MikroTik Traffic Flow

Network Monitoring / PRTG

MikroTik User Meeting
26-January-2019
Beirut - Lebanon

Khalil Chamseddine – khalil@tahandos.com
MikroTik RouterOS is rich in many features
About me, the MikroTik Certified Trainer

• Name: Khalil Chamseddine
• Experience: Software, Hardware and Networking
• MikroTik Certified Trainer in Lebanon and Region:
  • MTCNA
  • MTCWE
  • MTCTCE
  • MTCUME
  • MTCRE
  • MTCIPv6
  • MTCINE
• Contact:
  • https://Tahandos.com
  • E-Mail: khalil@tahandos.com
  • Phone: +961-3-892792
All MikroTik Certifications – 4 weeks

- **MTCNA**
  - Network

- **MTCUME**
  - RADIUS, Hotspot

- **MTCINE**
  - BGP, MPLS, VPLs

- **MTCRE**
  - OSPF Routing

- **MTCWE**
  - Wireless

- **MTCTCE**
  - Firewall & QoS

- **MTCIPv6**
  - IP version 6

7 certifications - Flexible Schedule

Networking - Routing - Traffic Control
Firewall - Gateway - Bandwidth - VPN
Outline

• Network Monitoring and FLOW

• MikroTik Traffic Flow

• MikroTik RouterOS and PRTG
  • How To, Step By Step
  • Sample Reporting
Simple question: What do we want to know?

• Who is consuming the bandwidth?
  • From inside out
  • From outside in

• What they are consuming?

• Which protocols and services?
  • HTTP
  • Email
  • Video
  • Voice
  • Torrent
  • …
Simple question: Why do we want to know?

• Identification / Solving
  • Traffic Classification
  • Flow-based detection
  • DoS Trace back
  • ...

• Traffic Analysis
  • Inter-AS traffic analysis
  • Reporting on application proxies
  • ...

• Accounting
  • Cross verification from other sources
  • ...

January-2019
MikroTik MUM Beirut 2019 - Khalil Chamseddine - Tahandos.com
Simple question: What do we need to get?

- Nice presented reports that shows clear situation
How we are supposed to know it?

- Observation Point / Interface
- Flow Exporter: Exports Flow Records
- Flow Collector: Receives Flow Records / present them nicely

![Diagram showing network flows and components](image)
Bandwidth Monitoring Alternatives

- Bandwidth monitoring is a method for measuring the actual bandwidth available on a local system.

- **SNMP**
  - Usually it is considered lighter than other options.
  - Gets total amount of traffic and some layer 2 and layer 3 statistics like number of errors, number of broadcasts...

- Packet Sniffer
- ...
- xFlow
General Flow Definition

• A flow is defined as a set of packets having common properties:
  • one or more packet header fields (e.g. destination IP address, transport header field),
  • one or more characteristics of the packet
  • ...

• a packet belongs to a flow record if it completely matches all defined flow properties.
Flow Exporting Protocols

- CISCO NetFlow
- Juniper...
- HPE...
- IETF IPFIX

- MikroTik Traffic Flow
  - a system that provides statistic information about packets which pass through the router.
  - network monitoring and accounting
  - identify various problems that may occur in the network
  - analyze, optimize the overall network performance
  - MikroTik Traffic-Flow is compatible with Cisco NetFlow, it can be used with various utilities which are designed for Cisco's NetFlow.
NetFlow Flow definition

- NetFlow defines a flow as the combination of the following seven key-fields:
  - Source IP address.
  - Destination IP address.
  - Source port number.
  - Destination port number.
  - Layer 3 protocol type.
  - ToS byte
  - Logical interface, whether input (ingress) or output (egress)
Flow formats

• Differ in the format of the export massage
• Version 1 - never use it 😊

• Version 5 – limited to inbound traffic (ingress) and IPv4.

• Version 9 - a new format which can be extended with new fields and record types because of its template-style design
  • Version 9 is independent of the underlying transport protocol whether it is TCP, UDP, or SCTP
  • Support for IPv6 and bi-directional flows (ingress and egress)
  • Support for MPLS/VLAN...
IPFIX: IP Flow Information Export

- IETF: Internet Engineering Task Force

- IPFIX: Official Standard for all flow technologies
  - Sometimes described as NetFlow Version 10
  - used CISCO NetFlow version 9 as a base
  - common, universal standard of export for Internet Protocol flow information from routers, probes and other devices that are used by mediation systems, accounting/billing systems and network management systems to facilitate services such as measurement, accounting and billing
  - defines how IP flow information is to be formatted and transferred from an exporter to a collector

- IPFIX is a push protocol, i.e. each sender will periodically send IPFIX messages to configured receivers without any interaction by the receiver.
MikroTik IPFIX

• MikroTik Traffic Flow template
How To

• Configure the Exporter (MikroTik)

• Configure the Flow Record (MikroTik)

• Apply it to the Interface (MikroTik)

• Configure the Flow Monitor (PRTG)
How we are supposed to know it?

