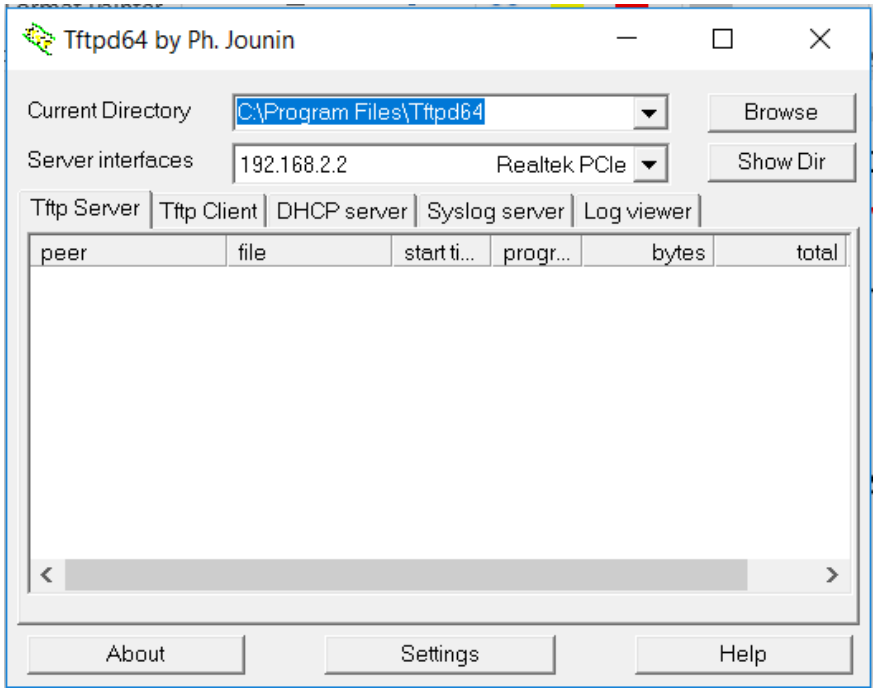
ISHOD 4 – NADZOR MREŽE + BACKUP

Nadzor mreže nam je ključan u produkciji kako bi bili svjesni svega što se događa u našoj mreži, od ispada linka ili nekog servisa, do nadzora prometa, brzine,...te naravno sve moramo imati backupirano....za ove potrebe koristit ćemo dva alata....pa krenimo:

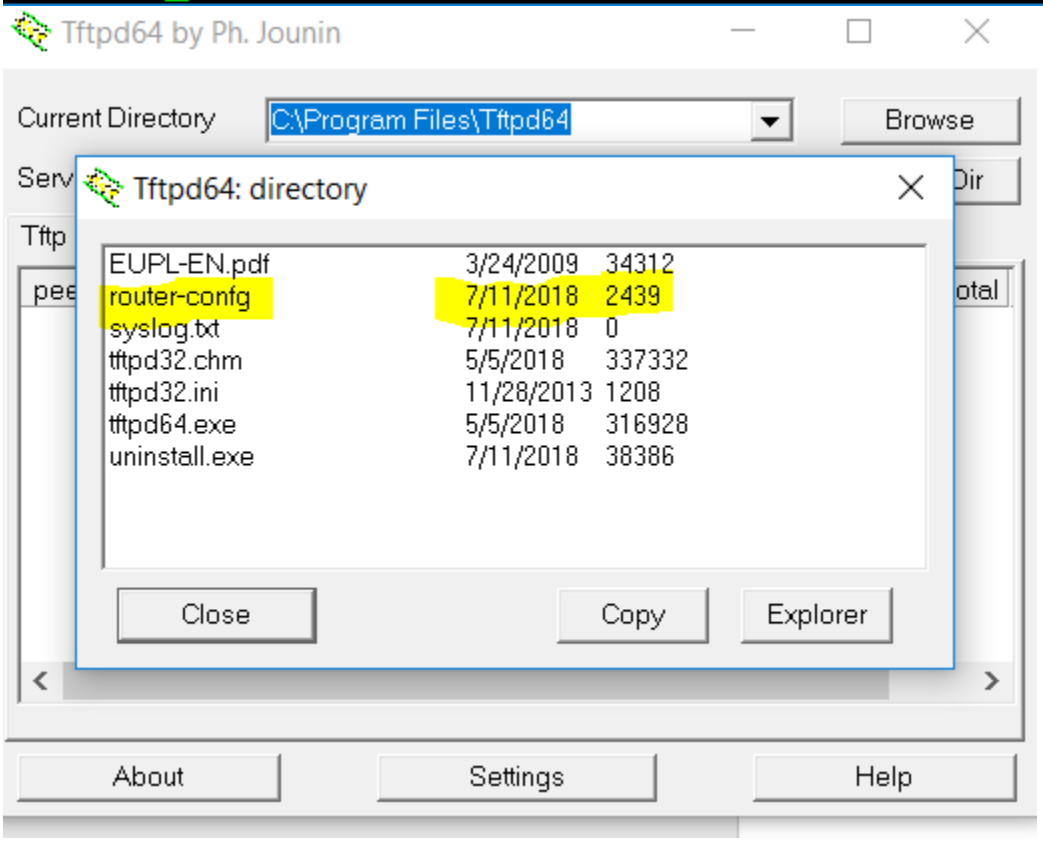
1. BACKUP + SYSLOG

   Za ove potrebe koristit ćemo alat TFTPd64 (na ispitu će vas čekati instaliran)



Na routeru izvšimo par jednostavnih komandi da bi prebacili npr. Konfu iz NVRAM-a na tftp server koji je na našem Pcu:

```
Router#copy startup-config tftp:
Address or name of remote host []? 192.168.2.2
Destination filename [router-confg]?
!!
2439 bytes copied in 0.060 secs (40650 bytes/sec)
Router#
```



SYSLOG TRAP-ovi:

