



MUM SAUDI ARABIA

OCTOBER 2017

Jonathan “JAY” Soriano

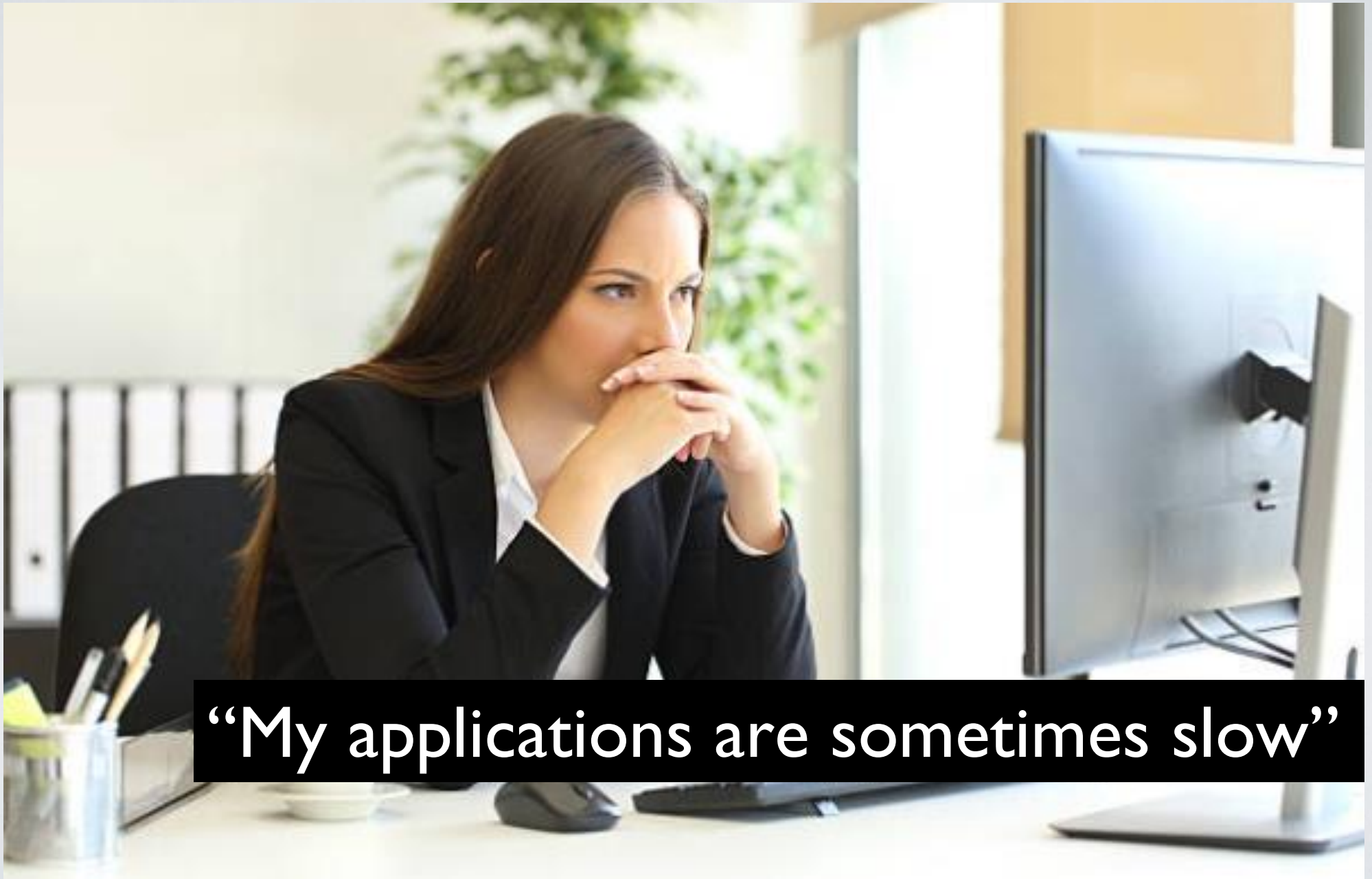
- Networking Enthusiast
- MikroTik user since 2011
- Unofficial Trainer





Identifying and Managing Traffic in RouterOS

Challenge



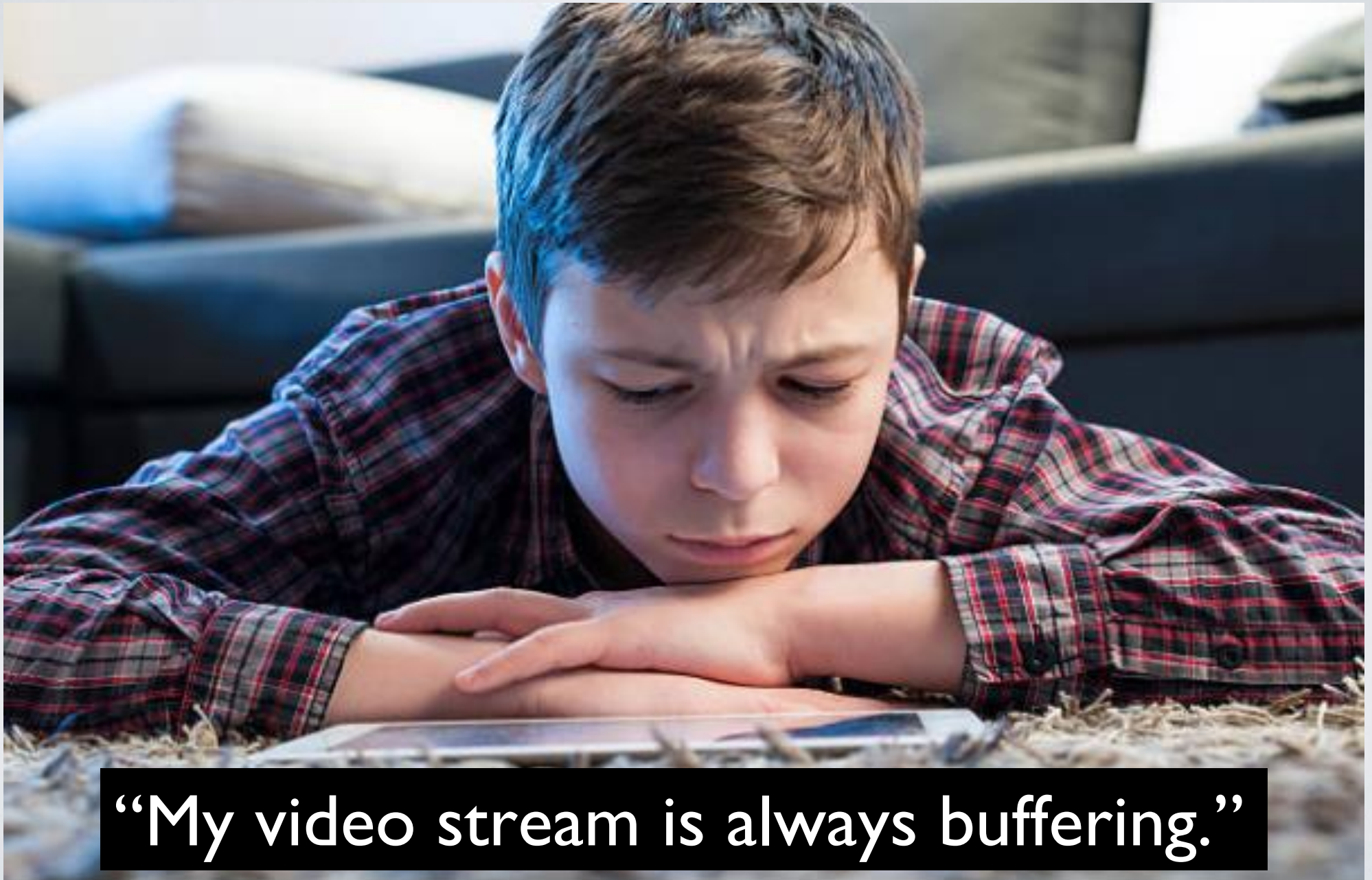
“My applications are sometimes slow”

