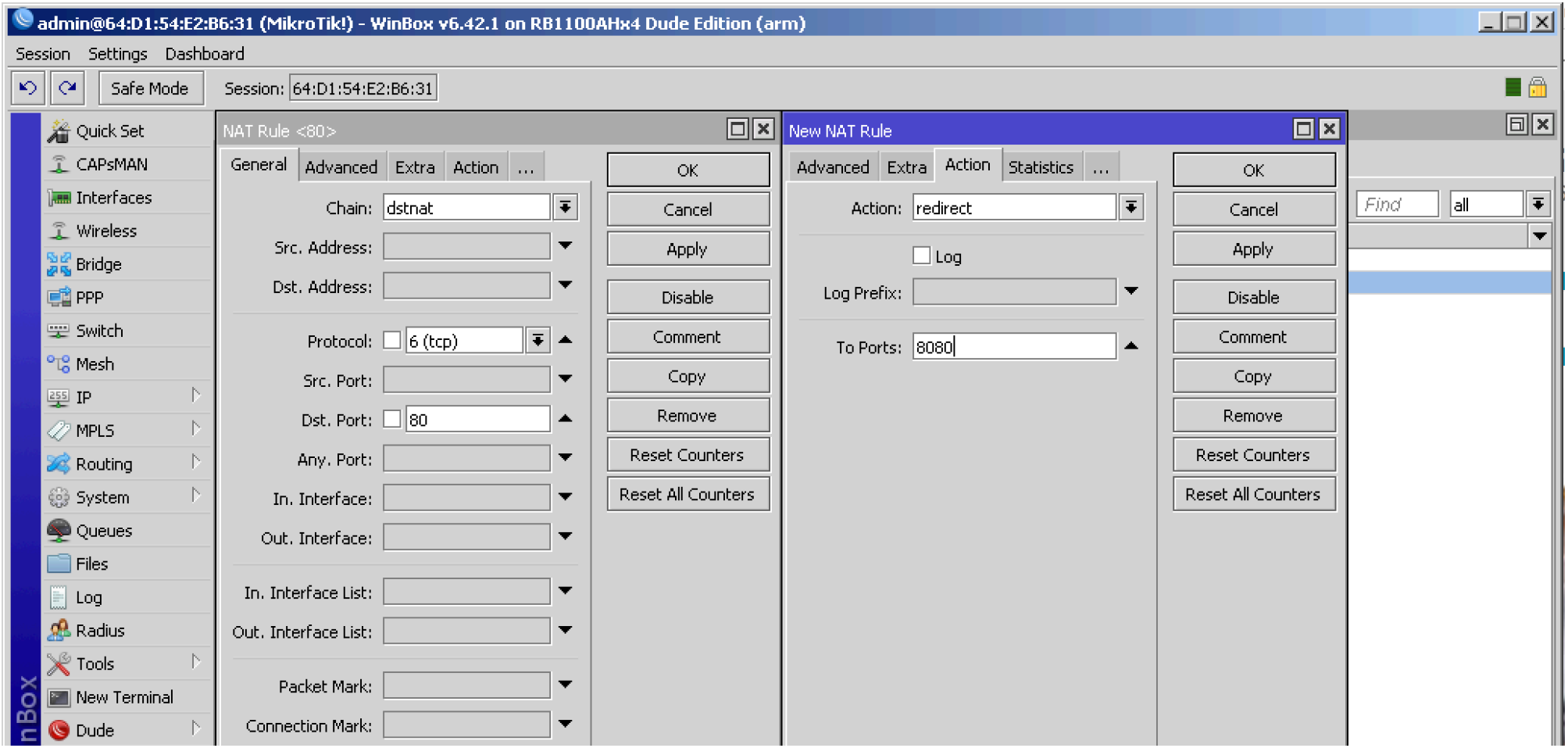


Figure 10.1. Web proxy basic operation scheme

Web Proxy

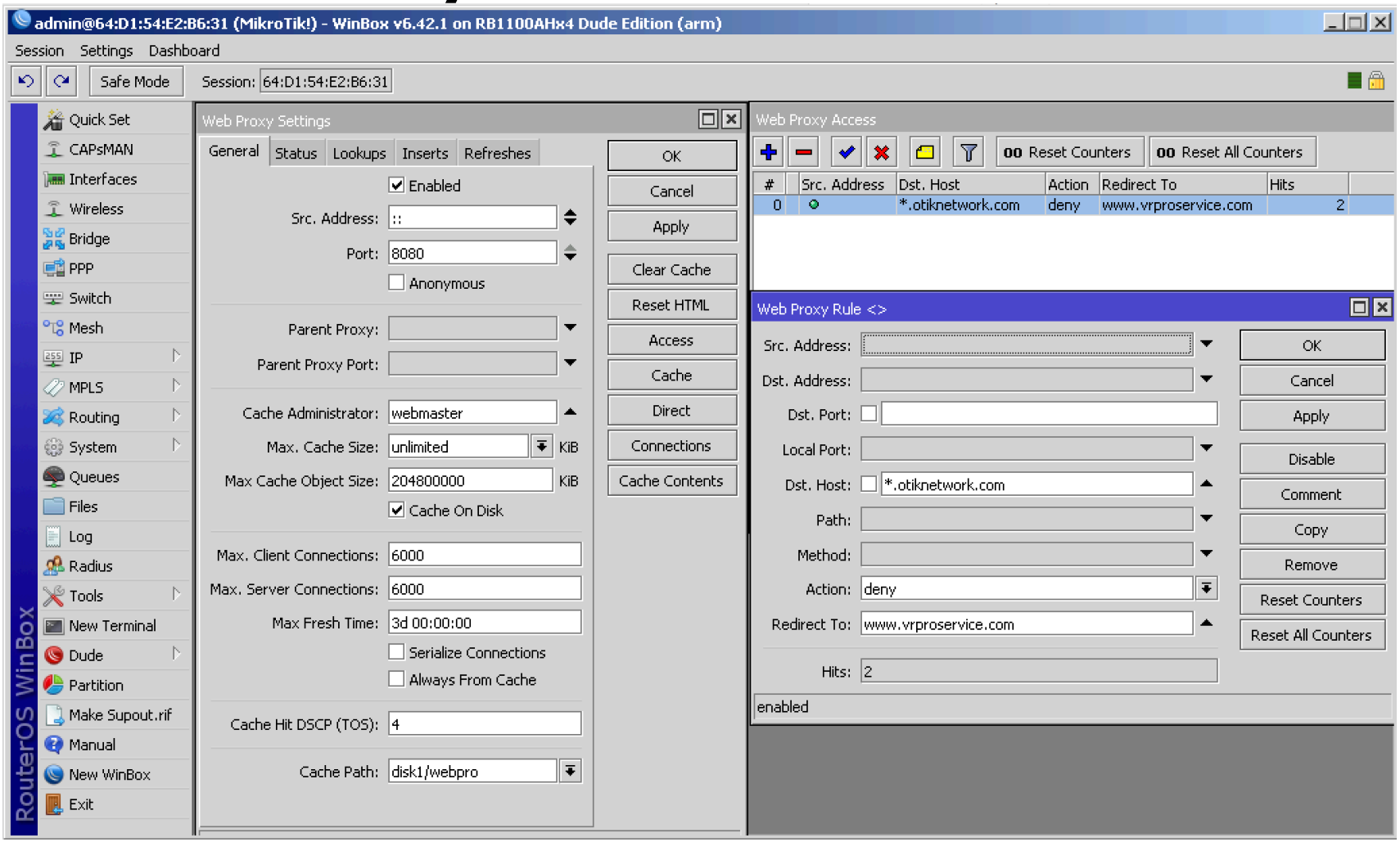
- สามารถเก็บ Cache และจำกัดการเข้าถึง HTTP ได้
- ไม่สามารถใช้งานกับ HTTPS ได้
- ต้อง Redirect HTTP จาก Router มาด้วย
- สามารถป้องกันการเข้าถึงและ Redirect ไปยังเว็บไซต์ใหม่ที่ต้องการได้
- สามารถเรียกไปยัง Web Proxy ตัวอื่นๆได้เพื่อใช้งาน Cache ในกรณีที่ขนาด HDD ไม่พอจัดเก็บข้อมูล

