Table of Contents

Настройка и управление	
Дополнительные настройки	

Настройка и управление

Управление данным сервисом на уровне отдельных абонентов осуществляется с помощью fdpi ctrl.

Формат команды:

```
fdpi_ctrl команда --service 11 [список опций] [список_IP или login]
```

Подробный синтаксис команд и способы задания IP-адресов описаны в разделе Команды управления.



Подключение трансляции адресов для абонента осуществляется через услугу 11.

CG-NAT

Создаем профиль услуги CG-NAT, в котором определяем параметры пула IP-адресов:

```
fdpi_ctrl load profile --service 11 --profile.name test_nat --profile.json
'{ "nat_ip_pool" : "5.200.43.0/24,5.200.44/25", "nat_tcp_max_sessions" :
2000, "nat_udp_max_sessions" : 2000 }'
```

Описание параметров находится в таблице ниже.



В случае привязки к login нескольких IP или подсетей, счетчик сессий индивидуален для каждого IP-адреса.



При указании диапазона внешних IP-адресов можно указать один или несколько диапазонов через запятую, можно динамически добавить дополнительные диапазоны в ранее созданный пул.

Из диапазона можно исключить крайние адреса (по соглашению о бесклассовой адресации, это адреса шлюза и широковещательный), добавив в определение диапазона символ "~" в конце определения cidr, например: 5.200.43.0/24~.

NAT 1:1

Создание профиля услуги NAT $1:1^{1}$, в котором определить диапазон IP-адресов пула:

```
\verb|fdpi_ctrl load profile --service 11 --profile.name test_nat --profile.json|\\
```

```
'{ "nat_ip_pool" : "5.200.44.0/24,5.200.44/25", "nat_type" : 1 }'
```

Описание параметров находится в таблице ниже.

При указании диапазона внешних IP адресов можно указать один или несколько диапазонов через запятую, можно динамически добавить дополнительные диапазоны в ранее созданный пул.



Из диапазона можно исключить крайние адреса (по соглашению о бесклассовой адресации, это адреса сети и широковещательный) добавив в определение диапазона символ " \sim " в конце определения cidr, например: 5.200.43.0/24 \sim .

Временное ограничение: каждый из отдельных пулов в общем списке пулов должен содержать публичных адресов не меньше, чем число рабочих потоков.

Управление услугой NAT

Подключить абоненту услугу 11 с заданными ранее параметрами пула:

```
fdpi_ctrl load --service 11 --profile.name test_nat --ip 192.168.0.1 или
fdpi_ctrl load --service 11 --profile.name test_nat --login test_subs или
fdpi_ctrl load --service 11 --profile.name test_nat --cidr 192.168.1.0/24
```

Просмотреть список всех NAT профилей:

```
fdpi_ctrl list all profile --service 11
```

Дополнительные настройки

Дополнительно в глобальных параметрах /etc/dpi/fastdpi.conf можно задать:

- nat ports
- nat_max_profiles
- nat_exclude_private
- nat_private_cidr
- lifetime flow
- lifetime_flow_long

Описание параметров находится в таблице ниже.

С версии 12.0 появилась возможность выбрать метод хеширования flow по рабочим потокам. При использовании нового метода распределение адресов не зависит от количества рабочих потоков. Настраивается параметром rx_dispatcher в fastpdi.conf (для принятия

изменений требуется **restart** сервиса). Значения параметра описаны в таблице ниже.

Для того чтобы гарантировать NAT преобразование для приватного IP-адреса в любой публичный IP-адрес при использовании NAT 1:1, необходимо указать диапазон IP-адресов, который используется в NAT 1:1. Настраивается параметром nat_transcode_cidr в fastdpi.conf (для принятия изменений требуется **restart** сервиса):

nat_transcode_cidr=201.201.210.0/24,201.210.210.0/29

Описание параметра находится в таблице ниже.

Параметр nat_transcode_cidr актуален **только** при использовании нового метода распределения **и** использовании NAT 1:1. В других случаях данный параметр не учитывается, его наличие не считается ошибкой.