Challenge



“My voice calls drop at times.”

Challenge



“My video stream is always buffering.”

Why

- ✓ Slow link to the service provider network
- ✓ Poor physical & logical network planning & implementation
- ✓ Underpowered hardware
- ✓ Malicious software, online and offline threats.
- ✓ Excessive downloaders, uploaders.

Identify

Filter

Mangle

DNS

Address List

Manage

Queues



hAP ac

RB962UiGS-5HacT2HnT

Identify

to recognize something

Filter

Block MAC

General

Chain: forward 

Out. Interface: ☐ ether1  ▲

Advanced

Src. MAC Address: ☐ C0:D3:C0:31:E8:D1 ▲

Action

Action: drop 

Block IP

General

Chain: forward 

Src. Address: ☐ 192.168.88.4 ▲

Out. Interface: ☐ ether1  ▲

Action

Action: drop 

Mangle

Identify Port & Protocol

General

Chain: prerouting

Protocol: ☐ 6 (tcp)

Dst. Port: ☐ 80,8080,20,21,443

General

Chain: prerouting

Protocol: ☐ 17 (udp)

Dst. Port: ☐ 80,8080,20,21,443

Mark Connection

Action

Action: mark connection

New Connection Mark: web-connection

☒ Passthrough

Mark Packet

General

Chain: prerouting

Connection Mark: ☐ web-connection

Action

Action: mark packet

New Packet Mark: web-packet

☐ Passthrough

Mangle

Firewall

Filter Rules

NAT

Mangle

Raw

Service Ports

Connections

Address Lists

Layer7 Protocols

+

−

✓

✗

📄

🔍

00 Reset Counters

00 Reset All Counters

Find

all

⬇

#	Action	Chain	Protocol	Dst. Port	Bytes	Packets	
⋮ Web							
0	 mark connection	prerouting	6 (tcp)	80,8080,443,20,21	0 B	0	
1	 mark connection	prerouting	17 (udp)	80,8080,443,20,21	0 B	0	
2	 mark packet	prerouting			0 B	0	

3 items

Connection Bytes

Mark Connection

General	
Chain:	prerouting 
Protocol:	☐ 6 (tcp)  ▲
Dst. Port:	☐ 80,8080,20,21,443 ▲

General	
Chain:	prerouting 
Protocol:	☐ 17 (udp)  ▲
Dst. Port:	☐ 80,8080,20,21,443 ▲

Advanced	
Connection Bytes:	3000001-0 ▲

Action	
Action:	mark connection 
New Connection Mark:	3M-connection 
☒ Passthrough	

