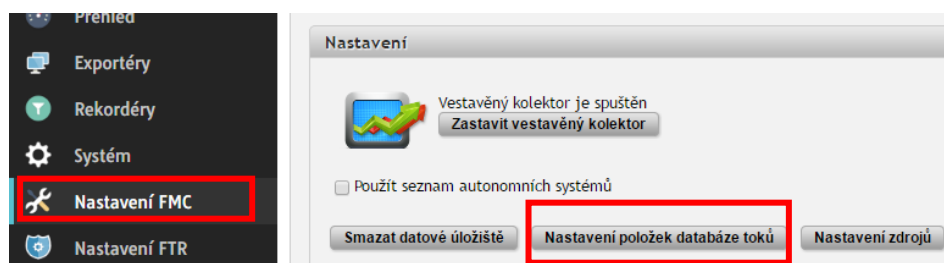


Příprava výstupu Flowmon Data Retention pro Mikrotik NAT

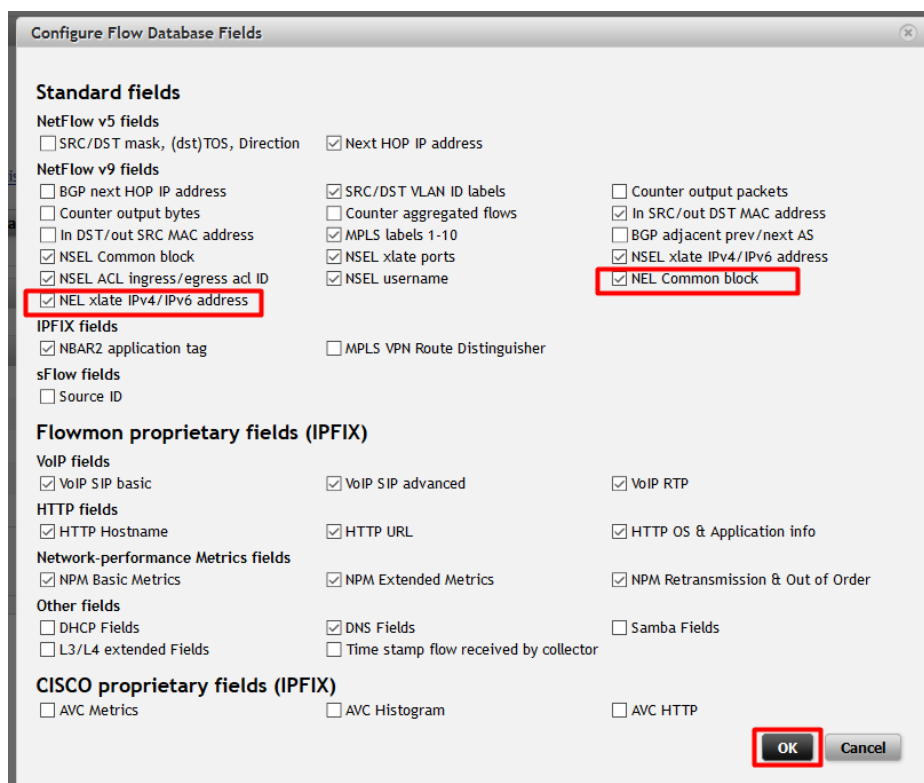
Mikrotik RouterOS verze 6.29 a vyšší ovlivňuje korelaci NAT v modulu Flowmon Data Retention. Tento dokument podrobně popisuje, jak pro RouterOS 6.29 vyšší zapnout NEL rozšiřující položky pro správnou NAT korelaci a následnou analýzu.