Web Proxy



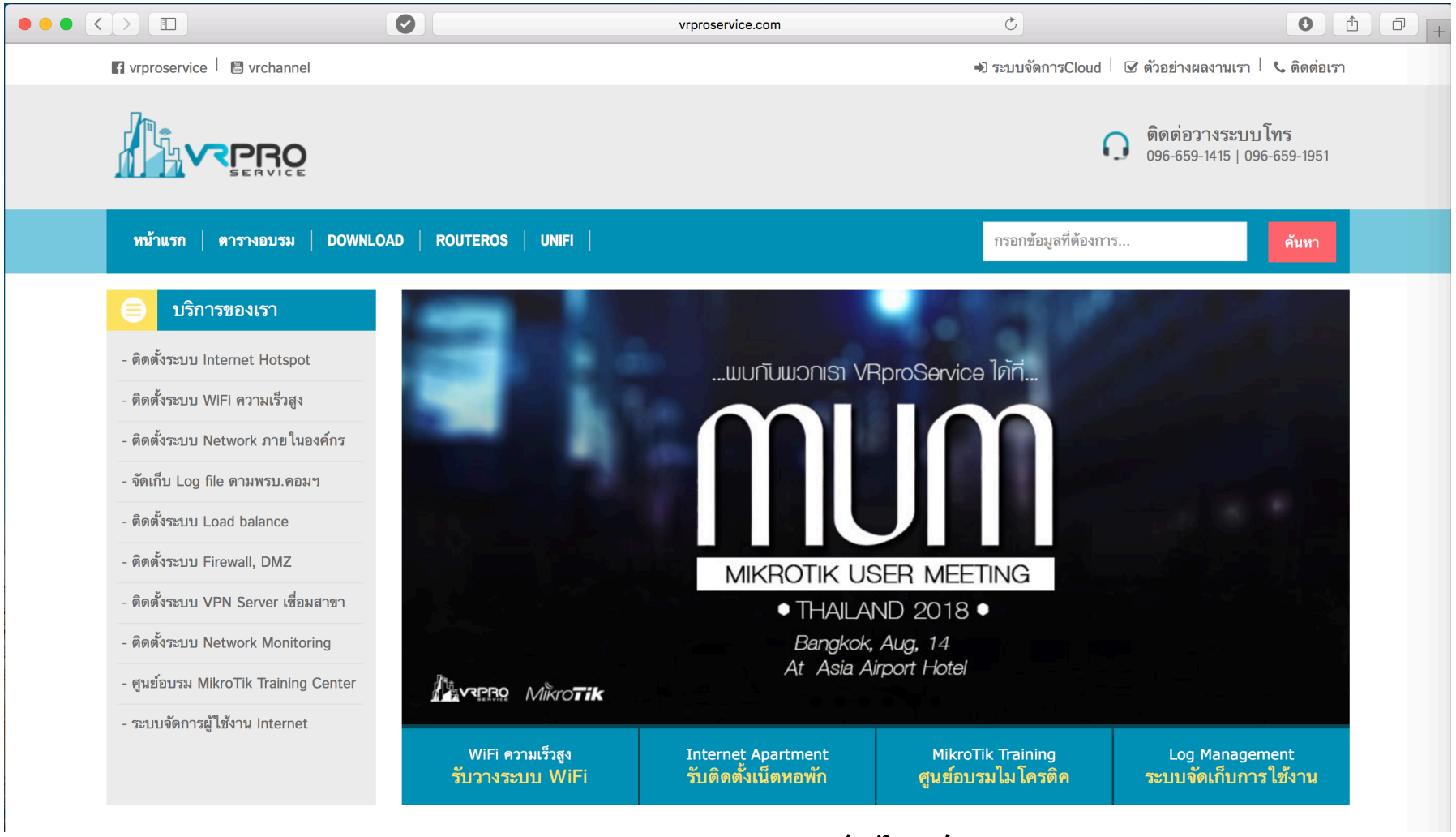
ตัวอย่างการตั้งค่าใน /ip firewall nat

Web Proxy



ตัวอย่างการตั้งค่าใน /ip proxy

Web Proxy



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