Mark Packet

General	
Chain:	prerouting 
Connection Mark:	☐ 3M-connection  ▲

Action	
Action:	mark packet 
New Packet Mark:	3M-packet 
☐ Passthrough	

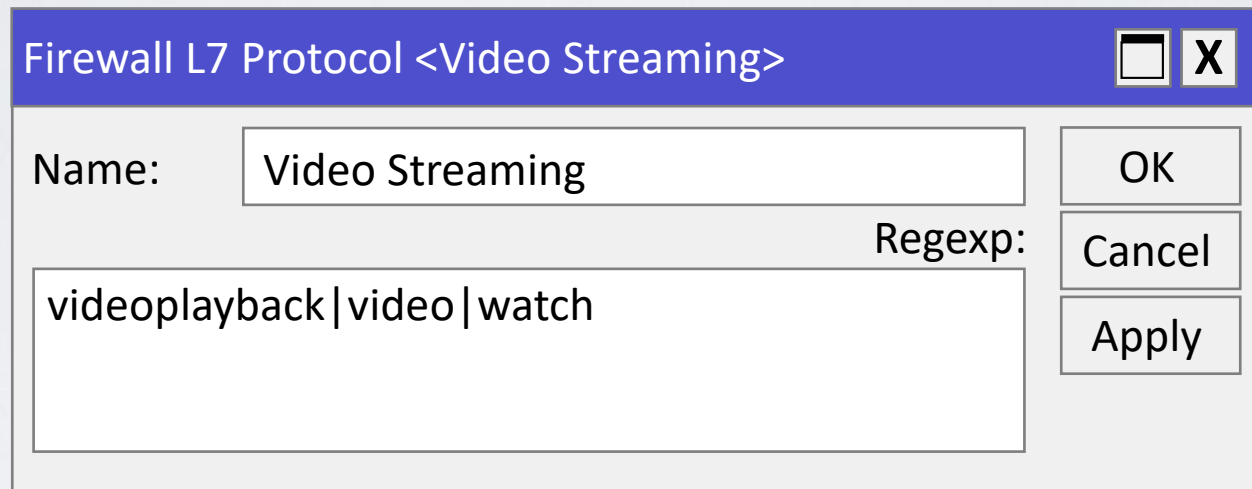
Mangle

#	Action	Chain	Protocol	Dst. Port	Bytes	Packets	Comment
0	mark connection	prerouting	6 (tcp)	80,8080,443,20,21	25.1 KiB	202	Web
1	mark connection	prerouting	17 (udp)	80,8080,443,20,21	964.3 KiB	12 968	
2	mark connection	prerouting	6 (tcp)	80,8080,20,21,443	0 B	0	Download more than 3Mb
3	mark connection	prerouting	17 (udp)	80,8080,20,21,443	884.5 KiB	12 287	
4	mark packet	prerouting			31.2 MiB	35 369	3M Packet
5	mark packet	prerouting			1655.6 KiB	2 244	Web Packet

6 items

Layer-7

Layer-7



Firewall L7 Protocol <Video Streaming>

Name: Video Streaming

Regexp: videoplayback|video|watch

OK

Cancel

Apply

Layer-7

Mark Connection

General

Chain: prerouting 

Advanced

Layer7 Protocol: ☐ Video Streaming 

Action

Action: mark connection 

New Connection Mark: Video-connection 

☒ Passthrough

Mark Packet

General

Chain: prerouting 

Connection Mark: ☐ Video-connection  ▲

Action

Action: mark packet 

New Packet Mark: Video-packet 

☐ Passthrough

Mangle

Firewall								
Filter Rules		NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols
						Reset Counters		Reset All Counters
		Find		all				
#	Action	Chain	Protocol	Dst. Port	Bytes	Packets	Comment	
0	mark connection	prerouting			316.3 MiB	358 674	Video	
1	mark packet	prerouting			300.4 MiB	340 861	Video Packet	
2	mark connection	prerouting	6 (tcp)	80,8080,443,20,21	14.6 MiB	152 851	Web	
3	mark connection	prerouting	17 (udp)	80,8080,443,20,21	12.3 MiB	157 629		
4	mark connection	prerouting	6 (tcp)	80,8080,20,21,443	6.1 MiB	132 492	Download more than 3Mb	
5	mark connection	prerouting	17 (udp)	80,8080,20,21,443	6.0 MiB	90 024		
6	mark packet	prerouting			609.5 MiB	663 391	3M Packet	
7	mark packet	prerouting			84.1 MiB	112 898	Web Packet	

DNS

DNS Cache

DNS Cache

Flush Cache

Find

	Name	Type	Data	TTL	
	r3.sn-hvcpat-g0i6.googlevideo.com	A	86.51.31.206	00:14:07	
	r5--sn-4g5e6nl6.googlevideo.com	CNAME	r5.sn-4g5e6nl6.googlevideo.com	00:23:06	
	r5--sn-hpa7znsz.googlevideo.com	CNAME	r5.sn-hpa7znsz.googlevideo.com	00:14:08	
	r5.sn-4g5e6nl6.googlevideo.com	A	74.125.104.75	00:23:06	
	r5.sn-hpa7znsz.googlevideo.com	A	173.194.182.138	00:14:08	
	r6--sn-5hne6n7e.googlevideo.com	CNAME	r6.sn-5hne6n7e.googlevideo.com	00:23:07	
	r6--sn-hvcpat-g0ir.googlevideo.com	CNAME	r6.sn-hvcpat-g0ir.googlevideo.com	00:24:18	
	r6.sn-5hne6n7e.googlevideo.com	A	74.125.8.12	00:23:07	
	r6.sn-hvcpat-g0ir.googlevideo.com	A	86.51.30.177	00:24:18	
	r7--sn-hvcpat-g0ir.googlevideo.com	CNAME	r7.sn-hvcpat-g0ir.googlevideo.com	00:23:05	
	r7.sn-hvcpat-g0ir.googlevideo.com	A	86.51.30.178	00:23:05	
	r8--sn-q0c7dn7y.googlevideo.com	CNAME	r8.sn-q0c7dn7y.googlevideo.com	00:28:41	
	r8.sn-q0c7dn7y.googlevideo.com	A	173.194.5.77	00:28:41	
	r12--sn-5hne6ney.googlevideo.com	CNAME	r12.sn-5hne6ney.googlevideo.com	00:14:52	
	r12.sn-5hne6ney.googlevideo.com	A	173.194.156.81	00:14:52	
	r13--sn-5hne6nee.googlevideo.com	CNAME	r13.sn-5hne6nee.googlevideo.com	00:20:55	
	r13--sn-5hne6nse.googlevideo.com	CNAME	r13.sn-5hne6nse.googlevideo.com	00:17:24	
	r13.sn-5hne6nee.googlevideo.com	A	173.194.153.146	00:20:55	
	r13.sn-5hne6nse.googlevideo.com	A	74.125.8.221	00:17:24	

82 items

DNS

Script

Script <video>

Name: video

Owner: jay

Policy:

☒ ftp	☒ reboot
☒ read	☒ write
☒ policy	☒ test
☒ password	☒ sniff
☒ sensitive	☒ romon
☐ dude	

Last Time Started: Oct/18/2017 00:56:50

Run Count: 203

Source:

```
local myServers { "video" }
local myListName "Youtube"
local myTimeout "00:30:00"

/p dns cache all {
  foreach i in=$myServers do={
    foreach j in=$myListName do={
      do {
        local myName [get $j name]
        local myType [get $j type]
        local myData [get $j data]

        if ($myType = "A") do={
          do {
            /ip firewall address-list add address=$myData list=$myListName comment="$i-$myName" timeout=$myTimeout
          } on-error={
            put "DNSCACHE: Error on $myName $myData $myType"
          }
        }

        if ($myType = "CNAME") do={
          local currentName $j
          local nextName [find where (name=$myData && type="CNAME")]

          while ($nextName != "") do={
            set currentName $nextName
            resolve $currentName
            set nextName [find where (name=[get $nextName data] && type="CNAME")]
          }

          resolve [get $currentName data]
        }

        foreach k in=$myListName do={
          set myData [get $k data]
          do {
            /ip firewall address-list add address=$myData list=$myListName comment="$i-$myName" timeout=$myTimeout
          } on-error={
            put "DNSCACHE: Error on $myName $myData $myType"
          }
        }
      }
    }
  }
} on-error={
  put "DNSCACHE: Missing Entry"
}
```

