Межсетевые экраны с возможностями NAT

- Используемая терминология и основные понятия
  - Частные и внешние сети
  - Понятие сессии
  - Шлюз прикладного уровня (ALG)
- Статическое и динамическое назначение адресов
- Варианты выполнения NAT
  - Традиционный (или исходящий) NAT
  - Двунаправленный (Two-Way) NAT
  - Двойной NAT
- Сеть с частными адресами и туннели
  - Туннелирование преобразованных пакетов
  - Магистральные (Backbone) разделенные на сегменты частные сети
- Свойства NAT
  - Поддержка FTP
  - Приложения с несколькими взаимозависимыми сессиями

Частные и внешние сети

- **Адресной областью** будем называть такую совокупность адресов, в которой дейтаграммы могут маршрутизироваться к любому хосту, адрес которого принадлежит данной области. Для этого как минимум необходимо, чтобы каждый хост в адресной области имел уникальный IP-адрес.
- **Внешней** или публичной **сетью** будем называть сеть, в которой все хосты имеют уникальные сетевые адреса, которые назначены IANA или другой регистрирующей организацией. В терминологии NAT такая сеть часто называется внешней сетью.
- **Частной сетью** будем называть сеть, в которой хосты имеют зарезервированные для частных сетей адреса. В RFC 1918 для частных сетей определены три диапазона IP-адресов:
  - С 10.0.0.0 по 10.255.255.255 (10.0.0.0/8 в CIDR нотации)
  - С 172.16.0.0 по 172.31.255.255 (172.16.0.0/12 в CIDR нотации)
  - С 192.168.0.0 по 192.168.255.255 (192.168.0.0/16 в CIDR нотации)
- Эти адреса могут использоваться во многих организациях независимо друг от друга.
- Однако, если в дальнейшем эти организации решат взаимодействовать друг с другом или с публичным интернетом, они либо должны назначить новые адреса во всех своих сетях, либо использовать **NAT на граничных маршрутизаторах**.

Частные и внешние сети

- Термин «**прозрачная маршрутизация**» используется для описания маршрутизации, выполняемой NAT.
- **Традиционная маршрутизация**, выполняемая традиционными маршрутизаторами, отличается тем, пакеты маршрутизируются **внутри одной области адресов**.
- Прозрачная маршрутизация означает **маршрутизацию дейтаграммы между различными адресными областями**, при которой выполняется модификация адреса в IP-заголовке таким образом, чтобы он принадлежал области адресов, в которой дейтаграмма маршрутизируется.
- Маршрутизатор NAT расположен на границе между двумя областями адресов и преобразует адреса в IP-заголовках таким образом, что пакет корректно маршрутизируется при переходе из одной области в другую.
- Маршрутизатор NAT имеет соединения с несколькими областями адресов, при этом он не должен распространять некорректную для области информацию (например, посредством протоколов маршрутизации) о сетях из одной области адресов в другую.
- **Прозрачная маршрутизация между хостами в частной области и внешней области** – основная функция маршрутизатора NAT.

Частные и внешние сети

- NAT обеспечивает возможность прозрачной маршрутизации к хостам из различных адресных областей.
- Это достигается **изменением адреса отправителя и поддержкой информации об этом изменении таким образом, чтобы дейтаграммы для этой сессии маршрутизировались бы нужному отправителю из этой области**.
- Данное решение можно использовать только в том случае, если приложения не используют IP-адреса в протоколе более высокого уровня.
- Например, идентификация конечных точек с помощью DNS-имен, а не IP-адресов делает приложения менее зависимыми от реальных адресов, которые использует NAT, и не приводит к необходимости также изменять и содержимое, когда NAT изменяет IP-адрес.
- Трансляция адресов позволяет хостам в частной сети прозрачно взаимодействовать с получателем во внешней сети и наоборот.
- Существуют различные варианты NAT, терминология преобразования адресов в этих случаях может несколько отличаться.
- NAT рассматривается исключительно **для IPv4**.

Частные и внешние сети

- Функциональность NAT не может быть прозрачной для всех приложений, и по этой причине она часто используются вместе со шлюзом прикладного уровня (**ALG**).
- При принятии решения о развертывании NAT необходимо **определить требования приложений** и оценить необходимость развертывания дополнений к NAT (например, ALG), чтобы обеспечить прозрачность преобразования NAT для приложений.
- ***Стандартные режимы IPSec, в которых IP-адреса конечных точек не изменяются, не работают с NAT. Такие протоколы как AH и ESP защищают содержимое IP-заголовков от изменения, а одна из основных функций NAT как раз и состоит в изменении адресов в IP-заголовке пакета.***

Частные и внешние сети

- Несмотря на частую путаницу понятий, **NAT не является частью функциональности в межсетевом экране, относящейся к безопасности**.
- Свойство NAT, относящееся к безопасности, – обеспечение того, что хосты с внешней стороны межсетевого экрана не могут инициировать соединение с хостом, расположенным позади NAT.
- Другой способ добиться того же самого можно с помощью политик межсетевого экрана, которые в той или иной степени отслеживают состояния.
- Однако использование NAT в межсетевом экране обычно означает, что **нет необходимости конфигурировать политику, которая обеспечивает аналогичную защиту**, поэтому часто считается, что NAT выполняет функцию безопасности.

