Содержание

Monitoring traffic distribution by class

SSG allows traffic distribution by class to be monitored.

1. Enable traffic prioritization. For the example, we will use the following prioritization rules:

```
dns cs0
http cs0
https cs0
Bittorrent cs7
ICMP cs0
TCP Unknown cs7
GOOGLEVIDEO cs1
default cs2
```

2. In the `/etc/dpi/fastdpi.conf` configuration, set the parameter:

```
dbg_log_mask=0x4
```

3. Enable common channel polysync (the example shown is polysync with full channel width restriction):

```
htb_inbound_root=rate 1300mbit
htb_inbound_class0=rate 8bit ceil 1300mbit
htb_inbound_class1=rate 8bit ceil 1300mbit
htb_inbound_class2=rate 8bit ceil 1300mbit
htb_inbound_class3=rate 8bit ceil 1300mbit
htb_inbound_class4=rate 8bit ceil 1300mbit
htb_inbound_class5=rate 8bit ceil 1300mbit
htb_inbound_class6=rate 8bit  ceil 1300mbit
htb_inbound_class7=rate 8bit  ceil 1300mbit
htb_root=rate 1300mbit
htb_class0=rate 8bit ceil 1300mbit
htb_class1=rate 8bit ceil 1300mbit
htb_class2=rate 8bit ceil 1300mbit
htb_class3=rate 8bit ceil 1300mbit
htb_class4=rate 8bit ceil 1300mbit
htb_class5=rate 8bit ceil 1300mbit
htb_class6=rate 8bit  ceil 1300mbit
htb_class7=rate 8bit  ceil 1300mbit
```

4. Update the configuration:

```
service fastdpi reload
```

If polyscing for a shared channel is applied for the first time, you must restart the service:

```
service fastdpi restart
```

5. Use the following custom settings for the zabbix agent installed on the SSG:

ssg_userparams.conf

6. Import the template to the Zabbix server as described in the section "Monitoring via SNMP agent":

zbx_export_templates.xml

If necessary, change the interface names in the template and in the custom parameter file

View flow and protocol statistics

By flow

1. IPv4/IPv6
2. protocol type: 0 - IPv4, 1 - IPv6
3. total allocated records
4. a queue with a short lifespan:
    1. occupied records
    2. reusable
    3. difference 3.1 - 3.2 (number of active flows)
5. also for the long line
6. also total

Example:

```
fdpi_ctrl stat --flow
IPv4 0 6784000 834 814 20 0 0 0 834 814 20
```

By protocols

1. internal index of protocol statistics
2. protocol name
3. protocol port number
   direction subs -→ inet
4. number of packages
5. volume in bytes ip total
6. dropped packages
7. dropped byte
   direction inet -→ subs number of packages etc.

Example:

```
fdpi_ctrl stat --proto
Autodetected fastdpi params : dev='em1', port=29001
connecting 94.140.198.68:29001 ...

================================
94 'ntp' 123 0 0 0 0 91 23569 0 0
4081 'sip' 5060 0 0 0 0 2479 1170579 0 0
5812 'Bittorrent' 49165 0 0 0 0 0 0 3 495
5866 'ICMP' 65025 0 0 0 0 225 18900 0 0
5871 'TCP Unknown' 65030 0 0 0 0 41034 3448836 0 0
5880 'UDP Unknown' 65041 3900 4227600 0 0 277 24825 0 0
6000 'ARP' 65282 30 2520 0 0 30 2520 0 0
6056 'CHAMELEON' 49236 0 0 0 0 589 72475 0 0
```