Scheduler

Schedule <run every 5 seconds>

Name: run every 5 seconds

Start Date: Oct/17/2017

Start Time: 21:45:53

Interval: 00:00:05

Owner: jay

Policy:

☒ ftp	☒ reboot
☒ read	☒ write
☒ policy	☒ test
☒ password	☒ sniff
☒ sensitive	☒ romon
☐ dude	

Run Count: 276

Next Run: Oct/18/2017 01:01:58

On Event:

```
/system script run video
```

enabled

Address List

Firewall					
Filter Rules	NAT	Mangle	Raw	Service Ports	Connections
Address Lists	Layer7 Protocols				
Find					all
Name	Address	Timeout	Creation Time	Comment	
D Youtube	86.51.31.206	00:05:19	Oct/18/2017 ...	video-r3--sn-hvcpat-g0i6.googlevideo.com	
D Youtube	173.194.182.138	00:05:19	Oct/18/2017 ...	video-r5--sn-hpa7znsz.googlevideo.com	
D Youtube	173.194.156.81	00:05:19	Oct/18/2017 ...	video-r12--sn-5hne6ney.googlevideo.com	
D Youtube	74.125.8.221	00:09:15	Oct/18/2017 ...	video-r13--sn-5hne6nse.googlevideo.com	
D Youtube	86.51.30.173	00:09:15	Oct/18/2017 ...	video-r2--sn-hvcpat-g0ir.googlevideo.com	
D Youtube	74.125.68.105	00:13:14	Oct/18/2017 ...	video-googlevideo.com	
D Youtube	74.125.68.99	00:13:14	Oct/18/2017 ...	video-googlevideo.com	
D Youtube	74.125.68.104	00:13:14	Oct/18/2017 ...	video-googlevideo.com	
D Youtube	74.125.68.106	00:13:14	Oct/18/2017 ...	video-googlevideo.com	
D Youtube	74.125.68.147	00:13:14	Oct/18/2017 ...	video-googlevideo.com	
D Youtube	74.125.68.103	00:13:14	Oct/18/2017 ...	video-googlevideo.com	
D Youtube	173.194.138.102	00:13:15	Oct/18/2017 ...	video-r1--sn-q0c7dn76.googlevideo.com	
D Youtube	74.125.100.7	00:13:15	Oct/18/2017 ...	video-r2--sn-5hnekn7l.googlevideo.com	
D Youtube	173.194.153.146	00:13:15	Oct/18/2017 ...	video-r13--sn-5hne6nee.googlevideo.com	
D Youtube	86.51.30.178	00:13:15	Oct/18/2017 ...	video-r7--sn-hvcpat-g0ir.googlevideo.com	
D Youtube	74.125.104.75	00:13:15	Oct/18/2017 ...	video-r5--sn-4g5e6nl6.googlevideo.com	
D Youtube	74.125.8.137	00:13:16	Oct/18/2017 ...	video-r3--sn-5hnednlk.googlevideo.com	
D Youtube	74.125.8.12	00:13:16	Oct/18/2017 ...	video-r6--sn-5hne6n7e.googlevideo.com	
D Youtube	86.51.30.177	00:13:55	Oct/18/2017 ...	video-r6--sn-hvcpat-g0ir.googlevideo.com	
D Youtube	173.194.5.77	00:18:39	Oct/18/2017 ...	video-r8--sn-q0c7dn7y.googlevideo.com	
D Youtube	86.51.30.175	00:21:26	Oct/18/2017 ...	video-r4--sn-hvcpat-g0ir.googlevideo.com	
D Youtube	74.125.100.138	00:25:27	Oct/18/2017 ...	video-r4--sn-5hnedn7e.googlevideo.com	
D Youtube	74.125.8.154	00:29:17	Oct/18/2017 ...	video-r4--sn-5hnednlr.googlevideo.com	

Address List

Mark Connection

General

Chain: prerouting

Advanced

Dst. Address List: ☐ Youtube

Action

Action: mark connection

New Connection Mark: Video-connection

☒ Passthrough

Mark Packet

General

Chain: prerouting

Connection Mark: ☐ Video-connection

Action

Action: mark packet

New Packet Mark: Video-packet

☐ Passthrough

Mangle

Firewall																					
Filter Rules		NAT		Mangle		Raw		Service Ports		Connections		Address Lists		Layer7 Protocols							
												Reset Counters		Reset All Counters		Find		all			
#		Action	Chain	Protocol	Dst. Port	Bytes	Packets	Comment													
0		mark connection	prerouting			13.6 MiB	153 192	Video Address List													
1		mark connection	prerouting			474.8 MiB	542 404	Video													
2		mark packet	prerouting			855.7 MiB	971 182	Video Packet													
3		mark connection	prerouting	6 (tcp)	80,8080,443,20,21	24.5 MiB	167 549	Web													
4		mark connection	prerouting	17 (udp)	80,8080,443,20,21	30.4 MiB	314 872														
5		mark connection	prerouting	6 (tcp)	80,8080,20,21,443	6.1 MiB	132 492	Download more than 3Mb													
6		mark connection	prerouting	17 (udp)	80,8080,20,21,443	20.0 MiB	218 111														
7		mark packet	prerouting			929.1 MiB	1 024 928	3M Packet													
8		mark packet	prerouting			160.4 MiB	217 092	Web Packet													
9 items																					

Mangle

Other Traffic

[illegible]

Manage

maintain control over something

A wide-angle photograph of a busy airport arrivals hall. In the foreground, a man in a yellow jacket stands with his back to the camera, looking towards the immigration lanes. The hall is filled with people, many with luggage, waiting in lines. The floor is light-colored and polished. In the background, there are several digital displays showing weather information for Riyadh, with a temperature of 13°C. The ceiling is high with recessed lighting. The overall atmosphere is one of organized activity.