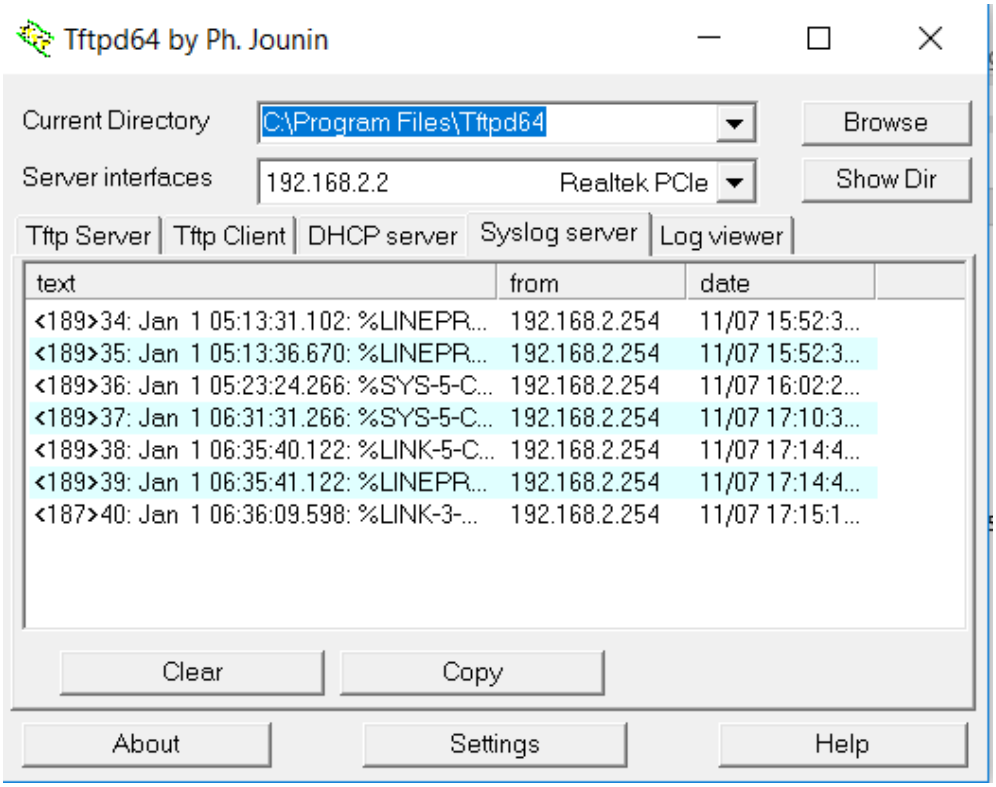
Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Jednostavno ih konfiguriramo:

```
Router(config)#logging host 192.168.2.2
Router(config)#logg
Router(config)#logging tr
Router(config)#logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>

Router(config)#logging trap
```

Kada podesimo host (adresu našeg PC-a na kojem je server) i odaberemo severity level, možemo u syslog serveru vidjeti prve logove, npr. Ugasimo/uplaimo interfejs i vidmo te događaje:



2. NADZOR MREŽE I PROMETA PRTG ALAT

Za nadzor mrežnih uređaja i prometa (netflow) koristit ćemo besplatan i moćan alat PRTG koji je jako jednostavan za korištenje i daje nam uvid u našu mrežu, gdje možemo raditi fine tuning po svakom uređaju i interfejsu te dodavati brojne senzore koji nam pomažu u nadzoru....pa krenimo...

2.1. Nadzor WAN i LAN interfejsa na routeru

Postavit ćemo senzore za wan i lan interfejse koji će nam raditi stalni ping kako bi nam nadzirali dostupnost interfejsa i dodatno ćemo postaviti limite kako bi nam javljao poruke ukoliko je promet premali (npr. to nam ukazuje da nešto nije uredu s klijentima ili serverima u lan mreži jer ne proizvode promet) ili prevelik (npr. dolazi do zagušenja, netko generira prevelik promet).

Za potrebe nadzora koristimo SNMP protokol s kojim naš nadzorni alat PRTG (on je server) prikuplja podatke od klijenta (to je naš router).

Na routeru trebamo podesiti nekoliko bitinih stvari za SNMP:

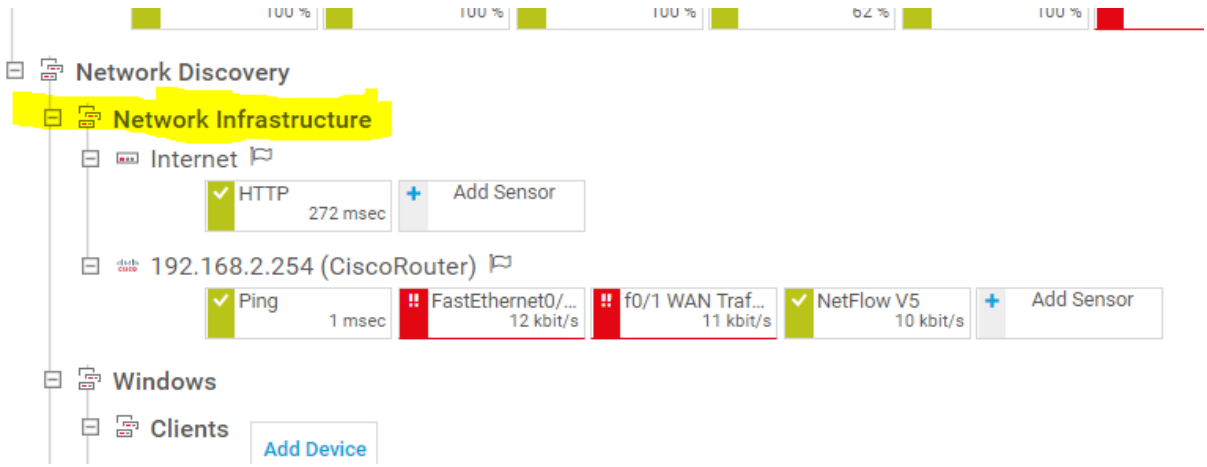
SNMP:

```
R1(config)#snmp-server community prtgRO RO
R1(config)# snmp-server community prtgRW RW
R1(config)# snmp-server trap-source FastEthernet0/0
R1(config)#snmp-server enable traps
R1(config)# snmp-server host 192.168.1.10 version 2c prtgRO
```

