## **Table of Contents**

astDPI monitoring and logs	3
Log file rotation	3
To view statistics via the terminal	3
flow	3
proto	4
Monitoring via SNMP agent (Zabbix-agent)	4
Agent Setup	4
Server setup	5
Monitoring traffic distribution by class	6

# **FastDPI monitoring and logs**

System logs are presented as text files that are located in the /var/log/dpi directory for DPI and PCRF modules. Types of messages in the log:

- 1. [CRITICAL] critical error, system operation is impossible without troubleshooting
- 2. [WARNING] warning, the system does not stop, but it is worth eliminating this malfunction
- 3. [TRACE] messages when the diagnostic trace mode is enabled
- 4. [INFO] notification of system actions
- 5. [ERROR] error when connecting services and policies, incorrect configuration

The FastDPI process by default logs all system actions to the following debug and statistics log files:

- 1. /var/log/dpi/fastdpi\_slave.log a log of traffic processing processes<sup>11</sup>
- 2. /var/log/dpi/fastdpi\_stat.log traffic processing statistics log
- 3. /var/log/dpi/fastdpi\_alert.log common fastDPI functions log

Blocking counters that are saved in the statistics log

### Log file rotation

File rotation provides a daily backup of the daily log. By default, this process is performed during the hours with the lowest system load. The log storage depth is defined in the configuration of /etc/logrotate.d/fastdpi by the parameter maxage, the value is specified **in days**.

### To view statistics via the terminal

#### 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

#### proto

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

#### Example:

```
fdpi_ctrl stat --proto
Autodetected fastdpi params : dev='eml', 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 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
```

### Monitoring via SNMP agent (Zabbix-agent)

We offer you the following set of parameters that can be taken from the SSG DPI:

- Errors in fastDPI process log /var/log/dpi/fastdpi\_alert.log
- Errors in the /var/log/messages system log
- Losses (Drop) on dna interfaces
- Traffic volume on interfaces
- Availability of control interfaces
- Number of HTTP and HTTPS requests processed
- Number of blocked resources by HTTP, HTTPS, IP
- Number of PPPoE sessions

You can use Zabbix Agent for monitoring.

Current and final supported version of agent and server is 6.0, Zabbix agent 1 should be used. For newer versions of Zabbix, monitoring will be done via SNMP.

### Agent Setup

1. Install Zabbix agent 1 on the DPI server according to the instructions on the Zabbix website.

In the first step, select the following values:

- Zabbix Packages
- $\circ$  Zabbix version: 6.0+
- $\circ~$  OS distribution: CentOS
- OS version: 8 STREAM
- Zabbix component: AGENT
- 2. Edit the configuration file /etc/zabbix/zabbix\_agentd.conf: change the parameters Server= and ServerActive= to your server address, hostname= to the server hostname.
- 3. Change the context of the /var/log/dpi/fastdpi\_stat.log file:

```
chcon unconfined_u:object_r:zabbix_log_t:s0
/var/log/dpi/fastdpi_stat.log
```

- 4. Open tcp/udp ports 10050 and 10051 in firewall
- 5. Upload the

ssg\_userparams.conf

file to the /etc/zabbix/zabbix\_agent.d/ directory

- 6. Edit the ssg\_userparams.conf file by replacing the interface number in UserParameter
- 02-00.0 should be replaced with the interface names of your server! The name must match the DPI config. If you have more than 2 interfaces in use, you must add a line similar to the existing parameters.

```
UserParameter=dpi.02-00.0.drops,tac /var/log/dpi/fastdpi_stat.log | sed
/'IF 02-00.0'/q | tac | sed -e 1,/'Actual Stats'/d | sed '6!D' | awk
'{print $1}' | sed 's/^.//'
```

7. Restart the agent: systemctl restart Zabbix-agent

#### Server setup

- 1. Install and configure Zabbix servers according to the instructions on the official website.
- 2. Add template

zbx\_export\_templates.xml

- 1) Go to Configuration section
- 2) Templates section
- 3) Click "Import"
- 4) Import template file
- 5) Save changes



- 3. Add a DPI server as a host
  - 1) Go to Monitoring section
  - 2) Hosts section
  - 3) Click "Create host"
  - 4) Set the required parameters, hostname, group and the previously added template

5	) Save	changes
-	, 54+6	changes

Z	ABBIX « 🔊	Hosts												3	treate host
23	bix	< 8		Host								×			
	۹			Heat IDMI Taxa	Massas	Investory For	untion Makie maner	ine.							
0	Monitoring 1	)	(4)	Hook IPMI Tago	Macros	inventory End	ypoon value mapp	ang (							
	Dashboard			* Host name	DPI-00								Remove		
	Problems			Visible name	DP1-00										
(2	Hosts			Templates	Name			Action							
	Latest data				VASE-mib	a a a a a b		Unlink Unlink and clea	Colect						
	Maps				type nere to	o search			Select						
	Discovery			* Groups	type here to	× search			Select						
Ğ	Services -			Interfaces	Туре	IP address		DNS name	Connect to	Port	Default				
:=	Inventory -	Name .	Interface		✓ SNMP	10.10.99.100			IP DNS	161	Remove	s	Graphs	Dashboards	Web
	Reports -	DPI-00	10.10.99.100		Add							s			
a	Configuration	DP1-02	10.10.99.104	Description								s			
		DPI-07	10.10.99.107									5	Graphs 31		
12	Administration ~	Zabbix server	127.0.0.1:100									s	Graphs 25	Dashboards 4	
									a					Displa	rying 4 of 4 found
				Monitored by proxy	(no proxy)	$\sim$									
				Enabled	~										
									_						
									(5)	Update Clon	e Full clone Delete	Cancel			
9	Support														
E	Integrations														
?	Help														
	Licar caltinne														
	oser senings v														
٩	Sign out							Zabbix 6.0.28. 0	2001–2024, <u>Zabbi</u>	x SIA					

4. Edit the template: change the names of the interfaces and keys so that they match the UserParameter.

### 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:

http cs0 https cs0 Bittorrent cs7 ICMP cs0 TCP Unknown cs7 GOOGLEVIDE0 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":



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

#### 1)

For each handler, its own fastdpi\_slave log is created, other log files are created in a single copy.