

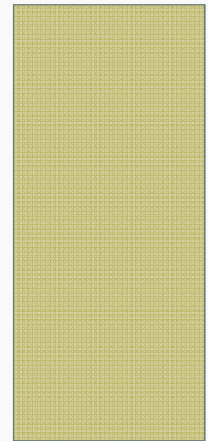
# **Bienvenue au CAMEROUN**



# MikroTik

## **FIREWALL ET GESTION DE BANDE PASSANTE**

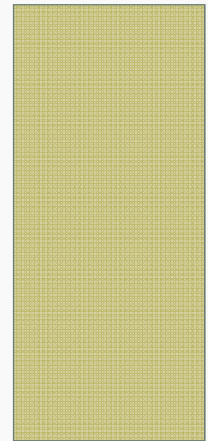
Mikrotik MUM – Yaoundé  
January 26, 2018



# MikroTik

## FIREWALL AND BANDWIDTH MANAGEMENT

Mikrotik MUM – Yaoundé  
January 26, 2018



# ULRICK NKWEDJA LAKOUDJI

- Using MikroTik since 2013 as Technical support in CLBCNET (MTN Partner)
- 2015 – Technical Team Coordinator at SOCAPRESCO (MTN Partner)
- 2017 – Certified MTCNA , MTCRE , CCNA Instructor, ...
- 2017 – NOC & SAV Engineer, SAV Supervisor at SWECOM

# SWECOM OVERVIEW

SWECOM stands for SOUTHWEST COMMUNICATION and it started as a cable distributor in Fako in 1998.

It later extended its distribution to some other regions by 2005.

However in 2008 SWECOM established an IT department and became an internet service provider (ISP) in Douala and in 2011 it extended to other regions.

Finally in 2014 it included VOD (VIDEO ON DEMAND) and IT solutions

Our activities :

HD Digital Cable Television

Video on Demand

Broadband Internet Connections

Interconnection

SWECOM is a FTTX provider



# OBJECTIVES

- Present advantages i gain by using Mikrotik in my network enviroment;
- How to set up firewall to manage the bandwidth;
- How to set up Queues to manage the bandwidth;
- Conclusion and questions

# ADVANTAGES OF USING MIKROTIK

- Sheap
- All in one – Many feature in the same material
- Many tools in one for troubleshooting
- Easy to manage and to access
- Mikrotik make my network administration more easier

# FIREWALL

Senario : At 9 am you are not able to browse on internet,  
What is wrong ?

- Internet is a crucial resource for enterprises of today
- The high disponibility of internet will be garanty
- To protect the router from unauthorized access, both originating from the WAN (Internet) or from the LAN (local).
- To protect the network that through the router.
- In MikroTik, firewall has many features that are all included in the IP Firewall menu.



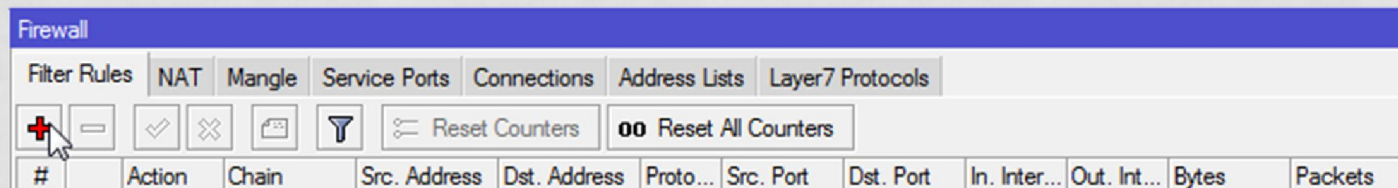
# FIREWALL : HOW TO CONFIGURE

How to configure firewall in mikrotik to protect our network ?

