Содержание

1 Описание и сценарии

Carrier Grade NAT позволяет:

- предоставлять один публичный IPv4-адрес несколькими абонентами без потери качества интернет соединения — за одним публичным IP-адресом может разместить до 100 приватных (идеальное соотношение — 1:10);
- продлить использование ограниченного адресного пространства IPv4 и сократить расходы на покупку IPv4-адресов на 90%;
- подготовиться к внедрению IPv6-адресации за счет поддержки Dual Stack v4-v6 (поддержки обеих версий протокола одновременно).

При использовании NAT необходимо учитывать, что в данном случае NAT является услугой, предоставляемой DPI, который не является маршрутизатором и работает в режиме прозрачного моста. Следует учитывать это при внедрении и конфигурировании своего оборудования.

Типы

CG-NAT (NAT44)

Трансляция сетевых адресов и портов позволяет нескольким абонентам совместно использовать один публичный адрес IPv4 и расширяет использование ограниченного адресного пространства IPv4.

BiNAT (NAT 1:1)

Трансляция сетевых адресов 1-к-1 позволяет предоставить услугу статического публичного IP адреса без изменения настроек на CPE через трансляцию всех портов приватного адреса в один публичный адрес.

Сценарии применения

L3-Connected NAT

В режиме Bridge (актуально для L3 BRAS) CKAT не имеет IP адреса на интерфейсах для обработки абонентского трафика. Исходя из этого, необходимо на бордере добавить статический маршрут для NAT пула адресов, в котором адресом следующего маршрутизатора будет являться, адрес, находящийся за CKAT.

Пример установки на сеть

В сети есть роутер R1, который является шлюзом для локальных абонентов с адресами 10.0.0.0/24, и пограничный роутер BR, который имеет связь с R1 в подсети 10.0.1.0/30. Между ними установлен DPI, на котором для абонентов включена услуга NAT. Для NAT пула выделим подсеть 100.0.0.0/24.

На R1 шлюзом является наш бордер. Для того чтобы обеспечить прохождение трафика из интернета к абонентам необходимо на бордере добавить маршрут: ip route add 100.0.0.0/24 via 10.0.1.2 После это трафик для NAT пула будет маршрутизироваться на Br в сторону R1, по пути к которому, попадая на DPI, будет подвергнут NAT. Трафик к адресам, для которых нет NAT трансляции будет дропнут на DPI.

L2-Connected NAT

В режиме L2 BRAS следует использовать в качестве следующего хопа в маршруте адрес, указанный в параметре bras_arp_ip. Данный маршрут позволяет маршрутизировать трафик для адресов из NAT пула в сторону DPI, где в пакетах адрес получателя будет изменен с белого на серый согласно таблице трансляций, и на следующий маршрутизатор в сети пакет доберется с уже “серым” получателем и уже дальнейшая маршрутизация в сети ничем не будет отличаться.

Пример установки на сеть

В данной схеме шлюзом для абонентов выступает DPI. На DPI настроен IP-адрес 10.10.10.1, на Border Router настроен IP-адрес 10.10.10.2. Для NAT пула выделим подсеть 100.0.0.0/24. Для того чтобы обеспечить прохождение трафика из интернета к абонентам, необходимо на бордере добавить маршрут: ip route add 100.0.0.0/24 via 10.10.10.1.

Варианты внедрения

CG-NAT

Классическая схема включения устройства CG-NAT в сеть — между BNG и роутером для обеспечения трансляции сетевых адресов. NAT log передается по протоколу IPFIX (NetFlow v10) на выделенный сервер или VM, где установлена база данный QoE Stor и GUI. Данное решение позволяет эффективно хранить и осуществлять поиск в NAT log.

CG-NAT + DPI

Мы предлагаем совместить функционал CG-NAT с DPI на одном устройстве, чтобы получить возможность не только транслировать адреса, но также распознавать и классифицировать трафик по протоколам и направлениям, использовать полисинг общего канала, размечать трафик, работать со статистикой (Full NetFlow и Clickstream).

Дополнительная информация об абонентах используется в отделах продаж, маркетинга и технической поддержки.

CG-NAT + DPI + BNG

Наиболее выгодный вариант — совместить функциональность CG-NAT, DPI и BNG на одном устройстве и таким образом построить гибкое и легко управляемое ядро сети — это значительно сокращает совокупную стоимость владения (TCO, Total Cost of Ownership) за счет компактности, высокой производительности, единообразного управления и эксплуатации.

В данной схеме, помимо трансляции сетевых адресов и глубокого анализа трафика также реализована авторизация IPoE/PPPoE абонентов, BGP/OSPF, интеграция с биллингом (AAA) осуществляется через PCRF.

Возможности CG-NAT от VAS Experts

Full Cone NAT

В функции CG-NAT используется технология Full Cone NAT, разрешающая отправку пакетов, приходящих с любой внешней системы, по внешнему отображаемому порту TCP/UDP, который представляет собой источник трафика от абонента.

Hairpinning

Абоненты внутри NAT обращаются к публичным адресам друг друга без трансляции и пересылки пакетов за пределы устройства.

Лимиты на TCP- и UDP-соединения для абонента

Для каждого пула IP-адресов индивидуально устанавливается лимит на количество TCP- и UDP-соединений для абонента, что позволяет оператору экономно распределять ресурсы адресного пространства между корпоративными и частными клиентами. При отсутствии активности неиспользуемые соединения закрываются, высвобождая порты.

Paired IP address pooling

Все соединения абонента с одного приватного адреса привязываются к одному публичному IP-адресу.

Журналирование трансляций

Сетевые трансляции записываются в текстовый файл или передаются на внешний коллектор по протоколу IPFIX (известному также, как NetFlow v10).

Прозрачность для P2P и онлайн-игр

Предсказуемое поведение NAT обеспечивается функциями Full Cone и HairPinning. Пользовательские квоты обеспечивают равномерное распределение публичных IP-портов между абонентами, а вирусы и вредоносные программы не могут истощить их ресурсы.

Поддержка ALG

Для операторов важно поддерживать связность для всех прикладных услуг и пользователей, обеспечивая при этом целостность приложений. ALG следят за тем, чтобы протоколы — такие, как FTP, TFTP, RTSP, PPTP, SIP, ICMP, H.323, ESP, MGCP и DNS — оставались работоспособными. Многие устаревшие реализации NAT не обеспечивают такого уровня прозрачности.

Поддержка VLAN и On-Stick

В CG-NAT поддержка VLAN экономит порты в оборудовании оператора и повышает эффективность использования NIC. Благодаря этому возможно определение входящего и исходящего трафика не по NIC, а по VLAN ID, что в свою очередь создает возможность использовать одну и ту же сетевую карту и для входящего, и для исходящего трафика. Эта опция особенно эффективна, когда используется вместе с LACP.

LACP

Link Aggregation Control Protocol позволяет объединять несколько физических портов для формирования единого логического канала и повышения отказоустойчивости.

Высокая доступность

Надежность решения гарантируется при помощи резервных режимов Active-Standby и Active-Active. В обоих вариантах задействовано два устройства: если первое (активное) выходит из строя, то трафик переключается на второе без потерь с помощью протоколов маршрутизации.