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 \bigcirc

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

🔏 Quick Set				
CAPsMAN				
Interfaces				
🚊 Wireless				
📲 🖁 Bridge				
📑 PPP				
°t <mark>8</mark> Mesh	400			
፼ IP ♪	ARP	DNS Settings		
🛒 IPv6 🗈	Accounting	Servers:	\$.8.8.8	ОК
🖉 MPLS 🗈 🗈	Addresses		2001:4860:4860::8888	Cancel
🐹 Routing	DHCP Client	Durania Carran	•	
∰ System ►	DHCP Relay	Dynamic Servers:		Арріу
Queues	DHCP Server		Allow Remote Requests	Static
Files	DNS	Max UDP Packet Size:	4096	Cache
E Log	Firewall			
A Radius	Hotspot	Query Server Timeout:	2.000 s	
Tools	IPsec	Query Total Timeout:	10.000 s	
New Terminal	Neighbors	Max, Concurrent Queries:	100	
S Dude	Packing	Max. Concurrent Queries.		
Make Supout rif	Pool	Max. Concurrent TCP Sessions:	20	
Manual	Routes	Cache Size:	2048 KiB	
New WinBox	SMB	Cache Max TTL:	7d 00:00:00	
Exit	SNMP	Cache Llead	16 K/P	
	Services	Cacrie Used:		

DNS Static			
+ - 🖌 🗶 🗂	T	Find	1
# Name	Regexp	Address	-
0 0	.*facebook.com	m 127.0.0.1	
I example.com		127.0.0.1	
DNS Static Entry <example.< td=""><td>com></td><td></td><td></td></example.<>	com>		
Name: example.com		ОК	
Regexp:		Cancel	
Address: 127.0.0.1		Apply	
TTL: 1d 00:00:00	s	Disable	
		Comment	
		Сору	•
		Remove	
enabled			

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

if you use name with <u>example.com</u>, then <u>www.example.com</u> won't work

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

NAT Rule <53>		NAT Rule <53>		NAT Rule <53>	
General Advanced Extra Action	ОК	General Advanced Extra Action	ОК	Advanced Extra Action Statistics	ОК
Chain: dstnat	Cancel	Chain: dstnat	Cancel	Action: redirect	Cancel
Src. Address:	Apply	Src. Address:	Apply	Log	Apply
Dst. Address:	Disable	Dst. Address:	Disable	Log Prefix:	Disable
Protocol: 🗌 6 (tcp) ∓ 🔺	Comment	Protocol: 🗌 17 (udp) ∓ 🔺	Comment	To Ports: 53	Comment
Src. Port:	Сору	Src. Port:	Сору		Сору
Dst. Port: 53	Remove	Dst. Port: 53	Remove		Remove
Any. Port:	Reset Counters	Any. Port:	Reset Counters		Reset Counters
In. Interface:	Reset All Counters	In. Interface:	Reset All Counters		Reset All Counters
Out. Interface:		Out. Interface:			
In. Interface List:		In. Interface List:			
Out. Interface List:		Out. Interface List:			
Packet Made		Packet Made			
Routing Mark:		Routing Mark:			
Routing Table:		Routing Table:			
Connection Type:		Connection Type:			

Setup new rule with same action, port and chain, but has diffrent 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
C:4.
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
Ping statistics for 127.0.0.1:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = Oms, Maximum = Oms, Average = Oms
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

	🎢 Quick Set			
	CAPsMAN			
	Interfaces			
	🚊 Wireless			
	📲 🚰 Bridge		Web Proxy Settings	
	📑 PPP		General Status Lookups Inserts Refreshes	OK
	🕎 Switch	400		Creat
	°t¦8 Mesh	ARP		Cancel
	255 IP 🗅	Accounting	Src. Address:	Apply
	👳 IPv6 🛛 🗅	Addresses	Port: 8080 🗢	Clear Cache
	🖉 MPLS 🛛 🗅	Cloud	Anonymous	Devet UTM
	🎉 Routing 🛛 🗅	DHCP Client	Parent Prover	Reset HIML
	💮 System 🗈	DHCP Relay		Access
	Queues	DHCP Server	Parent Proxy Port:	Cache
	Files	DNS	Cache Administrator: michael@takeuchi.id	Direct
	E Log	Firewall	May Casha Sizer and T KB	Connections
	A Radius	Hotspot		Connections
	🗶 Tools 🗈	IPsec	Max Cache Object Size: 2048 KiB	Cache Contents
	New Terminal	Neighbors	Cache On Disk	
	🛄 Make Supout.rif	Packing	Max. Client Connections: 600	
	Manual	Pool	Max. Server Connections: 600	
	New WinBox	Routes	May Freeh Time: 3d 00:00:00	
×	Exit	SNMP	Serialize Connections	
B		Services	Always From Cache	
Vin		Settings		
>		Socks	Cache Hit DSCP (TOS): 4	
Ö		TFTP	Carla Bath, unb annua	
je		Traffic Flow	Cache Path: web-proxy	
put		UPnP		
Ř		Web Proxy	unknown	

