Содержание

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
2. /var/log/dpi/fastdpi_stat.log - traffic processing statistics log
3. /var/log/dpi/fastdpi_alert.log - common fastDPI functions log

Note: For each handler, its own fastdpi_slave log is created, other log files are created in a single copy.

Blocking counters that are saved in the statistics log

We offer you the following set of parameters that can be received from the VAS Experts DPI:

1. fastDPI process errors from the */var/log/dpi/fastdpi_alert.log* log file
2. system log errors from */var/log/messages*
3. drops within the DNA interfaces
4. traffic volumes on the interfaces
5. availability of management interfaces
6. the number of processed requests over HTTP and HTTPS
7. the number of blocked resources over HTTP, HTTPS, IP
8. the number of PPPoE sessions

You can use zabbix agent for monitoring. Installation Description:

1. Install zabbix agent on the server:

```
rpm -ivh
http://repo.zabbix.com/zabbix/2.4/rhel/6/x86_64/zabbix-release-2.4-1.el6.noa
rch.rpm
yum install zabbix-agent
```

2. Update SELinux policy

```
yum update selinux-policy
```

3. Put

skat_userparams.conf

to the /etc/zabbix/zabbix_agent.d/ directory and zabbix_agentd.conf to the /etc/zabbix/

4. Edit /etc/zabbix/zabbix_agentd.conf file:

```
Server=%zabbix server address%
ServerActive=%zabbix server address%
Hostname=%server hostname%
```

5. 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
```

6. Add to the /etc/sysconfig/iptables the following rule before -A INPUT -j REJECT:
-A INPUT -p tcp --dport 10050 -j ACCEPT

7. Reload iptables rules:

```
service iptables reload
```

8. Add zabbix agent to start on boot and start it:

```
chkconfig zabbix-agent on
service zabbix-agent start
```

9. Import prepared template in Zabbix

- For version 4.2 (new) - zbx_template_dpi_4.2.xml
- For version 3.4 (new) - zbx_template_dpi_3.4.xml
- For version 2.4 (old) - zbx_template_dpi.xml

In the Zabbix server control panel add a new host, bind this template.

10. Disable requests for network interfaces that are not used in dpi by clicking on enabled on the right in the zabbix GUI

Lock counters that are stored in the statistics log