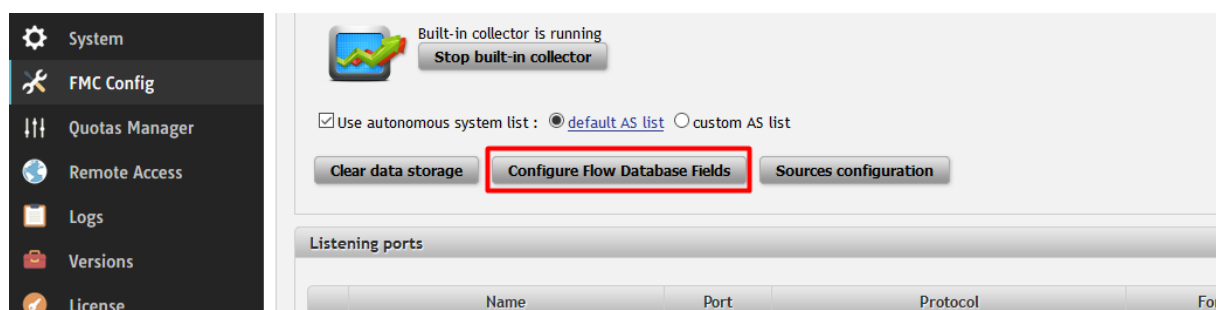


## Preparing of Data retention output with Mikrotik NAT information

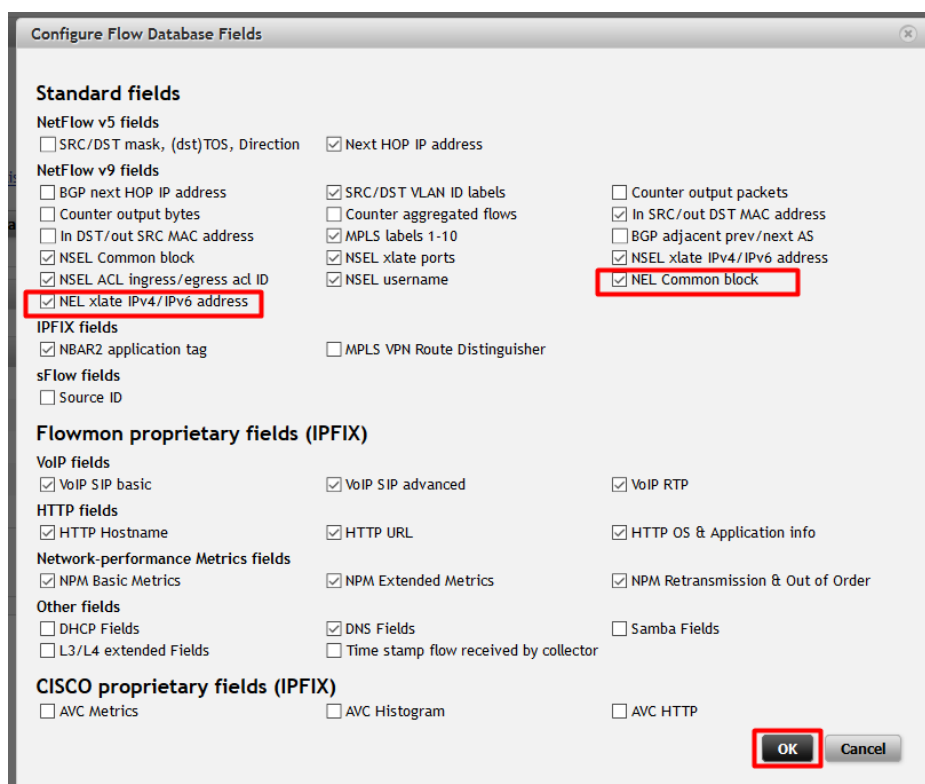
Mikrotik RouterOS version 6.29 and higher affects the NAT correlation in Flowmon Data Retention Module. This document provides step-by-step instructions for RouterOS 6.29 and higher to enable NEL extensions for correct NAT correlation and subsequent analysis.