2. Web Proxy – Blocking

• Go to Access Menu on The Left

Web Proxy Access								×□
🔶 🖃 🖉 🖉 🕜 Rese	t Counters	00 Reset All Co	unters	Find				
# Src. Address Dst. Address	Dst. Host	Path	Method	Action	Redirect To	Hits	-	
0 • 192.168.3.0/29	80	*.example.com			deny			0
Web Proxy Rule <192.168.3.0/29>								
Src. Address: 192.168.3.0/29		ОК						
Dst. Address:	•	Cance	I					
Dst. Port: 20		Apply						
Local Port:	•	Disable	•					
Dst. Host: *.example.com		Comme	nt					
Path:	-	Сору						
Method:		Remov	e					
Action: deny	•	Reset Cou	nters					
Redirect To:	•	Reset All Co	unters					
Hits: 0								
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.

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	ОК
Dst. Address: 8.8.8.8	Cancel
Gateway: 192.168.137.1	Apply
Check Gateway:	Disable
Type: blackhole	Comment
Distance: blackhole unicast	Copy
Scope: Unreachable	

3. Route Policy – Testing

Route List							٦×
Routes Nexthops Rules	VRF						
	Ŭ			Fine		all	₹
Dst. Address	Gateway		Distance	Routing Mark	Pref. S	Source	-
AS 0.0.0/0	192.168.137.1 reachable ether 1-W	VAN					
ASB 8.8.8.8	192.168.137.1		1	1			
DAC 192.168.88.0/24	ether2-LAN reachable		()	192.1	68.88.1	
DAC 192.168.137.0/24	ether1-WAN reachable		()	192.1	68.137.	10
4 items							
[admin@MikroTik] > pin	ng 8.8.8.8						
SEQ HOST		SIZE TTL TIME	STATUS				
0			no route to	host			
1			no route to	host			
2			no route to	host			
3			no route to	host			
4			no route to	host			
5			no route to	host			
6			no route to	host			
7			no route to	host			
8			no route to	host			
9			no route to	host			

no route to host

sent=11 received=0 packet-loss=100%

10

3. Route Policy – Result

C:\Windows\system32\cmd.exe Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. E 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.

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

🔏 Quick Set			
CAPsMAN			
🛲 Interfaces			
🚊 Wireless			
📲 Bridge			
📑 PPP			
°t <mark>8</mark> Mesh			
😇 IP 🗈 🗅	ARP	Firewall	
👳 IPv6 🛛 🗅	Accounting	Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols	
🖉 MPLS 🗈 🗈	Addresses	🔄 🕂 🗁 🔗 🖆 🍞 00 Reset Counters 🛛 00 Reset All Counters	Find all
😹 Routing 🛛 🗅	DHCP Client	# Action Chain Src. Address Dst. Address Proto Src. Port Dst. Port In. Inter Out. Int Bytes	Packets 💌
∰ System ►	DHCP Relay		
Queues	DHCP Server		
Files	DNS		
E Log	Firewall		
A Radius	Hotspot		
🗶 Tools 🔹 🗈	IPsec		
New Terminal	Neighbors		
E KVM	Packing		
Make Supout if	Pool		
Manual	Routes		
New WinBox	SMB	0 items	
Exit	SNMP		
	Services		
	Settings		
	Socks		
p Q	TFTP		
B	Traffic Flow		
no	UPnP		
ž	Web Proxy		
_		-	