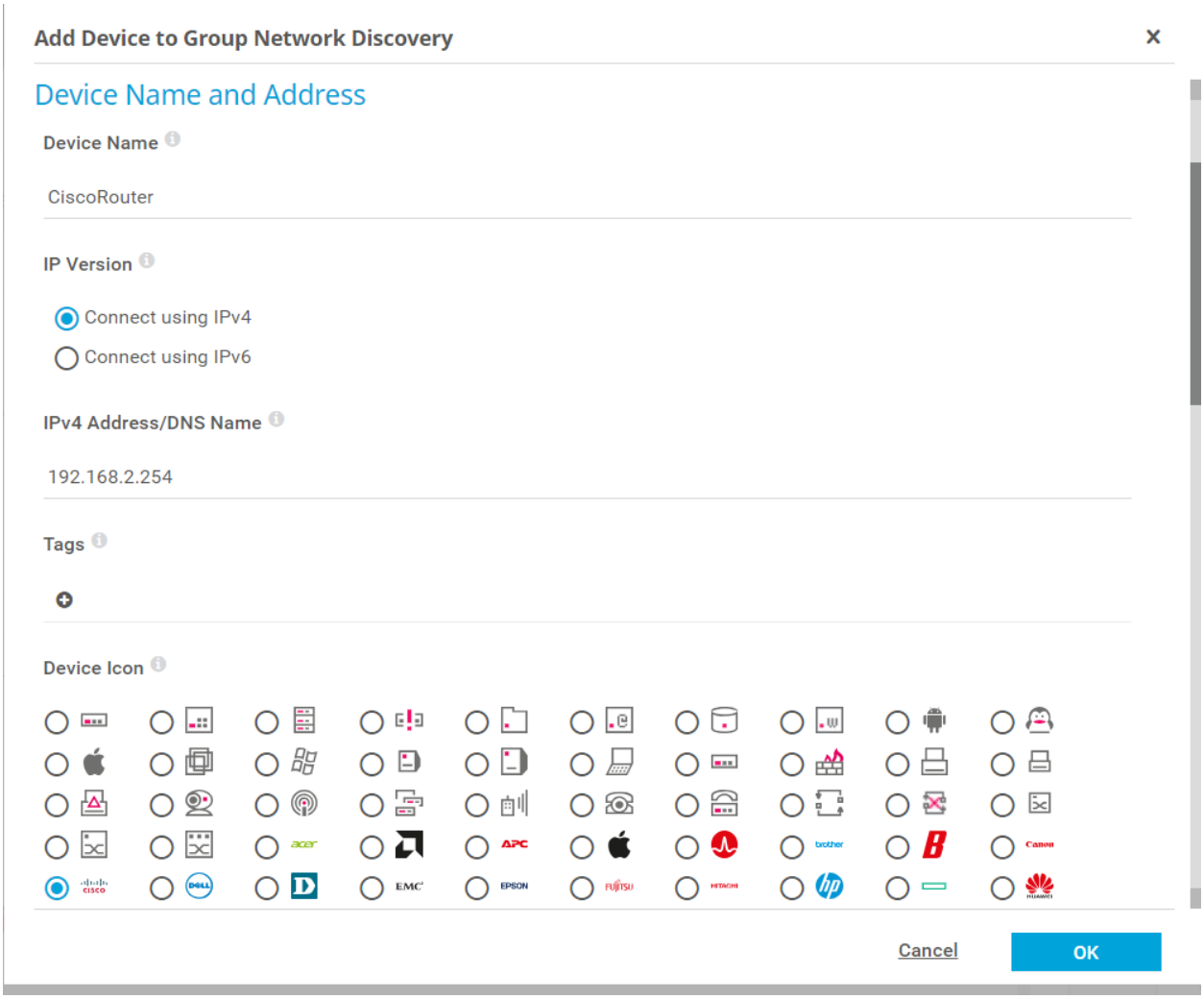
Moramo postaviti community (to je naziv grupe npr prtgRO), RO znači read only, RW read write, podesimo source interface, enablamo trap-ove (trapovi su informacije koje će server tražiti od klijenta, kada upišemo enable otvaramo praktički sve) i na kraju podesimo ip adresu našeg PC-a i verziju zajedno s communityem jer ćemo te iste podatke podesiti na serveru.

A sad krenimo na server....

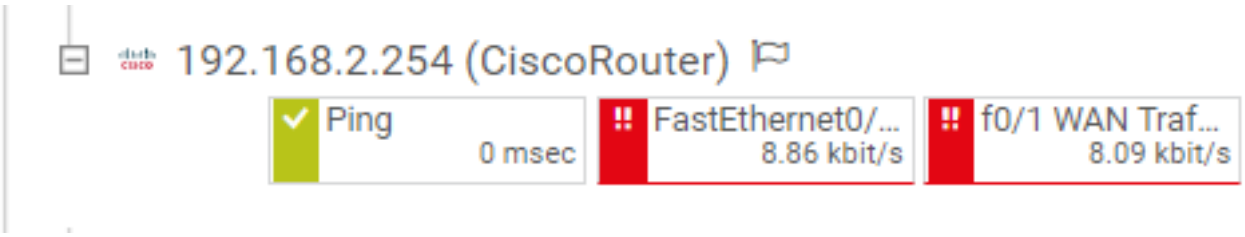
Desni klik na Network Infrastructure i odaberemo add device