First Time Arrivals

Arrivals with
Multiple Exit
Re- entry Visa

GCC Nationals

Class 1



Class 2



Class 3





Toll Plaza

Queues

Simple Queue

Queue List						
Simple Queues Interface Queues Queue Tree Queue Types						
+ - ✓ ✗ 📁 🌐 00 Reset Counters 00 Reset All Counters						
#	Name ^	Target	Upload...	Download ...	Upload	Download
1	📁 Total	192.168.88.0/24	5M	25M	114.2 kbps	3.5 Mbps
2	📁 User-2	192.168.88.2	5M	20M	0 bps	0 bps
3	📁 User-3	192.168.88.3	2M	10M	0 bps	0 bps
4	📁 User-4	192.168.88.4	2M	10M	159 bps	0 bps
5	📁 User-5	192.168.88.5	3M	10M	0 bps	0 bps
6	📁 User-6	192.168.88.6	5M	25M	2.6 kbps	1269 bps
7	📁 User-7	192.168.88.7	5M	25M	0 bps	0 bps
8	📁 User-8	192.168.88.8	5M	25M	0 bps	0 bps

Queue Tree

Queue List							
Simple Queues Interface Queues Queue Tree Queue Types							
+ - ✓ ✗ 📁 🌐 00 Reset Counters 00 Reset All Counters							
	Name ^	Parent	Packet Marks	Priority	Limit At ...	Max ...	Avg. Rate
	📁 Download	local-bridge		8	128k	5M	4.8 Mbps
	📁 a. web d	Download	web-packet	2	3M	5M	29.9 kbps
	📁 b. other d	Download	other-packet	4	1M	5M	419.9 kbps
	📁 c. video d	Download	Video-packet	6	500k	5M	4.4 Mbps
	📁 d. large file d	Download	3M-packet	8	500k	5M	0 bps
	📁 Upload	ether1		8	128k	1M	1005.7 kbps
	📁 a. web u	Upload	web-packet	2	512k	1M	853.1 kbps
	📁 b. other u	Upload	other-packet	4	256k	1M	11.9 kbps
	📁 c. video u	Upload	Video-packet	6	128k	1M	131.8 kbps
	📁 d. large file u	Upload	3M-packet	8	104k	1M	0 bps

Queues

Simple Queue

Queue List						
Simple QueuesInterface QueuesQueue TreeQueue Types						
00 Reset Counters00 Reset All Counters						
#	Name	Target	Upload...	Download ...	Upload	Download
1	Total	192.168.88.0/24	5M	25M	114.2 kbps	3.5 Mbps
2	User-2	192.168.88.2	5M	20M	0 bps	0 bps
3	User-3	192.168.88.3	2M	10M	0 bps	0 bps
4	User-4	192.168.88.4	2M	10M	159 bps	0 bps
5	User-5	192.168.88.5	3M	10M	0 bps	0 bps
6	User-6	192.168.88.6	5M	25M	2.6 kbps	1269 bps
7	User-7	192.168.88.7	5M	25M	0 bps	0 bps
8	User-8	192.168.88.8	5M	25M	0 bps	0 bps

Simple Queue

Parent Queue

Simple Queue <Total>

General

Advanced

Statistics

Traffic

Total

Total Statistics

Name: Total

Target: 192.168.88.0/24



Dst.:



Target Upload

Target Download

Max Limit: 5M



25M



bits/s

Simple Queue

Parent Queue

Simple Queue <Total>

General

Advanced

Statistics

Traffic

Total

Total Statistics

Packet Marks:



Target Upload

Target Download

Limit At:

unlimited



unlimited



bits/s

Priority:

8

8

Bucket Size:

0.100

0.100

ratio

Queue Type:

pcq-upload-default



pcq-download-default



Parent:

none



Simple Queue

Child Queue

Simple Queue <User-2>

General

Advanced

Statistics

Traffic

Total

Total Statistics

Name:

User-2

Target:

192.168.88.2

Dst.:

Target Upload

Target Download

Max Limit:

5M

20M

bits/s

Simple Queue

Child Queue

Simple Queue <User-2>

General

Advanced

Statistics

Traffic

Total

Total Statistics

Packet Marks:



Target Upload

Target Download

Limit At:

unlimited



unlimited



bits/s

Priority:

8

8

Bucket Size:

0.100

0.100

ratio

Queue Type:

default-small



default-small



Parent:

Total



Queues

Simple Queue

Queue List						
Simple QueuesInterface QueuesQueue TreeQueue Types						
00 Reset Counters00 Reset All Counters						
#	Name	Target	Upload...	Download ...	Upload	Download
1	Total	192.168.88.0/24	5M	25M	114.2 kbps	3.5 Mbps
2	User-2	192.168.88.2	5M	20M	0 bps	0 bps
3	User-3	192.168.88.3	2M	10M	0 bps	0 bps
4	User-4	192.168.88.4	2M	10M	159 bps	0 bps
5	User-5	192.168.88.5	3M	10M	0 bps	0 bps
6	User-6	192.168.88.6	5M	25M	2.6 kbps	1269 bps
7	User-7	192.168.88.7	5M	25M	0 bps	0 bps
8	User-8	192.168.88.8	5M	25M	0 bps	0 bps

Queues

Queue Tree

Queue List

Simple Queues

Interface Queues

Queue Tree

Queue Types



00 Reset Counters

00 Reset All Counters

	Name	Parent	Packet Marks	Priority	Limit At ...	Max ...	Avg. Rate
	Download	local-bridge		8	128k	5M	4.8 Mbps
	a. web d	Download	web-packet	2	3M	5M	29.9 kbps
	b. other d	Download	other-packet	4	1M	5M	419.9 kbps
	c. video d	Download	Video-packet	6	500k	5M	4.4 Mbps
	d. large file d	Download	3M-packet	8	500k	5M	0 bps
	Upload	ether1		8	128k	1M	1005.7 kbps
	a. web u	Upload	web-packet	2	512k	1M	853.1 kbps
	b. other u	Upload	other-packet	4	256k	1M	11.9 kbps
	c. video u	Upload	Video-packet	6	128k	1M	131.8 kbps
	d. large file u	Upload	3M-packet	8	104k	1M	0 bps