Firewall Rule <80,443>				
General Advanced Extr	a Action	Statisti	cs	ОК
Chain: fo	rward		₹	Cancel
Src. Address:			•	Apply
Dst. Address:			•	Disable
Protocol:	6 (tcp)	₹		Comment
Src. Port:			-	Сору
Dst. Port:	80,443			Remove
Any. Port:			-	Reset Counters
P2P:			-	Reset All Counters
In. Interface:	ether2-LA	N Ŧ		
Out. Interface:	ether1-W	AN Ŧ	•	
In. Interface List:			•	
Out. Interface List:			-	
Packet Mark:			-	
Connection Mark:			-	
Routing Mark:			-	
Routing Table:			-	
Connection Type:			-	
Connection State:			-	
Connection NAT State:			•	

4. Content Filter – Applying

Firewall Rule <80,443>	
General Advanced Extra Action Statistics	ОК
Src. Address List:	Cancel
Dst. Address List:	Apply
Layer7 Protocol:	Disable
	Comment
	Сору
Connection Bytes:	Remove
Connection Rate:	Reset Counters
Per Connection Classifier:	Reset All Counters
Src. MAC Address:	

4. Content Filter – Result

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

Connecting	× +							- P	×
(i) example.com/		×	Q Search	☆	Ê	+	⋒		≡



4. Content Filter – Result

Firewall																Ξ×
Filter F	ules NAT	Mangle	Service Ports	Connections	Address Li	sts Li	ayer7 Protocol	8								
+	- 0	× 🖻	9 00 Re:	set Counters	00 Reset	All Cou	unters						[Find	all	₹
#	Action	Chain	Src. Addr	ress Dst.	Address Pro	tocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Layer7 Protocol	Content	Bytes	Packets		•
0	💥 drop	forward			6 (ср)		80,443	ether2-LAN	ether1-WAN		example	7.5 Ki	3	22	
1																

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)+.*

[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		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		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	e dot m	atch newlines x ignore whitespace in regex of	o perform #	{} substitutions only once

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

5. Layer 7 Firewall – Applying

New Firewall Rule	×	New Firewall Rule		New Firewall Rule
General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics
Chain: forward	Cancel	Src. Address List:	Cancel	Action: drop
Src. Address: 192.168.3.0/24	Apply	Dst. Address List:	Apply	
Dst. Address:	Disable	Layer7 Protocol: 🗌 example 두 🔺	Disable	Log Prefix:
Protocol: 6 (tcp) 🖛 🔺	Comment	Content:	Comment	
Src. Port:	Сору	Connection Bytes:	Сору	
Dst. Port: 280,443	Remove	Connection Rate:	Remove	
Any. Port:	Reset Counters	Per Connection Classifier:	Reset Counters	
P2P: ▼	Reset All Counters	Src. MAC Address:	Reset All Counters	
In. Interface: 🗌 ether2-LAN 🐺 🔺				
Out. Interface: ether1-WAN 🗧 🔺		Out. Bridge Port:		

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 ③

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 ininterface=ether2-LAN protocol=tcp src-address=192.168.3.0/24

6. Dst. IP Address/Port Block – Applying (2)

Firewall	Firewall Rule <192.168.3.0/24->80,443>	Firewall Rule <192.168.3.0/24->80,443>	Firewall Rule <192.168.3.0/24->80,443>		
Filter Rules NAT Mangle Service Ports	General Advanced Extra Action Statistics	General Advanced Extra Action Statistics	General Advanced Extra Action Statistics		
+ - • × 7	Chain: forward	Src. Address List:	Action: drop		
Name ∠ Address ● local-website 10.10.10.10	Src. Address: 192.168.3.0/24	Dst. Address List: 🗌 local-website 🔻 🔺			
local-website 10.10.10.20 local-website 10.10.10.30	Dst. Address:	Layer7 Protocol:	Log Prefix:		
local-website 10.10.10.40 local-website 10.10.10.50	Protocol: 6 (tcp) 🔻 🔺	Content:			
local-website 10.10.10.60 local-website 10.10.10.70	Src. Port:	Connection Bytes:			
local-website 10.10.10.80 local-website 10.10.10.90	Dst. Port: 80,443	Connection Rate:			
local-website 10.10.10.100 local-website 10.10.10.110	Any. Port:	Per Connection Classifier:			
	P2P:	Src. MAC Address:			
	Out. Interface:	Out. Bridge Port:			

