Содержание

Мини Firewall 3

Мини Firewall

Услуга предназначена для повышения защищенности от взлома оборудования абонентов с белыми[1)] адресами (IPv4 и IPv6). На адрес абонента закрываются все входящие запросы на порты ниже указанного порога (обычно 1024 - на все системные порты), но при этом некоторые порты можно оставить открытыми, например, для доступа к домашнему NAS. Также можно заблокировать некоторую вредоносную активность, исходящую от абонента, например если в результате анализа netflow или получения abuse выяснилось, что абонент занимается спамом, то можно закрыть ему исходящие порты, связанные с почтовой рассылкой.

Нужно учитывать, что часто в этом случае абонент не виновен, просто его компьютер заражен вирусом или является частью чужой ботнет-сети. В этом случае рекомендуется показать абоненту страницу уведомления с помощью услуги 6 с описанием проблемы и предложением подписки на антивирус, и тем самым повысить продажи доп. услуг. В дальнейшем этот сервис планируется еще больше автоматизировать в QoE Store/Маркетинговых кампаниях в части диагностики заражения, блокирования вредоносной активности и автоматической выдачи оповещения.

Управление данным сервисом на уровне отдельных абонентов осуществляется с помощью fdpi_ctrl

Формат команды:

```
fdpi_ctrl команда --service 13 [список_опций][список_IP или Login]
```

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

Примеры:

активировать мини Firewall для конкретного абонента с именованным (заранее сконфигурированным) профилем

```
fdpi_ctrl load profile --service 13 --profile.name полный_firewall --
profile.json '{  "max_port" : 1024, "port_holes" : [ 80, 8080 ], "out_port"
: [ 25, 465 ] }'
fdpi_ctrl load --service 13 --profile.name полный_firewall --login
ivan.ivanovich
```

где в формате json задаются следующие настройки профиля
max_port - номер порта, ниже которого блокируется доступ
port_holes - список портов, к которым разрешается доступ в обход ограничения max_port
out_port - список портов, на которые закрыт исходящий трафик

Подключение абоненту мини Firewall с анонимным профилем (профиль без имени, который существует до отключения услуги у абонента)

```
fdpi_ctrl load --service 13 --profile.json '{  "max_port" : 1024,
"port_holes" : [ 80, 8080 ], "out_port" : [ 25, 465 ] }' --login
ivan.ivanovich
```

Поиск абонентов, которым подключен мини Firewall с заданным именем профиля

```
fdpi_ctrl list all --service 13 --profile.name полный_firewall
```

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

```
fdpi_ctrl del profile --service 13  --profile.name полный_firewall
```

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

```
fdpi_ctrl load profile --service 13 --profile.name полный_firewall --
profile.json '{  "max_port" : 1024, "port_holes" : [ 80 ] }'
```

Максимальное количество профилей для мини Firewall задается настроечным параметром в /etc/dpi/fastdpi.conf

```
 max_profiles_frwl=24
```

где 24 значение по умолчанию (максимально возможное значение 65535)


Это холодный параметр и его изменение требует рестарта.

1)
В случае серых адресов роль своеобразной защиты играет NAT