Содержание

Управление

Управление данным сервисом на уровне отдельных абонентов осуществляется с помощью fdpi_ctrl

Формат команды:

```
fdpi_ctrl команда --service 10 [список опций] [список_IP или login]
```

Подробнее синтаксис команд и способы задания IP адресов описаны в разделе Команды управления

Примеры:
Создание профиля с именем и подключение услуги блокировки с профилем для нескольких абонентов

```
fdpi_ctrl load profile --service 10  --profile.name test_protect --
profile.json '{ "ddos_trace" : 1, "ddos_reqsec_threshold" : 100,
"ddos_reqsec_variation" : 5, "ddos_pktsec_threshold" : 1000,
"ddos_pktsec_variation" : 5, "ddos_check_server" : "captcha.server.ru/?",
"ddos_security_key" : "123", "syncf_protection" : 0 , "syncf_trace" : 0 ,
"syncf_check_tmout" : 0 , "syncf_tracking_packs_time" : 0 ,
"syncf_unconfirmed_percent" : 0 , "syncf_threshold" : 0  }'
fdpi_ctrl load --service 10 --profile.name test_protect --ip 192.168.0.1
fdpi_ctrl load --service 10 --profile.name test_protect --ip 192.168.0.2
```

где в формате json задаются настройки профиля услуги
Настроечные параметры описаны в соответствующих разделах:
ddos_trace,ddos_reqsec_threshold,ddos_reqsec_variation,ddos_pktsec_threshold,ddos_pktsec_variation, ddos_check_server,ddos_security_key
syncf_protection,syncf_trace,syncf_check_tmout,syncf_tracking_packs_time,syncf_unconfirmed_percent,syncf_threshold

В профиле возможно указание только части параметров, например только параметров для ddos защиты, тогда защита от syn flood будет неактивна. Остальные неуказанные параметры примут значения по умолчанию.

Поиск абонентов, которым подключено оповещение с заданным именем профиля

```
fdpi_ctrl list all --service 10 --profile.name test_protect
```

Удаление именованного профиля (не должно быть абонентов, которые его используют)

```
fdpi_ctrl del profile --service 10  --profile.name test_protect
```

Изменение настроек (профиля) услуги (новые настройки применятся ко всем абонентам с заданным профилем услуги)

```
fdpi_ctrl load profile --service 10  --profile.name test_protect --
```

```
profile.json '{ "ddos_reqsec_threshold" : 0, "ddos_reqsec_variation" : 5,
"ddos_pktsec_threshold" : 0, "ddos_pktsec_variation" : 5, "syncf_protection"
: 1 , "syncf_trace" : 1 , "syncf_check_tmout" : 500 ,
"syncf_tracking_packs_time" : 180 , "syncf_unconfirmed_percent" : 25 ,
"syncf_threshold" : 100  }'
```

Список созданных профилей для услуги и их настроек

```
fdpi_ctrl list all profile --service 10
```

Деактивировать защиту для конкретного абонента

```
fdpi_ctrl del --service 10 --ip 192.168.0.1
```

Просмотр статуса защиты

```
fdpi_ctrl list status --service 10 --ip 192.168.0.1
Вывод команды:
192.168.0.1   synf=0  ddos=1
```

- synf=0 syn-flood защита не активна
- ddos=1 ddos защита активна

Максимальное количество профилей для ddos защиты задается настроечным параметром в */etc/dpi/fastdpi.conf*

```
max_profiles_ddos=32
```

где 32 значение по умолчанию, а 65535 максимально возможное значение Это холодный параметр и его изменение требует рестарта.