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)

wall									
ter Rules NAT Ma	angle Raw Service Po	rts Connections	Address Lists	Layer7 Protoco					
+ *									
Name 🗡	Address	Creation Time							
o blocked-web	facebook.com	Mar/25/2017 08:	57:19						
;;;facebook.com									
Is blocked-web	31.13.78.35	Mar/25/2017 09:	02:48						
 blocked-web 	youtube.com	Mar/25/2017 09:	03:02						
;;; youtube.com									
blocked-web	74.125.200.190	Mar/25/2017 09:	03:02						
;;; youtube.com									
blocked-web	74.125.200.136	Mar/25/2017 09:	03:02						
;;; youtube.com									
blocked-web	74.125.200.93	Mar/25/2017 09:	03:02						
;;; youtube.com									
blocked-web	74.125.200.91	Mar/25/2017 09:	03:02						
	ter Rules NAT Ma Name Solution Name Solution Solu	wwall ter Rules NAT Mangle Raw Service Po Image: Service Po Image: Service Po Image: Service Po Image: Name Address Image: Service Po Image: Service Po Address Image: Service Po Name Address Image: Service Po Image: Service Po Service Po Image: Service Po Image: Service Po Service Po Image: Service Po Image: Service Po Service Po Service Po Image: Service Po Service Po Service Po	wall ter Rules NAT Mangle Raw Service Ports Connections Image Address Creation Time Image Image Address Creation Time Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image <thimage< th=""> <td>wall ter Rules NAT Mangle Raw Service Ports Connections Address Lists Image X Image X Service Ports Connections Address Lists Image X Image X Image X Service Ports Connections Address Lists Name X Address Creation Time Image X Service Ports Creation Time Image Address Creation Time Mar/25/2017 08:57:19 Service Ports Service Ports Image Address Creation Time Mar/25/2017 09:03:02 Service Ports Service Ports Image Image Address Mar/25/2017 09:03:02 Service Ports Service Ports Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image</td></thimage<>	wall ter Rules NAT Mangle Raw Service Ports Connections Address Lists Image X Image X Service Ports Connections Address Lists Image X Image X Image X Service Ports Connections Address Lists Name X Address Creation Time Image X Service Ports Creation Time Image Address Creation Time Mar/25/2017 08:57:19 Service Ports Service Ports Image Address Creation Time Mar/25/2017 09:03:02 Service Ports Service Ports Image Image Address Mar/25/2017 09:03:02 Service Ports Service Ports Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image					

Firewall Address	List <blocked-web></blocked-web>		
Name:	blocked-web	₹	ОК
Address:	facebook.com		Cancel
Timeout:		•	Apply
Creation Time:	Mar/25/2017 08:57:19		Disable
			Comment
			Сору
			Remove
enabled			

 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)

New Firewall Rule		Firewall Rule <192.168.3.0/24->80,443>		Firewall Rule <192.168.3.0/24->80,443>		
General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics		
Chain: forward	Cancel	Src. Address List:	Cancel	Action: drop		
Src. Address: 192.168.3.0/24	Apply	Dst. Address List: Diocked-web 🗧 🔺	Apply	Log		
Dst. Address:	Disable	Layer7 Protocol:	Disable	Log Prefix:		
Protocol: 6 (tcp) 🗧 🔺	Comment	Content:	Comment			
Src. Port:	Сору	Connection Bytes:	Сору			
Dst. Port: 🗌 80,443	Remove	Connection Bate:	Remove			
Any. Port:	Reset Counters	Per Connection Classifier:	Reset Counters			
P2P:	Reset All Counters		Reset All Counters			
In. Interface: 🗌 ether2-LAN 🗧						
Out. Interface: 🗌 ether1-WAN 🔻 🔺		Out. Bridge Port:				

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 \bigcirc

are we finish? NO! we need to see the main problem ③

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 outinterface=ether1-WAN protocol=tcp

add action=drop chain=forward dst-port=1701 in-interface=ether2-LAN outinterface=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 srcaddress=192.168.3.0/24

add action=drop chain=forward dst-address=0.0.0.0/0 srcaddress=192.168.3.0/24

Firewall												
Filter Ru	les NAT I	Mangle 3	Service Ports	Connection	Address	Lists La	ayer7 Protoco	ls				
+ -												
#	Action	Chain	Src. Addr	ress 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** and listed in **MikroTik Certified Consultant**