Содержание

9 Мониторинг

Мы предлагаем вам следующий набор параметров, которые можно снимать с DPI СКАТ:

1. Ошибки в логах процесса fastdpi /var/log/dpi/fastdpi_alert.log
2. Ошибки в системном логе /var/log/messages
3. Потери (Drop) на интерфейсах dna
4. Объем трафика на интерфейсах
5. Доступность интерфейсов управления
6. Количество обработанных запросов по HTTP и HTTPS
7. Количество заблокированных ресурсов по HTTP, HTTPS, IP

Для мониторинга можно использовать zabbix agent. Описание по установке.

1.Установить на сервер zabbix agent:

```
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.Обновить SELinux policy

```
yum update selinux-policy
```

3.Поместить skat_userparams.conf в директорию /etc/zabbix/zabbix_agent.d/ и zabbix_agentd.conf в /etc/zabbix/

4.Отредактировать файл /etc/zabbix/zabbix_agentd.conf:

```
Server=%адрес zabbix сервера%
ServerActive=%адрес zabbix сервера%
Hostname=%hostname сервера%
```

5.Изменить контекст файла /var/log/dpi/fastdpi_stat.log:

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

6.Добавить в /etc/sysconfig/iptables правило перед -A INPUT -j REJECT:
-A INPUT -p tcp --dport 10050 -j ACCEPT

7.Перечитать правила iptables:

```
service iptables reload
```

7.Добавить агента в автозапуск и запустить его:

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

8. Импортировать подготовленный шаблон в Zabbix

- Для версии 3.4 (новый) - zbx_template_dpi_3.4.xml
- Для версии 2.4 (старый) - zbx_template_dpi.xml

В панели управления Zabbix сервером добавить новый хост, привязать данный шаблон.

9. В GUI zabbix отключить запросы по сетевым интерфейсам, которые не используются в dpi - кликнуть на enabled справа