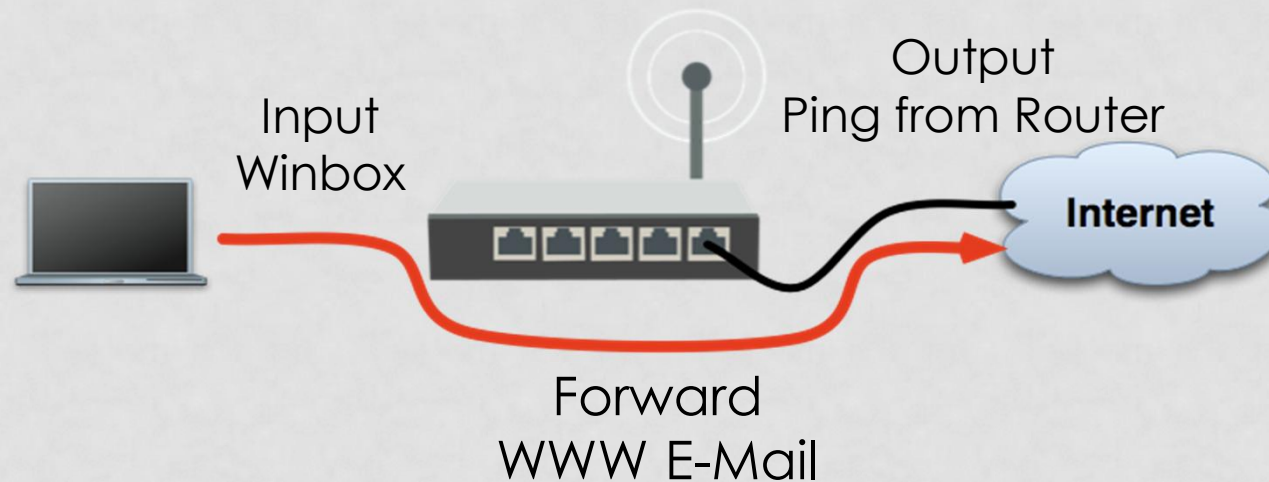
- Basic Firewall in MikroTik configure at IP>Firewall>Filter Rule



A lot of traffic to be filtered, which one allowed (accept) and which one will be rejected (drop).



# FIREWALL : HOW TO



Chain :

## **Input**

All incoming packets are checked against the rules in this chain.

## **Output**

All outgoing packets are checked against the rules in this chain.

## **Forward**

All packets being sent to another computer are checked against the rules in this chain.

To manage the bandwidth the chain **Forward** is the one used.

# FIREWALL : HOW TO

MikroTik has firewall feature to block content

- Block client who will access web which contain the word "porn", "youtube", etc.

In IP>Firewall>Filter Rule

Add chain=forward, go to advanced tab content=youtube, action=drop

The image displays three overlapping screenshots of the MikroTik WinBox 'New Firewall Rule' configuration window, illustrating the steps to create a content-filtering rule.

- Leftmost window (General tab):** Shows the 'Chain' dropdown menu set to 'forward'. Other fields like 'Src. Address', 'Dst. Address', 'Protocol', 'Src. Port', 'Dst. Port', 'Any. Port', 'In. Interface', and 'Out. Interface' are visible but empty.
- Middle window (Advanced tab):** Shows the 'Content' field with the text 'youtube' entered. Other fields like 'Src. Address List', 'Dst. Address List', 'Layer7 Protocol', 'Connection Bytes', 'Connection Rate', 'Per Connection Classifier', and 'Src. MAC Address' are visible but empty.
- Rightmost window (Action tab):** Shows the 'Action' dropdown menu set to 'drop'. The 'Log' checkbox is unchecked, and the 'Log Prefix' field is empty.

# FIREWALL : HOW TO

One great option in mikrotik firewall is to set time within that the rule will be active or not.

*/ip firewall filter*

*add action=drop chain=input disabled=no in-interface=LAN-ether2 protocol=icmp time=8h-10h30m,sun,mon,tue,wed,thu,fri,sat*

Mikrotik firewall as many other advanced feature like:

- Bloking P2P to minimize bandwidht consupction

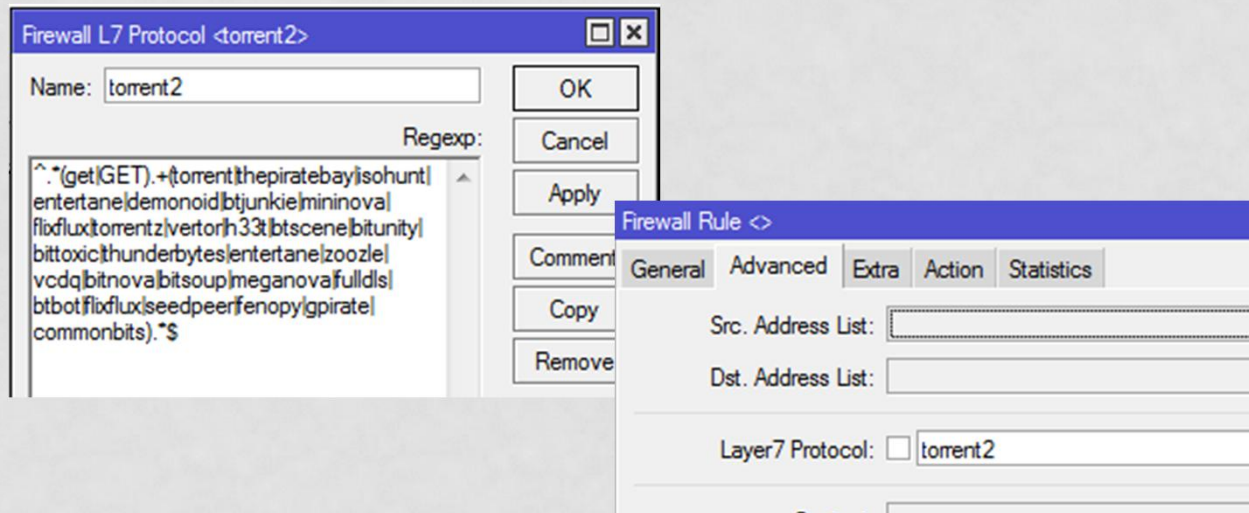
The image displays two side-by-side screenshots of the Mikrotik WinBox 'New Firewall Rule' configuration window. The left screenshot shows the 'General' tab with the following settings: Chain: forward, Src. Address: (empty), Dst. Address: (empty), Protocol: (empty), Src. Port: (empty), Dst. Port: (empty), Any. Port: (empty), and P2P:  all-p2p. The right screenshot shows the 'Action' tab with the Action: drop setting.

# FIREWALL : HOW TO

This option is not more available in new Router OS

- Layer 7 Protocol using regular expression

Exemple of blocking access to torrent site using layer 7 Protocol



We can also use firewall to save bandwidth by denying downloading based on file extension : .mp3, .exe, .avi , etc.

# FIREWALL : END

Mikrotik firewall is a powerful and flexible tool. Easy to set and to manage.

We can use firewall to manage the bandwidth usage as well as protecting our network.

One other feature we have is the queues

# QUEUES

Queues are used to limit and prioritize traffic:

- limit data rate for certain IP addresses, subnets, protocols, ports, and other parameters
- limit peer-to-peer traffic
- prioritize some packet flows over others
- configure traffic bursts for faster web browsing
- apply different limits based on time
- share available traffic among users equally, or depending on the load of the channel

# QUEUES

There are two different ways how to configure queues in RouterOS:

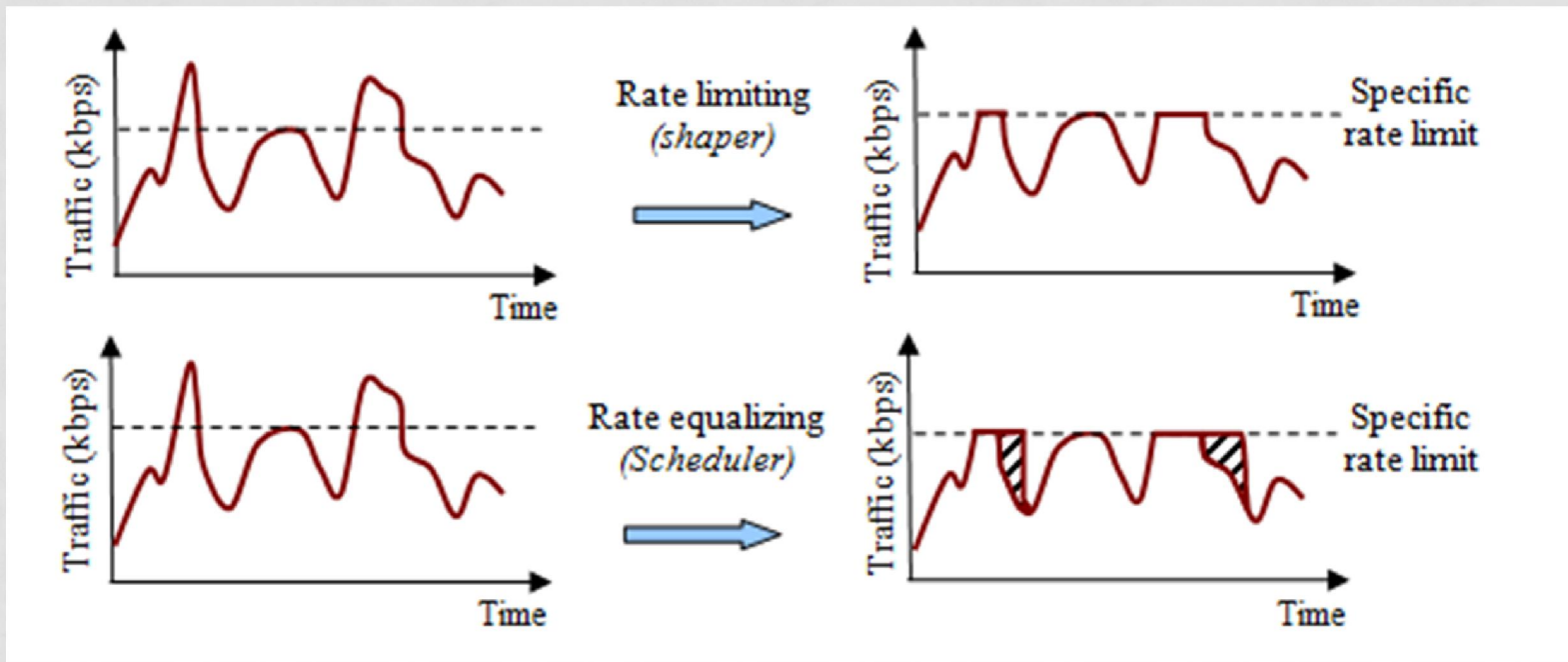
**/queue simple** menu - designed to ease configuration of simple, everyday queuing tasks (such as single client upload/download limitation, p2p traffic limitation, etc.).

**/queue tree** menu - for implementing advanced queuing tasks (such as global prioritization policy, user group limitations). Requires marked packet flows from [/ip firewall mangle](#) facility.

Rule order is important for queue rules



# QUEUES



Rate limiting is used to control the rate of traffic flow sent or received on a network interface.

The simplest way to limit data rate for specific IP addresses and/or subnets, is to use simple queues.

# QUEUES : HOW TO


















The screenshot displays the Mikrotik WinBox interface. On the left is the WinBox menu with 'Queues' highlighted. The main window shows the 'Queue List' with tabs for 'Simple Queues', 'Interface Queues', 'Queue Tree', and 'Queue Types'. A red circle highlights the '+' icon in the toolbar, with an arrow pointing to the 'New Simple Queue' dialog box.

The 'New Simple Queue' dialog box has the following fields:

- Name: GUEST
- Target: 172.16.100.0/24
- Target Upload Max Limit: 256k
- Target Download Max Limit: 256k
- Units: bits/s

Additional settings include Burst Limit (unlimited), Burst Threshold (unlimited), and Burst Time (0 s). The dialog also features buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters, and Torch.

# QUEUES : HOW TO

20				.7.251	2M	2M
21				.255.35	8M	8M
22				.4.8	60M	60M
23				.250.250	40M	40M
24				.5.160/30	10M	10M
25		BOXTV		.5.204/30	unlimited	unlimited



Tells that the user traffic is less than the limit specified



Tells that the user traffic is about to reach the limit specified



Tells that the user traffic reach or exceed the limit specified

# QUEUES : END

Simple Queue □ ×

General | Advanced | Statistics | Traffic | Total | Total Statistics

	Target Upload	Target Download
Rate:	612.5 kbps	7.5 Mbps
Packet Rate:	249 p/s	821 p/s

Legend for Top Chart:  
■ Upload: 612.5 kbps  
■ Download: 7.5 Mbps

Legend for Bottom Chart:  
■ Upload Packets: 249 p/s  
■ Download Packets: 821 p/s

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Torch

# CONCLUSION

MikroTik is genial



## Questions & Answers