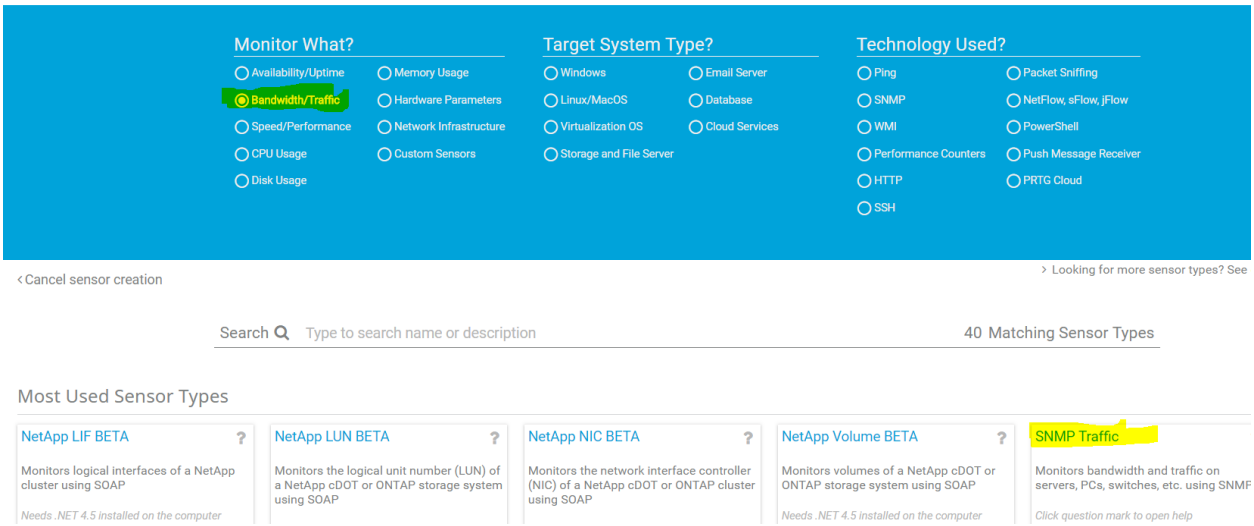
Zatim podesimo naziv i ip adresu našeg rutera kako bi ga dodali u nadzor...



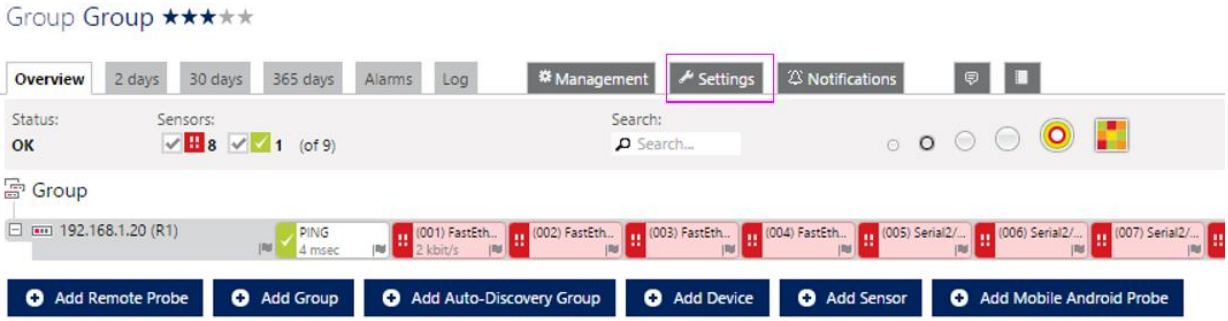
Kad smo dodali router u nadzor možemo dodati senzore za WAN i LAN interfejse kako bi nadzirali promet i kako bi dobivali poruke ukoliko se probiju limiti koje nadziremo!

