Table of Contents

How to monitor the DPI

Next set of parametrers can be given from DPI:

1. Errors in logs of fastdpi /var/log/dpi/fastdpi_alert.log
2. Errors in system log /var/log/messages
3. Drops on dna devices
4. Device traffic volume
5. State of control devices
6. Quantity of processed requests for HTTP, HTTPS
7. Quantity of locked requests for HTTP, HTTPS, IP

Zabbix Agent is used in the example.

1. Zabbix Agent installation:

```
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. Change SELinux policy

```
yum update selinux-policy
```

3. Put skat_userparams.conf into directory: /etc/zabbix/zabbix_agent.d/ and zabbix_agentd.conf into /etc/zabbix/

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

```
Server=%address of zabbix server%
ServerActive=%address of zabbix server%
Hostname=%servers' hostname%
```

5. Change file context /var/log/dpi/fastdpi_stat.log:

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

6. add into /etc/sysconfig/iptables the rule before -A INPUT -j REJECT:
-A INPUT -p tcp –dport 10050 -j ACCEPT

7. Reload iptables:

```
service iptables reload
```

7. Make agent start at reboot and run it:

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

8. import DPI template into Zabbix zbx_template_dpi.xml. In the management pannel of Zabix server insert a new host and link it to the imported template.

9. In Zabix GUI set off requests to network devices that isn't used in DPI - click on enabled from right