Nastavení sbírání NAT informací

1. Otevřete Configuration Center na svém kolektoru
2. Přejděte do Nastavení FMC -> Nastavení položek databáze toků

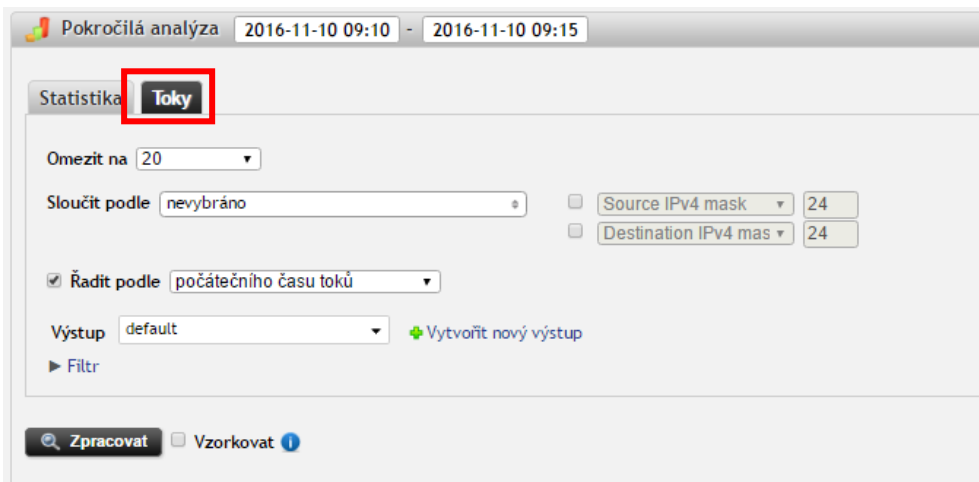


3. Zaškrtněte NEL Common block a NEL xlate IPv4/IPv6 address a uložte nastavení kliknutím na OK



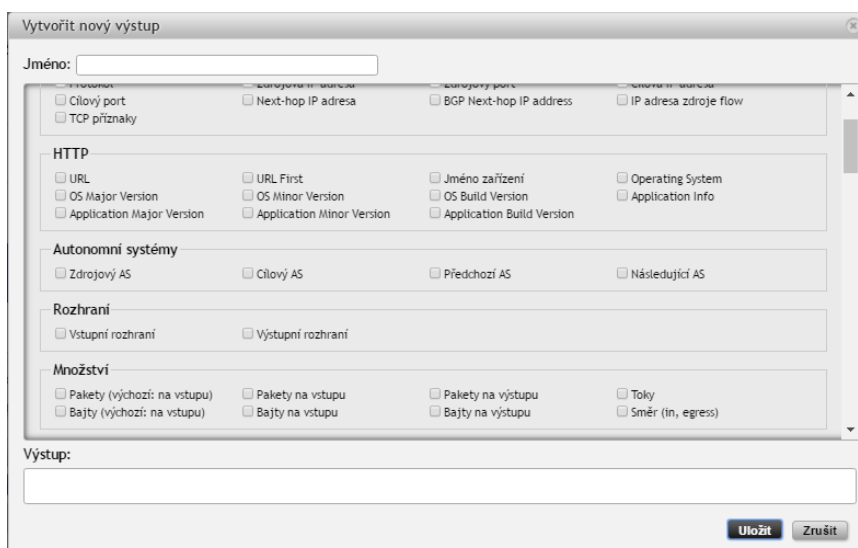
Příprava seznamu toků DR-NAT-Mikrotik

1. Otevřete Flowmon Monitoring Center
2. Přejděte na stránku Analýza
3. Vyberte záložku Toky v sekci Pokročilá analýza Advanced analysis section



4. Vytvořte nový výstup
 - a. Jméno: DR-NAT-Mikrotik
 - b. Vyberte položky v sekci **Datum a čas**: Počáteční čas,
 - c. Vyberte položky v sekci **IP**: Protokol, Zdrojová IP adresa, Zdrojový port, Cílová IP adresa, Cílový port, TCP příznaky
 - d. Vyberte položky v sekci **NEL**: NAT zdrojová IP adresa, NAT cílová IP adresa
 - e. Vytvořte výstup: pořadí polí upravte pomocí drag&drop na:

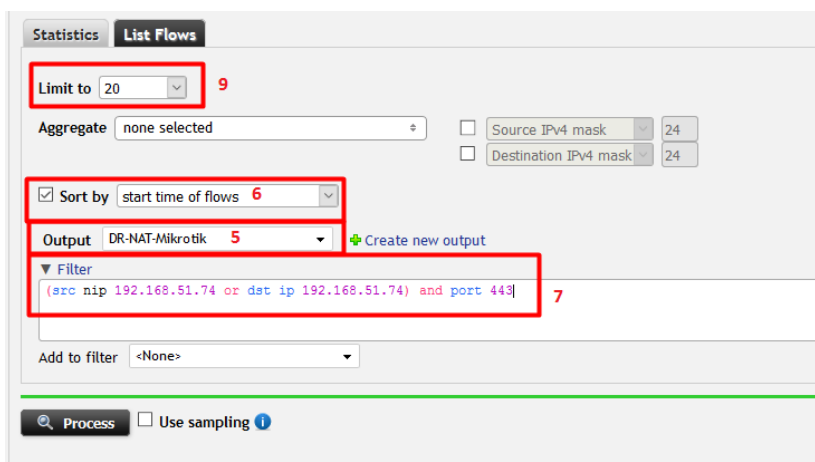
%ts %pr %sa %nsa %da %nda %sp %dp %flg



f. Klikněte na uložit

Analýza DR požadavku

1. Otevřete Flowmon Monitoring Center
2. Vyberte „Analýza“ v menu
3. Zvolte profil All Sources
4. Zvolte časový interval v grafu dle vašeho požadavku
5. V sekci Pokročilá analýza vyberte výstup: DR-NAT-Mikrotik
6. Vyberte Seřadit dle Počátečního času toků
7. Ve filtru použijte pravidlo s požadovanou NAT IP adresou <NAT_IP> and portem jako volitelným parametrem
(src nip <NAT_IP> or dst ip <NAT_IP>) and port <Port>
8. Tento filtr můžete dále rozšířit dalšími vyhledávacími parametry.
9. Pro potvrzení viditelnosti použijte Omezit na: 100 toků
10. Pro export dat do souboru použijte Omezit na: – výsledky jsou ke stažení v csv formátu v roletce *Předchozí výsledky*
11. Klikněte na Zpracovat



Příklad výstupu

Příklad ukazuje komunikaci NAT IP 192.168.51.74. Segment je 192.168.88.0/24. Můžeme vidět lokální IP 192.168.88.253 přes NAT IP s veřejnou IP. Privátní IP je uváděná jako Zdrojová IP pro odchozí provoz a Cílová NAT IP pro příchozí provoz.

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....