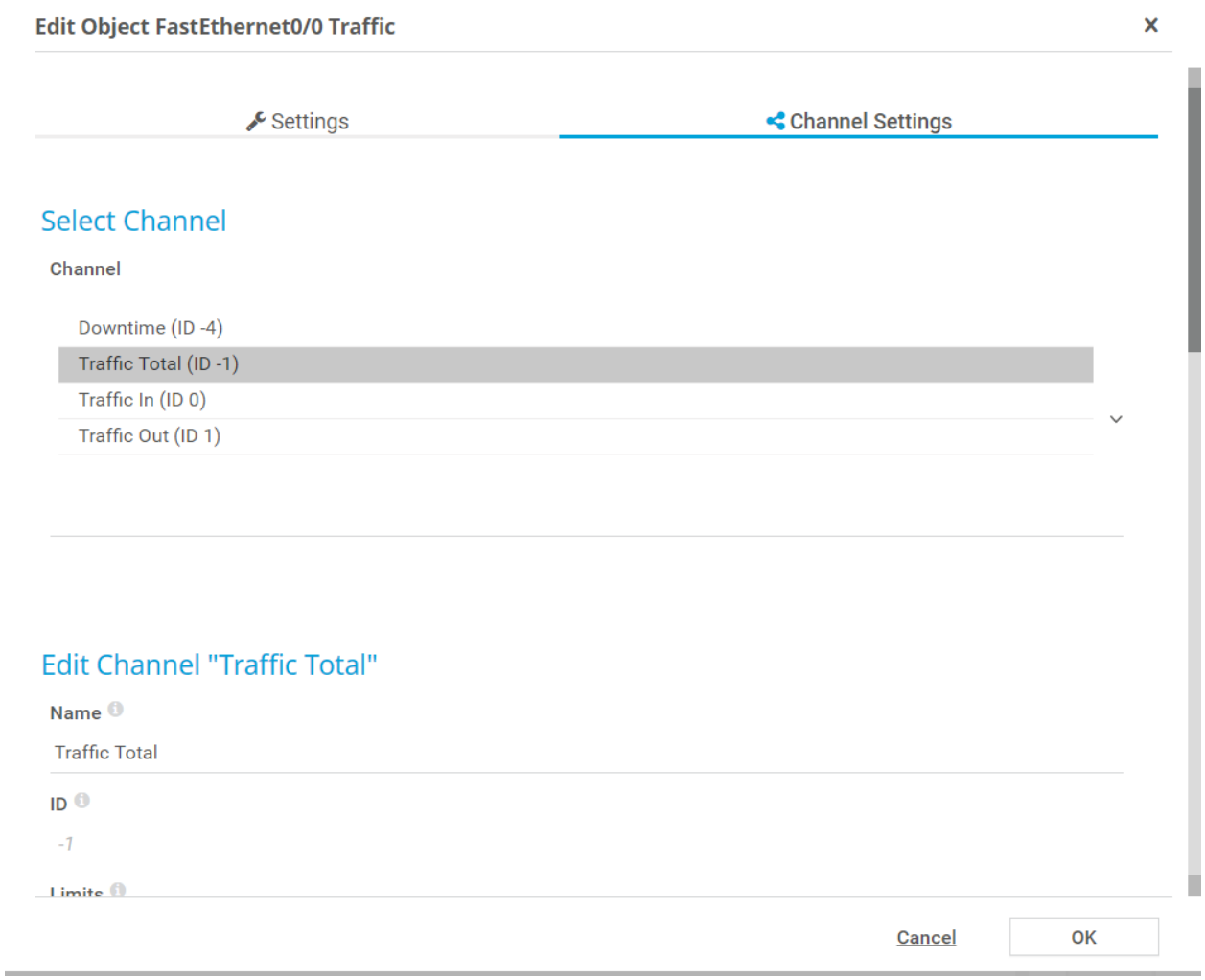


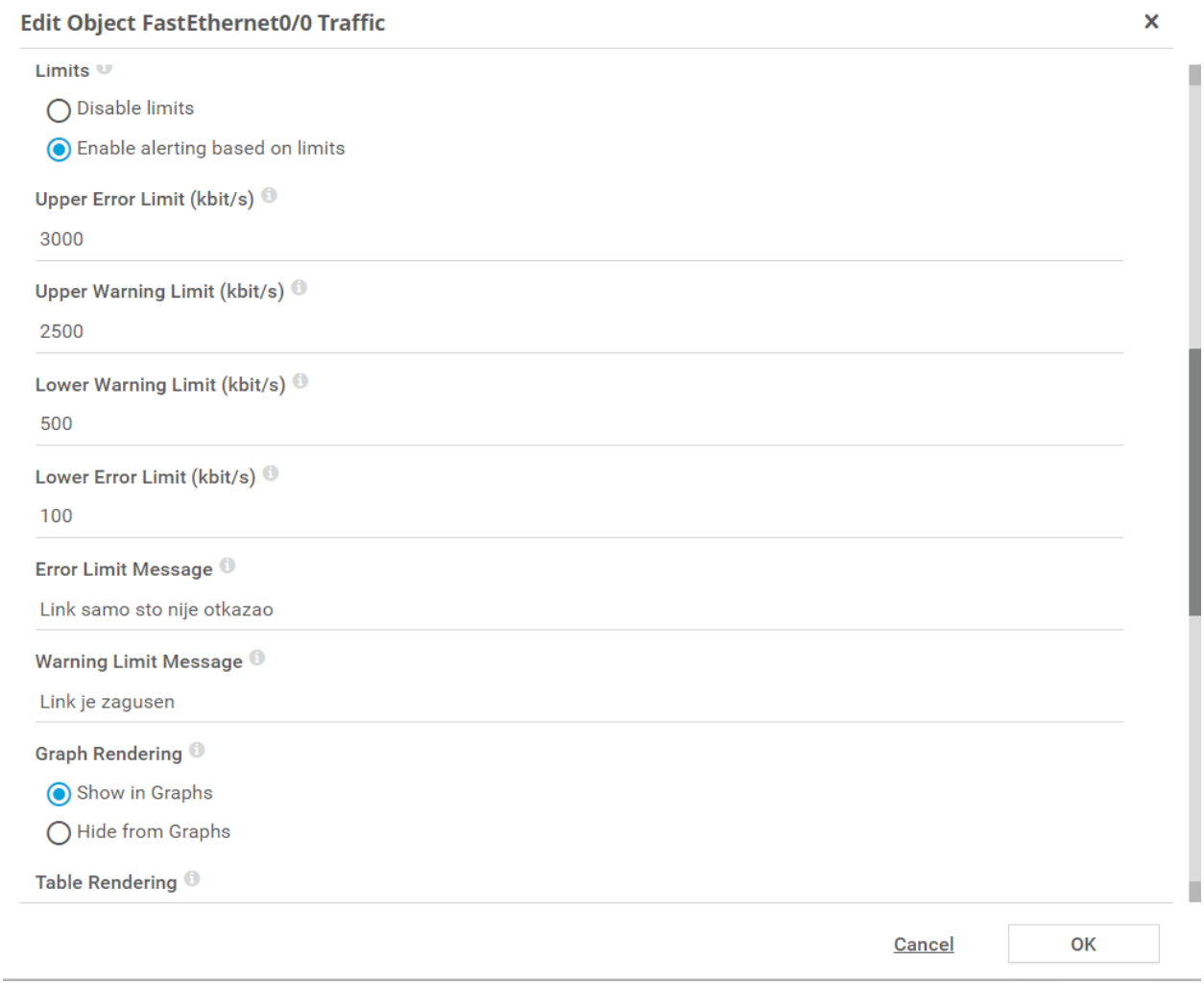
Add Sensor to Device 192.168.2.254 (CiscoRouter) [192.168.2.254]



Zatim editiramo senzore da bi postavili limite:

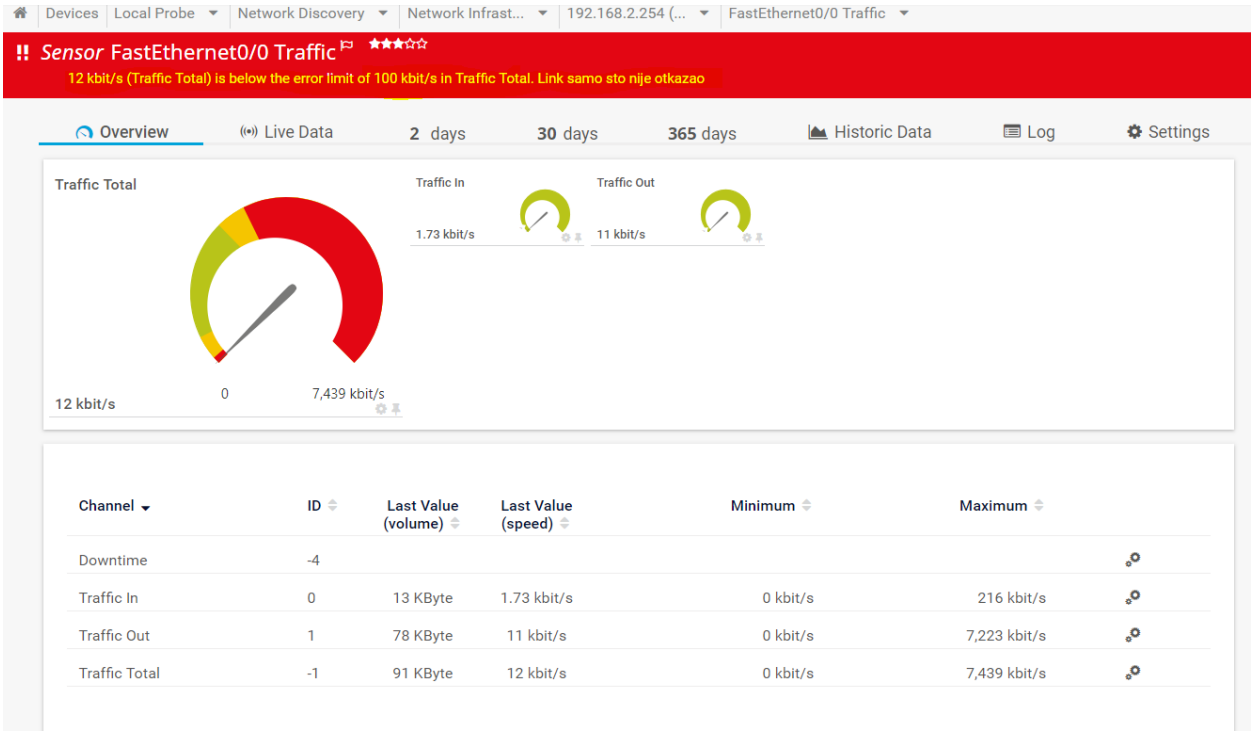



Edit Object FastEthernet0/0 Traffic
Settings
Channel Settings
Select Channel
Channel
Downtime (ID -4)
Traffic Total (ID -1)
Traffic In (ID 0)
Traffic Out (ID 1)
Edit Channel "Traffic Total"
Name
Traffic Total
ID
-1
Limits
Cancel
OK



Postavite dovoljno male limite kako bi ih na ispitu lako mogli dokazati da rade!

Zatim generiramo neki promet ...ping, ili još bolje youtube kako bi generirali promet i dobili poruke od PRTG-a da smo probili limite...



Morate dobiti ovakvu poruku ako je promet premali ili ga nema!

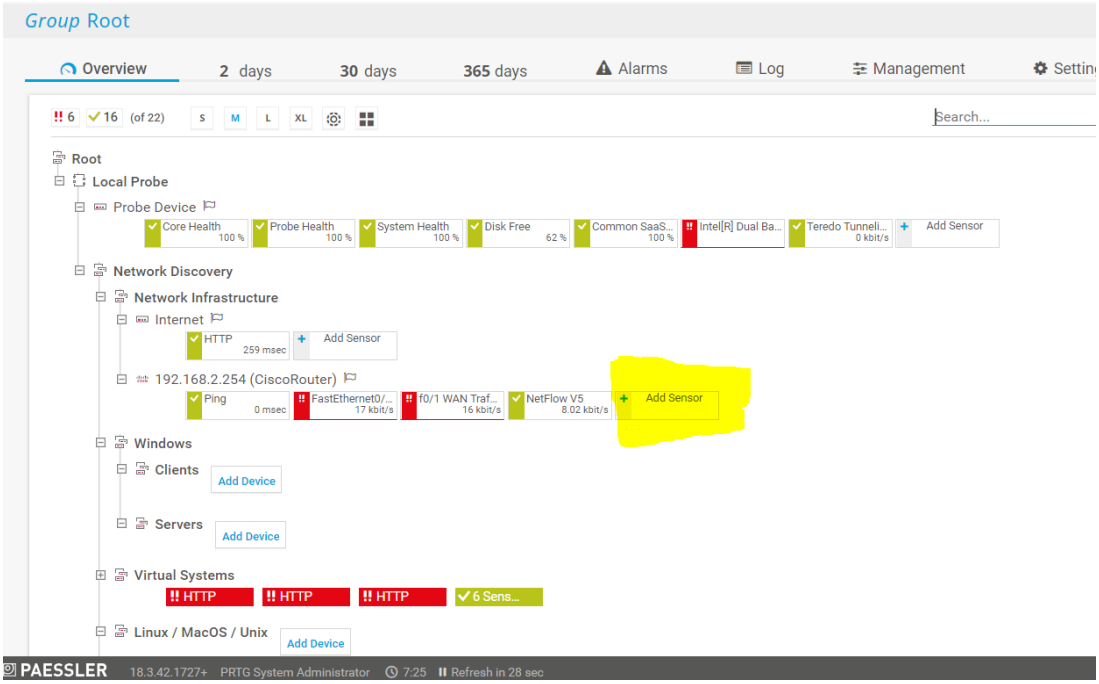
2.2. NETFLOW

Također želimo imati uvid i grafove o korištenju linka, tko nam surfa, gdje i koliko...
Za to koristimo senzor NETFLOW....pa idemo i to podesiti...