Network Diagram

Internet Source

Gateway modem

IP address: 192.168.1.1/24

MikroTik Router

ether1: DHCP client

ether2: Master port: none

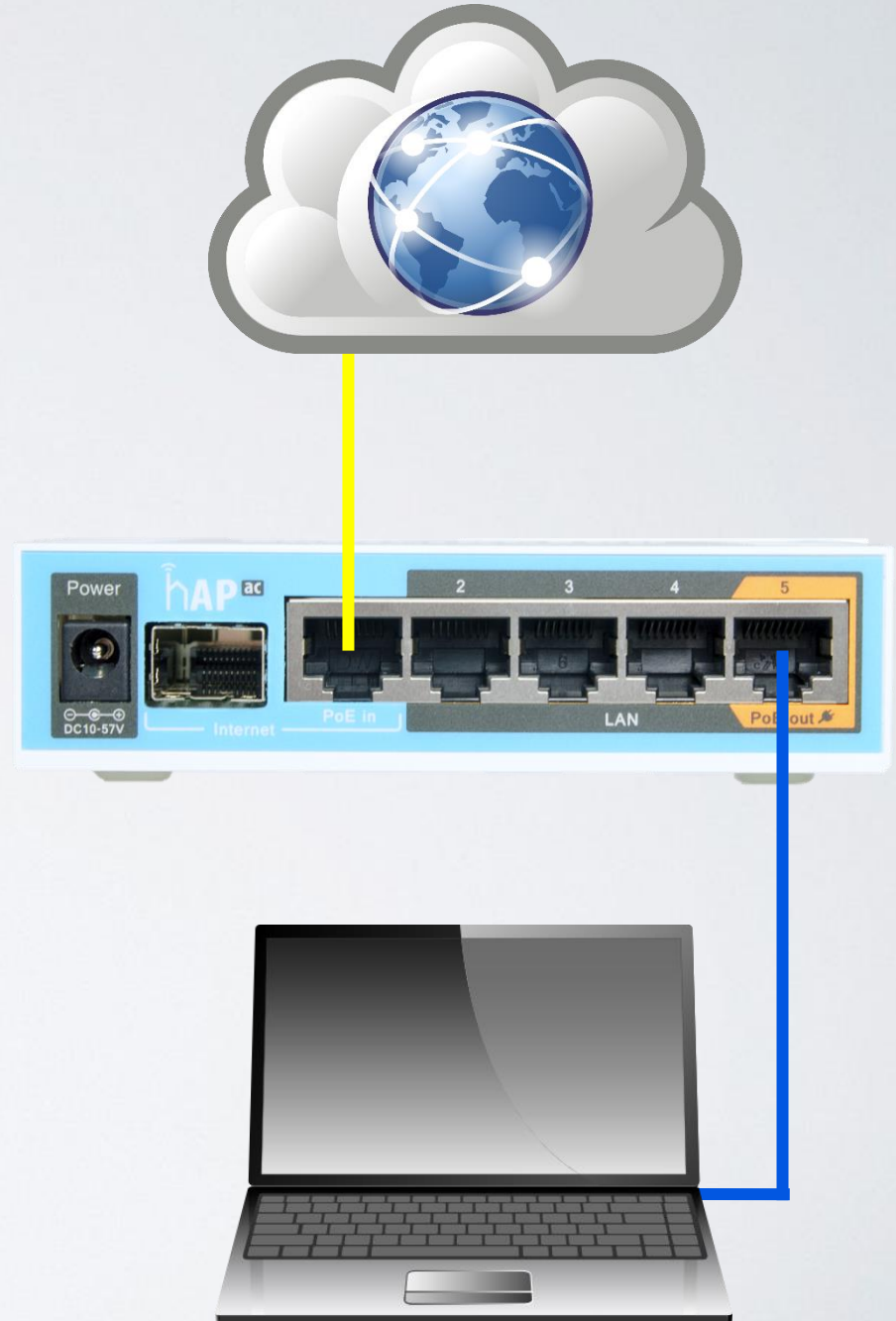
ether3,4,5: Master port: ether2

local-bridge: ether2 & wlan1 ports

local-bridge IP: 192.168.88.1/24

Your Computer

Ethernet: 192.168.88.111



Queue Tree

Parent Queue

Queue <Download>

General

Statistics

Name:

Download

Parent:

local-bridge

▼

Packet Marks:

▲▼

Queue Type:

pcq-download-default

▼

Priority:

8

Bucket Size:

0.100

Limit At:

128k

▲

bits/s

Max Limit:

5M

▲

bits/s

Queue <Upload>

General

Statistics

Name:

Upload

Parent:

ether1

▼

Packet Marks:

▲▼

Queue Type:

pcq-upload-default

▼

Priority:

8

Bucket Size:

0.100

Limit At:

128k

▲

bits/s

Max Limit:

1M

▲

bits/s

Queue Tree

Parent Queue

Queue List							
Simple Queues		Interface Queues		Queue Tree		Queue Types	
						 Reset Counters	 Reset All Counters
	Name	Parent	Packet Marks	Priority	Limit At ...	Max ...	Av ...
	Download	local-bridge		8	128k	5M	
	Upload	ether1		8	128k	1M	

Queue Tree

Child Queue

Queue <a. web d>

General

Statistics

Name:

a. web d

Parent:

Download

▼

Packet Marks:

web-packet

▼

◆

Queue Type:

pcq-download-default

▼

Priority:

2

Bucket Size:

0.100

Limit At:

3M

▲

bits/s

Max Limit:

5M

▲

bits/s

Queue <a. web u>

General

Statistics

Name:

a. web u

Parent:

Upload

▼

Packet Marks:

web-packet

▼

◆

Queue Type:

pcq-upload-default

▼

Priority:

2

Bucket Size:

0.100

Limit At:

512k

▲

bits/s

Max Limit:

1M

▲

bits/s

Queues

Queue Tree

Queue List

Simple Queues

Interface Queues

Queue Tree

Queue Types



00 Reset Counters

00 Reset All Counters

	Name	Parent	Packet Marks	Priority	Limit At ...	Max ...	Avg. Rate
	Download	local-bridge		8	128k	5M	4.8 Mbps
	a. web d	Download	web-packet	2	3M	5M	29.9 kbps
	b. other d	Download	other-packet	4	1M	5M	419.9 kbps
	c. video d	Download	Video-packet	6	500k	5M	4.4 Mbps
	d. large file d	Download	3M-packet	8	500k	5M	0 bps
	Upload	ether1		8	128k	1M	1005.7 kbps
	a. web u	Upload	web-packet	2	512k	1M	853.1 kbps
	b. other u	Upload	other-packet	4	256k	1M	11.9 kbps
	c. video u	Upload	Video-packet	6	128k	1M	131.8 kbps
	d. large file u	Upload	3M-packet	8	104k	1M	0 bps

“I am still learning.”