Параметры и возможные значения

Параметры профиля NAT					
Параметр	Значение				
nat_ip_pool string	Диапазон внешних IP адресов в формате CIDR. Размер пула должен быть не меньше числа рабочих потоков.				
<pre>nat_tcp_max_sessions integer</pre>	Максимальное количество ТСР сессий, которые может создать абонент. По умолчанию: 2000.				
nat_udp_max_sessions integer	Максимальное количество UDP сессий, которые может создать абонент. По умолчанию: 2000.				
nat_type integer	Задает тип профиля. Варианты: 0 CGNAT; 1 NAT 1:1.				
nat_ports string	Диапазон используемых для трансляции портов на внешних адресах. По умолчанию: 1024-65535.				
	Параметры fastdpi.conf				
Параметр	Значение				
nat_max_profiles integer	Максимальное количество профилей с параметрами пулов. По умолчанию: 4. Максимум: 65000 (при наличии достаточного объема оперативной памяти).				
nat_exclude_private integer	Исключает NAT преобразование если оба адреса приватные. Варианты: 0 off ← (по умолчанию). 1 Не делаем NAT для приватных адресов (ip_src и ip_dst приватные или находятся в nat_private_cidr). 2 ip_src — приватный с учетом nat_private_cidr и AS для dst_ip = local. 4 ip_src — приватный с учетом nat_private_cidr и AS для dst_ip = peer.				
nat_private_cidr string	Задает дополнительные диапазоны приватных адресов в дополнение к стандартным диапазонам ²⁾ . Максимум: 4 диапазона.				

Параметры fastdpi.conf				
Параметр	Значение			
lifetime_flow integer	Определяет время короткой очереди в секундах для TCP SYN, TCP FIN, UDP для всех соединений. По умолчанию: 60.			
lifetime_flow_long integer	Определяет время длинной очереди в секундах для TCP DATA установленного соединения для всех соединений. По умолчанию: 300.			
nat_whp_lifetime integer	Определяет время короткой очереди в секундах для NAT трансляции для TCP SYN, TCP FIN, UDP. Данный параметр переопределяет lifetime_flow только для NAT трансляций. По умолчанию: 75.			
nat_whp_lifetime_long integer	Определяет время длинной очереди в секундах для NAT трансляции для TCP DATA установленного соединения. Данный параметр переопределяет nat_whp_lifetime_long только для NAT трансляций. По умолчанию: 375.			
nat_transcode_cidr string Добавлен в версии 12.0	Задает CIDR публичных адресов оператора. Возможно указать только 2 CIDR (в случае использования большего количества CIDR, допустимо указание более широкого CIDR). Значения используются при перекодировке публичный -> приватный для NAT 1:1. Для приватного адреса может быть назначен любой публичный адрес для NAT 1:1.			
rx_dispatcher integer Добавлен в версии 12.0	Метод хеширования flow по рабочим потокам. Варианты: 0 прежний метод ← (по умолчанию). (IP_SRC+IP_DST)%N) & IP_MASK 1 метод с равномерной балансировкой по произвольному количеству потоков с поддержкой NAT 1:1 с требованием назначения конкретных адресов. (CRC(IP_SRC)%N+CRC(IP_DST)%N)%N 2 метод с равномерной балансировкой по произвольному количеству потоков без поддержки NAT 1:1 с требованием назначения конкретных адресов.			

операторы иногда используют трансляцию 1:1 как альтернативу маршрутизации белых IP до абонентских СРЕ, но важно понимать, что хотя эта схема немного упрощает администрирование, но она неравноценна как с точки зрения абонента, который обычно платит услугу белого адреса деньги, так и с сетевой, так как некоторое клиентское ПО знает про приватные адреса и ведет себя по другому, чем в случае с публичными адресами, например, мессенджеры WhatsApp/Viber/Skype/SIP вместо прямых P2P соединений начинают использовать stun-прокси сервера, которые часто перегружены, что может серьезно ухудшить качество голосовых и видеозвонков, не работает IPSEC VPN без поддержки NAT-Т или с авторизацией по сертификатам, абонент не может использовать свой публичный IPv4 в качестве IPv6 адреса через механизм 6to4, в торрентах перестает работать автоопределение локального ретрекера, трекеры абонентам с серыми адресами нередко выдают меньшее число пиров, что сказывается на скорости закачки и т.п. Для L2-connected абонентов лучшей альтернативой NAT1:1 является использование unnumbered адресов, которые нативно поддерживаются СКАТ BRAS. Кроме того при переходе к IPv6/Dual Stack оператору все равно придется научиться маршрутизировать публичные IPv6 адреса