- Observation Point / Interface
- Flow Exporter: MikroTik RouterBoard
- Flow Collector: PRTG
PRTG, the collector

• PRTG Network Monitor
  • PRTG: Paessler Router Traffic Grapher
  • Agentless network monitoring software
  • German Company: Paessler AG
  • First release: 2003

• PRTG is a full-service monitoring solution
  • It can monitor and classify system conditions like bandwidth usage or uptime and collect statistics from miscellaneous hosts as switches, routers, servers and other devices and applications
PRTG, the collector

• Sensors
  • over 200 different predefined sensors
  • application sensors and hardware-specific sensors

• Web Interface and Desktop Client
  • AJAX-based web interface
  • desktop application for Windows and macOS (beta status)

• Notifications and Reports
  • Email and SMS
  • push notification on smartphones using an app
  • customizable reports

• Pricing
  • based on sensors
  • 100 integrated sensors is available free of charge
  • Usually, each MikroTik Traffic-Flow device represents one sensor
PRTG, IPFIX Sensor

- The IPFIX sensor receives traffic data from MikroTik Traffic-Flow and shows traffic by type. It filters traffic into different channels:
  - Chat (IRC, AIM)
  - Citrix
  - FTP/P2P (file transfer)
  - Infrastructure (network services: DHCP, DNS, IDENT, ICMP, SNMP)
  - Mail (mail traffic: IMAP, POP3, SMTP)
  - NetBIOS
  - Remote control (RDP, SSH, Telnet, VNC)
  - WWW (web traffic: HTTP, HTTPS)
  - Total traffic
  - Other protocols (other UDP and TCP traffic)
PRTG Download and Install

• Go to https://www.paessler.com/

• Download PRTG (prtg.zip) and extract it; save the License name and key in a text file for later use

• Run the executable install. Steps are easy to follow.
  • Enter an email address to receive alerts

• When installation is complete
  • Login, Watch the video that pops up, change the password, set the SSL; it is yours to discover.. A lot of helping pop ups.. Read and follow..
PRTG First things first

- PRTG auto discovery will attempt to discover your network and create a sensor for each probe it discovers
- Wait till auto-discovery finishes. Review the discovered devices and the created sensors. You will see a lot of sensors: ping, DNS, HTTP, SSL ....
  - Better to stop auto-discovery: Automatic auto-discovery is set on group or device level. You can change it in your group's or device's settings, section Group Type or Device Type, setting Sensor Management.
- Delete all the sensors discovered automatically because PRTG is free for the first 100 sensors only
  - You can disable the initial auto-discovery in a fresh PRTG installation. Simply run the installer in command prompt and add /NoInitialAutoDisco=1 as parameter
How To

• Configure the Exporter (MikroTik)

• Configure the Flow Record (MikroTik)

• Apply it to the Interface (MikroTik)

• Configure the Flow Monitor (PRTG)
Exporter: MikroTik
Collector: PRTG

Observation Points: MikroTik Interfaces
MikroTik Traffic Flow Configuration

Traffic Flow Settings
- General
  - Enabled
  - Interfaces: bridgeWiFi
  - Cache Entries: 16k
  - Active Flow Timeout: 00:30:00
  - Inactive Flow Timeout: 00:00:15

Traffic Flow Targets
- Targets
  - Src. Address: 0.0.0.0
  - Dst. Address: 10.111.222.44
  - Port: 1234
  - Version: IPFIX

Traffic Flow Target <10.111.222.44>
- Src. Address: 0.0.0.0
- Dst. Address: 10.111.222.44
- Port: 1234

- Version: IPFIX
  - v9/IPFIX Template Refresh: 20
  - v9/IPFIX Template Timeout: 1800

Enabled
MikroTik Traffic Flow Configuration

• /ip traffic-flow set
  • #Settings for the exporter
  • interfaces=bridgeWiFi
    • #interfaces which will be used to gather statistics for traffic-flow
  • cache-entries=2k
    • #flows which can be in router's memory simultaneously
  • active-flow-timeout=30m
    • #maximum life-time of a flow
  • inactive-flow-timeout=15s
    • #how long to keep the flow active
  • enabled=yes

• /ip traffic-flow target
  • #Settings for the collector
  • add disabled=no
  • dst-address=10.111.222.44
  • port=1234
  • src-address=0.0.0.0
  • v9-template-refresh=20
  • v9-template-timeout=30m
  • version=ipfix
PRTG: Configure the Flow Monitor

• Select Add sensor

• Create a new device if necessary or use existing device
  • Usually the MikroTik RouterBoard is already discovered under network infrastructure