-Michelangelo, age 87

Disable Fasttrack for Queues to Work

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: special dummy rule to show fasttrack counters											
0	D pas...	forward								0 B	0
::: defconf: accept established,related,untracked											
1	✓ acc...	input								76 B	1
::: defconf: drop invalid											
2	✗ drop	input								0 B	0
::: defconf: accept ICMP											
3	✓ acc...	input			1 (icmp)					0 B	0
::: defconf: drop all not coming from LAN											
4	✗ drop	input								0 B	0
::: defconf: accept in ipsec policy											
5	✓ acc...	forward								0 B	0
::: defconf: accept out ipsec policy											
6	✓ acc...	forward								0 B	0
::: defconf: fasttrack											
7	X .. fastt...	forward								0 B	0
::: defconf: accept established,related, untracked											
8	✓ acc...	forward								0 B	0
::: defconf: drop invalid											
9	✗ drop	forward								0 B	0
::: defconf: drop all from WAN not DSTNATed											
10	✗ drop	forward								0 B	0

11 items (1 selected)

To Reset All Markings, select all then Remove

Firewall									
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols									
Tracking Find									
	Src. Address	Dst. Address	Protocol	Connection ...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes	
SC	192.168.1.100:37410	188.166.225.189:53	17 (udp)		00:00:00		0 bps/0 bps	58 B/74 B	▼
C	192.168.1.100:38451	255.255.255.255:5678	17 (udp)		00:00:03		0 bps/0 bps	141 B/0 B	▲
SC	192.168.1.100:39521	188.166.225.189:53	17 (udp)		00:00:01		0 bps/0 bps	63 B/63 B	
C	192.168.88.1:34276	255.255.255.255:5678	17 (udp)		00:00:03		0 bps/0 bps	147 B/0 B	
SCs	192.168.88.2	108.177.119.101	1 (icmp)		00:00:09		960 bps/480 bps	1776.9 KiB/1776....	
SACs	192.168.88.2:50000	117.207.115.212:45...	17 (udp)	torrent-cm	00:02:52		0 bps/0 bps	37.5 MiB/1180.8 ...	
SCs	192.168.88.2:50000	109.151.143.31:24921	17 (udp)	torrent-cm	00:00:00		0 bps/0 bps	131 B/317 B	
SCs	192.168.88.2:50000	86.173.237.229:16130	17 (udp)	torrent-cm	00:00:07		0 bps/0 bps	131 B/317 B	
SACs	192.168.88.2:52516	173.194.79.94:443	17 (udp)		00:01:29		0 bps/0 bps	2820 B/1855 B	
SACs	192.168.88.2:52710	157.56.106.189:3544	17 (udp)		00:02:58		712 bps/0 bps	260.1 KiB/165.7 ...	
SACs	192.168.88.2:54412	108.177.119.100:443	17 (udp)		00:02:08		0 bps/0 bps	19.3 KiB/9.0 KiB	
SACs	192.168.88.2:55896	8.8.8.8:53	17 (udp)		00:01:15		0 bps/0 bps	146 B/314 B	
SACs	192.168.88.2:58185	169.55.74.56:443	6 (tcp)		23:59:43	established	0 bps/0 bps	212.4 KiB/342.4 ...	
SACs	192.168.88.2:58209	195.122.177.224:443	6 (tcp)		23:56:38	established	0 bps/0 bps	23.3 KiB/19.7 KiB	
SACs	192.168.88.2:58211	40.77.229.52:443	6 (tcp)		23:44:54	established	0 bps/0 bps	6.8 KiB/8.5 KiB	
SACs	192.168.88.2:58218	198.178.123.8:7168	6 (tcp)		23:59:59	established	1600 bps/135.5 kbps	6.8 MiB/479.0 MiB	
SACs	192.168.88.2:58221	74.125.143.125:5222	6 (tcp)		23:59:53	established	0 bps/0 bps	162.0 KiB/109.1 ...	
SACs	192.168.88.2:58233	159.122.189.46:5938	6 (tcp)		23:59:57	established	0 bps/0 bps	103.6 KiB/67.3 KiB	
SACs	192.168.88.2:58251	145.239.13.147:443	6 (tcp)		23:59:52	established	0 bps/0 bps	137.2 KiB/94.4 KiB	▼
63 items					Max Entries: 218008				