### Enable collecting of NAT information

1. Open Configuration Center on your collector
2. Go to FMC Config -> Configure Flow Database Fields page

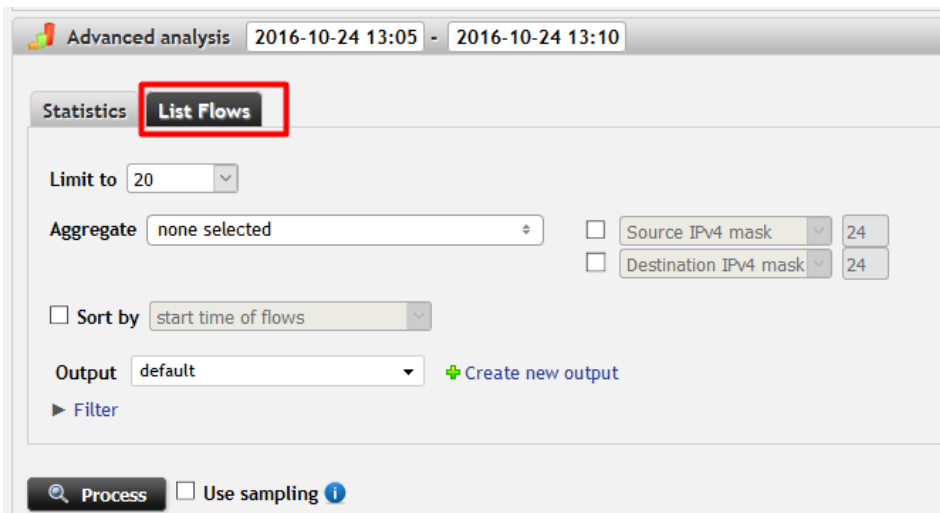


3. Select NEL Common block and NEL xlate IPv4/IPv6 address and save settings



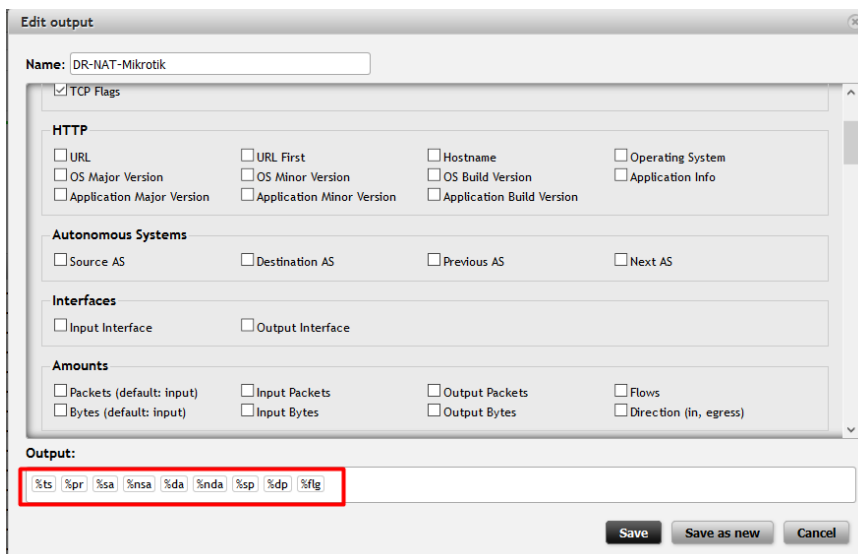
### Prepare list of flow DR-NAT-Mikrotik output

1. Open Flowmon Monitoring Center
2. Switch to Analysis page
3. Select List Flows in Advanced analysis section



4. Create new output
  - a. Name: DR-NAT-Mikrotik
  - b. Select fields in section **Date and time**: Start Time – first seen,
  - c. Select fields in section **IP**: Protocol, Source IP Address, Source port, Destination IP address, Destination port, TCP flags
  - d. Select fields in section **NEL**: NAT src IP address, NAT dst IP address
  - e. Make Output fields order using drag and drop:

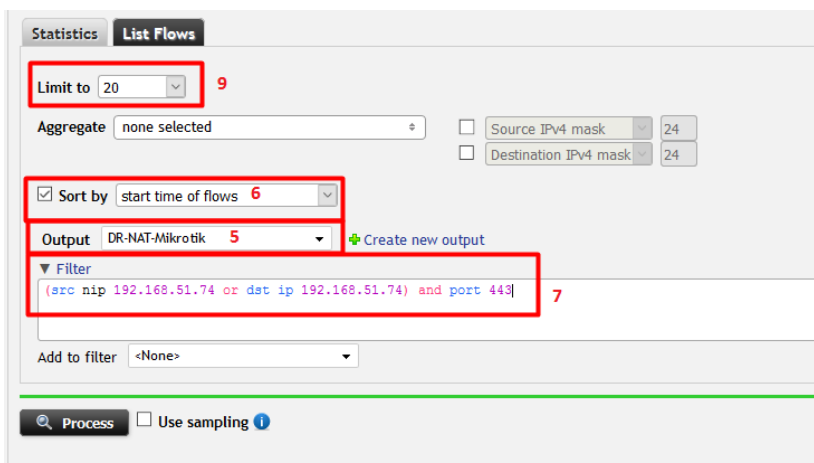
**%ts %pr %sa %nsa %da %nda %sp %dp %flg**



- f. Click Save

## Analysis of DR Request

1. Open Flowmon Monitoring Center
2. Select Analysis in menu
3. Select All Sources profile
4. Select timeslot in graph based on your request
5. In Advanced analysis select Output: DR-NAT-Mikrotik
6. Select Sort by start time of flows
7. In filter use rule with requested NAT IP address <NAT\_IP> and port as optional parameter  
(src nip <NAT\_IP> or dst ip <NAT\_IP>) and port <Port>
8. This filter can be extended with other search criteria
9. To confirm traffic visibility use Limit to: 100 lines
10. To export data into file use Limit to: unlimited – result has to be downloaded from Previous menu in csv format
11. Click Process



## Result Example

Result shows communication of NAT IP 192.168.51.74. Segment is 192.168.88.0/24. We can see local IP 192.168.88.253 over NAT IP with IP addresses in internet. Client private IP is in position Source IP for outgoing traffic and on Dst Nat IP for incoming traffic.

Start Time - first seen	IP Protocol	Source IP address	Src NAT IP	Destination IP address	Dst NAT IP	Source Port	Destination Port	TCP Flags
2016-10-10 12:41:48.260	TCP	74.125.133.189	74.125.133.189	192.168.51.74	192.168.88.253	443	61522	...AP...
2016-10-10 12:41:48.310	TCP	192.168.88.253	192.168.51.74	74.125.133.189	74.125.133.189	61522	443	...A....
2016-10-10 12:43:55.000	TCP	172.217.18.65	172.217.18.65	192.168.51.74	192.168.88.253	443	61711	...A....
2016-10-10 12:43:55.000	TCP	192.168.88.253	192.168.51.74	172.217.18.65	172.217.18.65	61712	443	...A....
2016-10-10 12:43:55.000	TCP	192.168.88.253	192.168.51.74	172.217.18.65	172.217.18.65	61711	443	...A....
2016-10-10 12:43:55.000	TCP	172.217.18.65	172.217.18.65	192.168.51.74	192.168.88.253	443	61712	...A....
2016-10-10 12:44:01.000	TCP	172.217.18.65	172.217.18.65	192.168.51.74	192.168.88.253	443	61714	...A....