• Select Sensor type IPFIX

• Set the sensor settings. Most important:
  • Sensor Name
  • UDP Port
  • Active Flow Timeout
Add a sensor

Add Sensor to Device hAP Mikrotik Traffic Flow [10.111.222.33]

Monitor What?
- Availability/Upptime
- CPU Usage
- Hardware Parameters
- Bandwidth/Traffic
- Disk Usage
- Network Infrastructure
- Speed/Performance
- Memory Usage
- Custom Sensors

< Cancel sensor creation

Search ipf

Matching Sensor Types

IPFIX
Monitors a switch using IPFIX

IPFIX (Custom)
Monitors a switch using IPFIX (customizable)

Basic Sensor Settings
- Sensor Name: IPFIX
- Tags: bandwidthsensor, netflowsensor
- Priority: ★★★☆☆

IPFIX Specific Settings
- Receive IPFIX Packets on UDP Port
  - Sender IP
  - Receive IPFIX Packets on IP
  - Active Flow Timeout (Minutes)
  - Sampling Mode
  - Log Stream Data to Disk for Debugging

This field is required.
Configure the Flow Monitor (PRTG)

```
Edit Object IPFIX

Basic Sensor Settings
- Sensor Name: IPFIX
- Parent Tags:
  - bandwidthsensor
  - netflowsensor
- Tags:
- Priority

IPFIX Specific Settings
- Receive IPFIX Packets on UDP Port: 1234
- Sender IP: 10.111.222.33
- Receive IPFIX Packets on IP:
  - Probe's Local IPs: 10.0.2.15
- Active Flow Timeout (Minutes): 30

Sampling Mode
- Off
- On

Log Stream Data to Disk (for Debugging)
- None (recommended)
- Only for the 'Other' channel
- All stream data

Channel Configuration

Group | Content
--- | ---
Web | WWW Traffic: HTTP, HTTPS
File Transfer | File Transfer: FTP (Control)
Mail | Mail Traffic: IMAP, POP3, SMTP
Chat | Chat, Instant Messaging: IRC, AIM
Remote Control | Remote Control: RDP, SSH, Telnet, VNC
Infrastructure | Network Services: DHCP, DNS, Idemp, ICMP, SNMP
NetBIOS | NetBIOS: NetBIOS
Citrix | Citrix
Other Protocols | Various: OtherUDP, OtherTCP
```
Sensor Overview

Sensor IPFIX

Overview

Top Talkers

Top Connections

Top Protocols

Add Toplist

Total

FTP/P2P
Infrastructure
Mail
Other

Remote Control
Various
WWW

0 kbit/s
9.23 kbit/s
0 kbit/s

32 kbit/s
0
65 kbit/s

Channel

ID

Last Value (volume)

Last Value (speed)

Minimum

Maximum

Downtime
-1
34 KByte
4.63 kbit/s
0 kbit/s
9.30 kbit/s

FTP/P2P
3002
34 KByte
4.63 kbit/s
0 kbit/s
9.30 kbit/s

Infrastructure
3007
34 KByte
4.63 kbit/s
0 kbit/s
9.31 kbit/s

Mail
3003
102 KByte
14 kbit/s
0 kbit/s
28 kbit/s

Other
0
0 KByte
0 kbit/s

Remote Control
3005
0 KByte
0 kbit/s

January-2019

MikroTik MUM Beirut 2019 - Khalil Chamseddine - Tahandos.com
PRTG: Add Top lists

• PRTG comes with primary top lists
  • Top Talkers
  • Top Connections
  • Top Protocols
  • Custom Toplist
Sensor Overview
Sensor Channels

![Sensor Channels](image.png)

### Channel ID Last Value (volume) Last Value (speed) Minimum Maximum

- **Downtime**
  - 4
  - 0 KByte
  - 0 kbit/s
  - 0 kbit/s
  - < 0.01 kbit/s

- **FTP/P2P**
  - 3002
  - 0 KByte
  - 0 kbit/s
  - 0 kbit/s
  - < 0.01 kbit/s

- **Infrastructure**
  - 3007
  - 1.79 KByte
  - 0.25 kbit/s
  - < 0.01 kbit/s
  - 1.68 kbit/s

- **Mail**
  - 3003
  - 0.05 KByte
  - < 0.01 kbit/s
  - 0 kbit/s
  - 0.03 kbit/s

- **NetBIOS**
  - 3008
  - 0.04 KByte
  - < 0.01 kbit/s
  - < 0.01 kbit/s
  - < 0.01 kbit/s

- **Other**
  - 0
  - 0 KByte
  - 0 kbit/s
  - 0 kbit/s
  - 0.02 kbit/s

- **Remote Control**
  - 3005
  - 0 KByte
  - 0 kbit/s
  - 0 kbit/s
  - < 0.01 kbit/s