No need to reboot or shutdown the device

References

```
/ip firewall layer7-protocol
add name="Video Streaming" regexp=videoplayback|video|watch

/ip firewall mangle
add action=mark-connection chain=prerouting comment="Video Address List" dst-address-list=Youtube new-connection-mark=Video-connection passthrough=yes
add action=mark-connection chain=prerouting comment="Video Layer7" layer7-protocol="Video Streaming" new-connection-mark=Video-connection passthrough=yes
add action=mark-packet chain=prerouting comment="Video Packet" connection-mark=Video-connection new-packet-mark=Video-packet passthrough=no
add action=mark-connection chain=prerouting comment=Web dst-port=80,8080,443,20,21 new-connection-mark=web-connection passthrough=yes protocol=tcp
add action=mark-connection chain=prerouting dst-port=80,8080,443,20,21 new-connection-mark=web-connection passthrough=yes protocol=udp
add action=mark-connection chain=prerouting comment="Large file more than 3Mb" connection-bytes=3000001-0 dst-port=80,8080,20,21,443 new-connection-mark=3M-connection passthrough=yes protocol=tcp
add action=mark-connection chain=prerouting connection-bytes=3000001-0 dst-port=80,8080,20,21,443 new-connection-mark=3M-connection passthrough=yes protocol=udp
add action=mark-packet chain=prerouting comment="3M Packet" connection-mark=3M-connection new-packet-mark=3M-packet passthrough=no
add action=mark-packet chain=prerouting comment="Web Packet" connection-mark=web-connection new-packet-mark=web-packet passthrough=no
add action=mark-connection chain=prerouting comment=Other dst-port=1000-65535 new-connection-mark=other-connection passthrough=yes protocol=tcp
add action=mark-connection chain=prerouting dst-port=1000-65535 new-connection-mark=other-connection passthrough=yes protocol=udp
add action=mark-packet chain=prerouting comment="Other Packet" connection-mark=other-connection new-packet-mark=other-packet passthrough=no

/queue tree
add limit-at=128k max-limit=5M name=Download parent=bridge queue=pcq-download-default
add limit-at=128k max-limit=1M name=Upload parent=ether1 queue=pcq-upload-default
add limit-at=3M max-limit=5M name="a. web d" packet-mark=web-packet parent=Download priority=2 queue=pcq-download-default
add limit-at=500k max-limit=3M name="d. large file d" packet-mark=3M-packet parent=Download queue=pcq-download-default
add limit-at=500k max-limit=3M name="c. video d" packet-mark=Video-packet parent=Download priority=6 queue=pcq-download-default
add limit-at=1M max-limit=4M name="b. other d" packet-mark=other-packet parent=Download priority=4 queue=pcq-download-default
add limit-at=512k max-limit=1M name="a. web u" packet-mark=web-packet parent=Upload priority=2 queue=pcq-upload-default
add limit-at=104k max-limit=256k name="d. large file u" packet-mark=3M-packet parent=Upload queue=pcq-upload-default
add limit-at=128k max-limit=500k name="c. video u" packet-mark=Video-packet parent=Upload priority=6 queue=pcq-upload-default
add limit-at=256k max-limit=768k name="b. other u" packet-mark=other-packet parent=Upload priority=4 queue=pcq-upload-default

/system scheduler
add interval=30s name="run every 30 seconds" on-event="/system script run video" policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon start-date=oct/10/2017 start-time=20:00:00
```

URL Links:

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

<https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter>

<https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Mangle>

<https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/L7>

https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Address_list

<https://wiki.mikrotik.com/wiki/Manual:IP/DNS>

https://wiki.mikrotik.com/wiki/Sync_Address_List_from_DNS_Lookup_Results_-_CNAME_and_A_Records

<https://wiki.mikrotik.com/wiki/Manual:Scripting-examples>

<https://wiki.mikrotik.com/wiki/Manual:Queue>

<http://www.istockphoto.com>

References

Script

Script <video>

Name: video

Owner: jay

Policy:

☒ ftp	☒ reboot
☒ read	☒ write
☒ policy	☒ test
☒ password	☒ sniff
☒ sensitive	☒ romon
☐ dude	

Last Time Started: Oct/18/2017 00:56:50

Run Count: 203

Source:

```
local myServers { "video" }
local myListName "Youtube"
local myTimeout "00:30:00"

/ip dns cache all {
  foreach i in=$myServers do={
    foreach j in=[find where (name~$i)] do={
      do {
        local myName [get $j name]
        local myType [get $j type]
        local myData [get $j data]

        if ($myType = "A") do={
          do {
            /ip firewall address-list add address=$myData list=$myListName comment="$i-$myName" timeout=$myTimeout
          } on-error={
            put "DNSCACHE: Error on $myName $myData $myType"
          }
        }

        if ($myType = "CNAME") do={
          local currentName $j
          local nextName [find where (name=$myData && type="CNAME")]

          while ($nextName != "") do={
            set currentName $nextName
            resolve $currentName
            set nextName [find where (name=[get $nextName data] && type="CNAME")]
          }

          resolve [get $currentName data]

          foreach k in=[find where (name=[get $currentName data] && type="A")] do={
            set myData [get $k data]
            do {
              /ip firewall address-list add address=$myData list=$myListName comment="$i-$myName" timeout=$myTimeout
            } on-error={
              put "DNSCACHE: Error on $myName $myData $myType"
            }
          }
        }
      } on-error={
        put "DNSCACHE: Missing Entry"
      }
    }
  }
}
```

```
/system script
add name=video owner=jay policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon source=:lo\
cal myServers { \"video\" } \r\
\n:local myListName \"Youtube\" \r\
\n:local myTimeout \"00:30:00\" \r\
\n\r\
\n/ip dns cache all { \r\
\n  :foreach i in=$myServers do={ \r\
\n    :foreach j in=[find where (name~$i)] do={ \r\
\n      :do { \r\
\n        :local myName [get $j name] \r\
\n        :local myType [get $j type] \r\
\n        :local myData [get $j data] \r\
\n\r\
\n        :if ($myType = \"A\") do={ \r\
\n          :do { \r\
\n            /ip firewall address-list add address=$myData lis\
t=$myListName comment=\"$i-$myName\" timeout=$myTimeout \r\
\n          } on-error={ \r\
\n            :put \"DNSCACHE: Error on $myName $myData $myTy\
pe\" \r\
\n          } \r\
\n        } \r\
\n\r\
\n        :if ($myType = \"CNAME\") do={ \r\
\n          :local currentName $j \r\
\n          :local nextName [find where (name=$myData && type=\"C\
NAME\")] \r\
\n\r\
\n          :while ($nextName != \"\") do={ \r\
\n            :set currentName $nextName \r\
\n            :resolve $currentName \r\
\n            :set nextName [find where (name=[get $nextName da\
ta] && type=\"CNAME\")] \r\
\n          } \r\
\n\r\
\n          :resolve [get $currentName data] \r\
\n\r\
\n          :foreach k in=[find where (name=[get $currentName dat\
a] && type=\"A\")] do={ \r\
\n            :set myData [get $k data] \r\
\n            :do { \r\
\n              /ip firewall address-list add address=$myData \
\_list=$myListName comment=\"$i-$myName\" timeout=$myTimeout \r\
\n            } on-error={ \r\
\n              :put \"DNSCACHE: Error on $myName $myData $ \
myType\" \r\
\n            } \r\
\n          } \r\
\n\r\
\n          } on-error={ \r\
\n            :put \"DNSCACHE: Missing Entry\" \r\
\n          } \r\
\n        } \r\
\n      } \r\
\n    } \r\
\n  } \r\
}
```