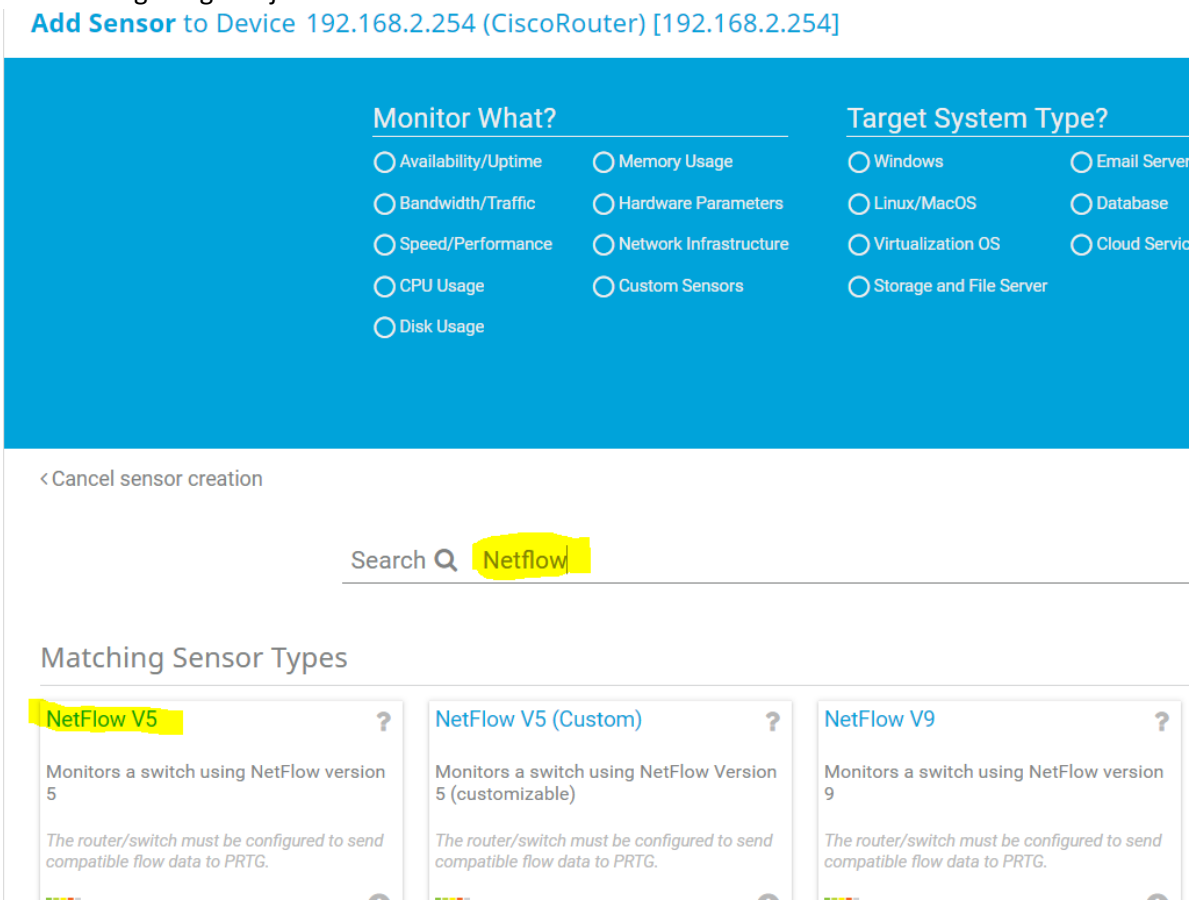
Prvo router konfamo:

```
R1(config)#int fa 0/0
R1(config-if)#ip flow ingress
R1(config-if)#ip flow egress
R1(config-if)#exi
R1(config)#ip flow-export source fa 0/0
R1(config)#ip flow-export ver 9
R1(config)#ip flow-export destination 192.168.0.22 9996
R1(config)#
```

