Содержание

DPI management configuration. Integration using the PUSH method

Subscriber Management (SM) allows you to assign services, manage bandwidth limits (policing), and perform other actions for individual subscribers.

SSG DPI identifies subscribers by their IP addresses, since no other subscriber information is present in IP packets. Therefore, if IP addresses are assigned dynamically, integration with the IP address assignment system (RADIUS or DHCP) is required, or the FastRadius (RADIUS Event Monitor. RADIUS Mapping) component must be installed.

Integration between the DPI platform and the billing system using the PUSH model assumes that the billing system (or an auxiliary system) independently sends information about the subscriber's assigned services and policing settings to the DPI before those settings are actually applied. The transmitted data is stored in the built-in UDR database and remains active immediately after a system reboot.

It is recommended to use the PULL integration method (via the RADIUS protocol). Product: BNG/BRAS.

To restore subscriber profile settings after a platform restart, you must enable the built-in database or place initialization scripts in the `/etc/dpi/init.d/` directory (similar to the standard Linux approach for managing traffic shapers or the boot process). The latter option has its own advantages and may be suitable for rapid migration from Linux/FreeBSD or hardware traffic shapers without their own database.

Common scenarios for preparing profiles used for financial blocking are described in the article Quick Start: Tariff Plan and Captive Portal.

The `fdpi_ctrl` utility is a high-performance API for DPI management.
Example: assigning a tariff plan (policing settings) to 30,000 subscribers takes less than one second:

```
time fdpi_ctrl load --policing rate_10M.cfg --file subsribers.lst
 Result processing file 'subsribers.lst' : 30000/30000/0/0/0
 real 0m0.344s
 user 0m0.009s
 sys 0m0.144s
```

Running commands remotely over SSH

To execute commands on the DPI server remotely via SSH without entering a password, it is recommended to use public key authentication.

On the management server, perform the following steps:

1. Create a public/private key pair:

   ```
   ssh-keygen -t rsa
   ```

   Accept the default values in the dialog. For convenience, leave the passphrase empty[1)]

2. Copy the public key to the DPI server using:

   ```
   ssh-copy-id dpi_user@dpi_host
   ```

   or manually:

   ```
   cat ~/.ssh/id_rsa.pub | ssh dpi_user@dpi_host "mkdir -p ~/.ssh && cat
   >> ~/.ssh/authorized_keys"
   ```

3. On the DPI server, verify and correct the permissions of the `authorized_keys` file:

   ```
   chmod 700 ~dpi_user/.ssh/
   chmod 600 ~dpi_user/.ssh/authorized_keys
   restorecon -Rv ~dpi_user/.ssh/
   ```

4. Verify that `fdpi_ctrl` can be executed remotely from the management server:

   ```
   ssh dpi_user@dpi_host "fdpi_ctrl load --service 6 --login test"
   ```

   If execution fails, check the `/var/log/secure` log on the DPI server and enable SSH diagnostic mode using `ssh -v ...`.

Running the fdpi_ctrl utility remotely

Commands are transmitted to the DPI over a TCP connection through the management port. Therefore, the firewall must allow external access to the management port.

To enable the DPI platform to accept management commands, configure the following parameters in `/etc/dpi/fastdpi.conf`:

1. Listening port number:

   ```
   ctrl_port=29000
   ```

2. Network interface name. By default, DPI listens only on the loopback interface:

   ```
   ctrl_dev=eth0
   ```

To run the `fdpi_ctrl` utility remotely:

1. In the DPI configuration file `/etc/dpi/fastdpi.conf`, enable listening on a management interface accessible from external hosts:

```
ctrl_dev=eth0
```

2. In the firewall configuration `/etc/sysconfig/iptables`, allow access to the port specified by `ctrl_port` and restrict access to the DPI host so that only the management server is permitted:

```
-A INPUT -m state --state NEW -m tcp -s 192.168.0.2 -p tcp --dport
29000 -j ACCEPT
```

3. Copy the `fdpi_ctrl` utility to the management server and run it with the `-r host:port` argument:

```
fdpi_ctrl load --service 6 --login test -r 192.168.0.1:29000
```

Whenever the DPI version is updated, the `fdpi_ctrl` utility on the management server must also be updated.

[1)]
Or use `ssh-agent` to store passphrases.