- **Total**
  - -1
  - 32 KByte
  - 4.34 kbit/s
  - 0 kbit/s
  - 31 kbit/s

- **Various**
  - 3009
  - 0.88 KByte
  - 0.12 kbit/s
  - < 0.01 kbit/s
  - 20 kbit/s

- **WWW**
  - 3001
  - 29 KByte
  - 3.96 kbit/s
  - < 0.01 kbit/s
  - 9.97 kbit/s
Sensor Live Data

1/25/2019 8:15:00 AM - 8:30:00 AM (Live Toplist, 98 % Complete)
Sensor Live Data Detailed list

<table>
<thead>
<tr>
<th>Pos</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Bytes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>[5.79.72.143]</td>
<td>[192.168.1.64]</td>
<td>527 MByte</td>
<td>81%</td>
</tr>
<tr>
<td>2.</td>
<td>[95.211.90.131]</td>
<td>[192.168.1.64]</td>
<td>99 MByte</td>
<td>15%</td>
</tr>
<tr>
<td>3.</td>
<td>x220 (192.168.250.184)</td>
<td>[5.79.72.143]</td>
<td>8,483 KByte</td>
<td>1%</td>
</tr>
<tr>
<td>4.</td>
<td>mrs08602-in-f141e100...</td>
<td>[192.168.1.64]</td>
<td>5,119 KByte</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>5.</td>
<td>a104-121-22-218.deploy...</td>
<td>[192.168.1.64]</td>
<td>2,834 KByte</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>6.</td>
<td>any-in-2678.1e100.net (...</td>
<td>[192.168.1.64]</td>
<td>2,205 KByte</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>7.</td>
<td>[159.148.147.206]</td>
<td>[192.168.1.64]</td>
<td>1,975 KByte</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>8.</td>
<td>[159.148.172.231]</td>
<td>[192.168.1.64]</td>
<td>1,776 KByte</td>
<td>&lt; 1%</td>
</tr>
</tbody>
</table>
Top Connections 1/25/2019 8:30:00 AM - 8:45:00 AM (Live Toplist, 15% Complete)
Top Connections Detailed List

<table>
<thead>
<tr>
<th>Pos</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>p3plprx03-v...</td>
<td>995</td>
<td>[192.168.1...</td>
<td>50036</td>
<td>TCP</td>
<td>21 KByte</td>
</tr>
<tr>
<td>2.</td>
<td>mrs08s03-l...</td>
<td>443</td>
<td>[192.168.1...</td>
<td>50037</td>
<td>TCP</td>
<td>3,689 Byte</td>
</tr>
<tr>
<td>3.</td>
<td>any-in-2578...</td>
<td>443</td>
<td>[192.168.1...</td>
<td>50045</td>
<td>TCP</td>
<td>3,555 Byte</td>
</tr>
<tr>
<td>4.</td>
<td>X220 (192...</td>
<td>50045</td>
<td>any-in-2578...</td>
<td>443</td>
<td>TCP</td>
<td>2,511 Byte</td>
</tr>
<tr>
<td>5.</td>
<td>X220 (192...</td>
<td>50037</td>
<td>mrs08s03-l...</td>
<td>443</td>
<td>TCP</td>
<td>2,213 Byte</td>
</tr>
<tr>
<td>6.</td>
<td>X220 (192...</td>
<td>50044</td>
<td>ef-in-1136.1...</td>
<td>443</td>
<td>TCP</td>
<td>2,173 Byte</td>
</tr>
<tr>
<td>7.</td>
<td>X220 (192...</td>
<td>50038</td>
<td>p3plprx03-v...</td>
<td>995</td>
<td>TCP</td>
<td>1,818 Byte</td>
</tr>
<tr>
<td>8.</td>
<td>X220 (192...</td>
<td>137</td>
<td>[192.168.2...</td>
<td>137</td>
<td>UDP</td>
<td>1,638 Byte</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1,197 Byte</td>
</tr>
</tbody>
</table>
Top Protocols 1/25/2019 8:30:00 AM - 8:45:00 AM (Live Toplist, 24 % Complete)
### Top Protocols details

<table>
<thead>
<tr>
<th>Pos</th>
<th>Channel</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Mail</td>
<td>25 KByte</td>
</tr>
<tr>
<td>2.</td>
<td>WWW</td>
<td>24 KByte</td>
</tr>
<tr>
<td>3.</td>
<td>Various</td>
<td>11 KByte</td>
</tr>
<tr>
<td>4.</td>
<td>Infrastructure</td>
<td>6,630 Byte</td>
</tr>
<tr>
<td>5.</td>
<td>NetBIOS</td>
<td>2,106 Byte</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>0 Byte</td>
</tr>
</tbody>
</table>
Thank you 😊

Questions?