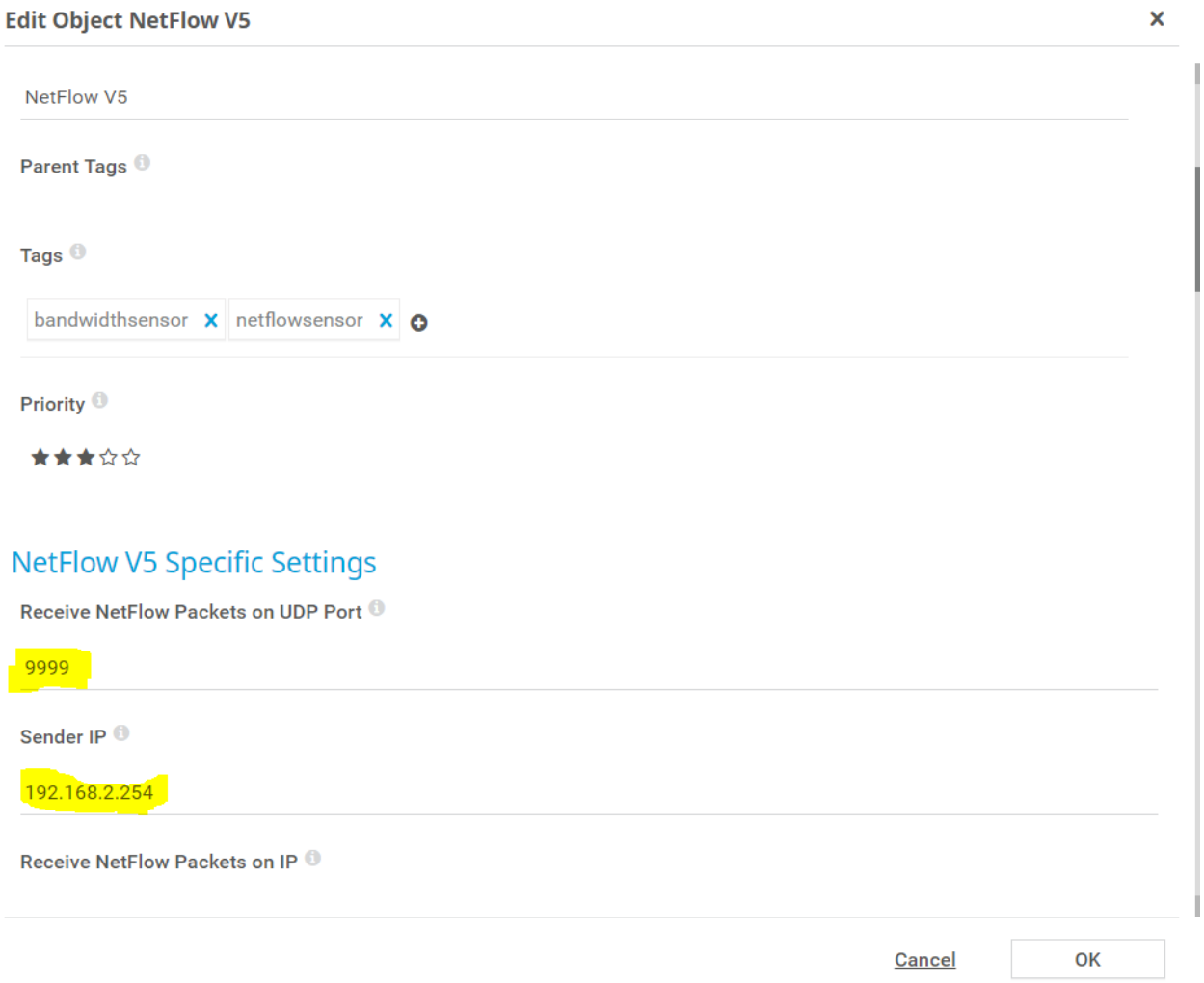
Zatim u PRTG-u odaberemo add sensor:

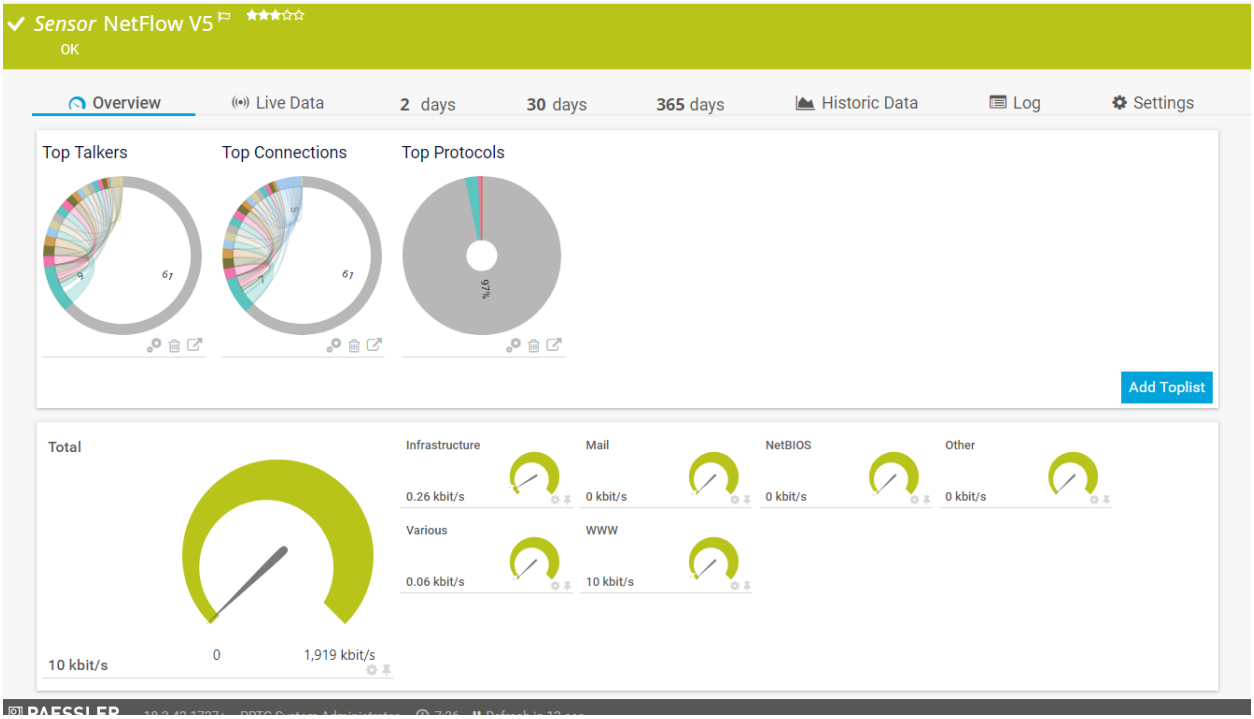


U tražilicu upišete Netflow da vam nađe senzor (jer PRTG ima jako puno senzora pa je tražilica korisna) i odaberete ga te ga dalje editirate:



Potrebno je podesiti ip adresu routera (LAN interfejs) i broj udp porta (stavimo bilo koji, ja sam stavio 9999, ali isti taj moramo podesiti i na routeru)




Sensor NetFlow V5
OK
Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings
Top Talkers
Top Connections
Top Protocols
97%
Add Toplist
Total
10 kbit/s
0
1,919 kbit/s
Infrastructure
0.26 kbit/s
Mail
0 kbit/s
NetBIOS
0 kbit/s
Other
0 kbit/s
Various
0.06 kbit/s
WWW
10 kbit/s