Частные и внешние сети

- Другим примером, когда NAT взаимосвязан с политикой безопасности, является возможность *идентификации источника трафика* в логах межсетевого экрана.
- Если используется NAT, он должен **записывать в логи частный адрес**, а не публичный адрес, на который NAT изменил частный.
- В противном случае в логах будут некорректно определяться многие хосты, которые будут представлены там единственным публичным адресом.
- В простейшем случае NAT представляет собой маршрутизатор, у которого существует сеть с частными адресами внутри и единственный публичный адрес снаружи.

Частные и внешние сети

NAT выполняет **преобразование частных адресов в один публичный адрес**. Способ этого отображения один-ко-многим зависит от реализации, но всегда включает следующее:

- Для хостов из внутренней сети, инициализирующих соединения ко внешней сети, выполняется преобразование **IP-адреса и порта источника** на другой IP-адрес и порт источника, которые определяются NAT.
- Затем NAT использует обратное преобразование IP-адреса и номеров портов для пересылки пакетов из внешней сети к хосту во внутреннюю сеть.
- **Хосты из внешней сети не могут инициировать соединения к внутренней сети**.
- В некоторых межсетевых экранах NAT может предоставлять доступ к определенным хостам внутри частной сети.

Понятие сессии

- Сессия характеризуется тем, что можно точно определить пакет, являющийся началом сессии, и, как правило, существует несколько пакетов, которые говорят о завершении сессии.
- **Направление, в котором передается первый пакет сессии, определяет направление всей сессии**.
- Можно считать, что **сессия – это совокупность трафика, который обрабатывается как единое целое**.
- TCP/UDP сессии однозначно определяются IP-адресом и портом источника и IP-адресом и портом получателя.
- Сессии ICMP-запросов определяются IP-адресом источника, ID ICMP-запроса и IP-адресом получателя.
- Все остальные сессии характеризуются IP-адресами источника и получателя и IP-протоколом.

Понятие сессии

- Трансляция адресов, выполняемая NAT, основана на сессии и включает **преобразование входящих и исходящих пакетов, принадлежащих сессии**.
- Заметим, что не гарантируется, что понятие сессии, определяемое для NAT, полностью совпадает с понятием сессии в приложении.
- Приложение может считать несколько сессий (с точки зрения NAT), которые **с точки зрения приложения** связаны между собой, как единую сессию или может не рассматривать свое взаимодействие с противоположной стороной как сессию.
- Для преобразования NAT важно отслеживать **инициализацию** и **завершение сессий**.

Понятие сессии

- Первый пакет TCP-сессии содержит информацию о начале сессии.
- Первый пакет TCP-сессии можно распознать по наличию бита **`SYN`** и отсутствию бита **`ACK`** во флагах TCP. Все TCP-пакеты, за исключением первого пакета, должны иметь установленный бит **`ACK`**.
- Однако не существует заранее определенного способа распознать начало **UDP-сессии** или любой не-TCP-сессии.
- Можно предложить **эвристический подход**, при котором предполагается, что первый пакет с несуществующими на текущий момент параметрами сессии начинает новую сессию.
- **Завершение TCP-сессии** происходит при получении флага **`FIN`** обеими сторонами сессии или когда одна из сторон посылает пакет с флагом **`RST`**.
- Однако при выполнении NAT, так как невозможно знать, что пакеты действительно доставлены получателю (они могут быть отброшены между хостом, выполняющим NAT, и получателем), невозможно точно знать, что пакеты, содержащие **`FIN`** или **`RST`**, будут последними пакетами в сессии (так как могут быть повторные передачи).
- Следовательно, надо предполагать, что сессия завершена только по истечении 4 минут (2 * на максимальное время жизни пакета) с момента определения завершения.

Понятие сессии

- Возможно, что TCP-сессия будет завершена без обнаружения этого события устройством, выполняющим NAT (например, в случае перезапуска одной или обеих сторон).
- Следовательно, **сбор мусора** является необходимым сервисом NAT, чтобы очистить неиспользуемые соединения.
- Однако в общем случае невозможно различить соединение, по которому долгое время ничего не передается, от соединений, которые больше не существуют.
- В случае **UDP-сессий** не существует единственного способа определить завершения сессии, так как это во многом зависит от приложения.
- Для определения завершения сессии используются различные **эвристические подходы**.
- Можно предположить, что TCP-сессии, которые не используются, скажем, в течение 24 часов, и не-TCP-сессии, которые не используются в течение пары минут, завершены.
- Часто такие предположения верные, но могут существовать случаи, когда предположения оказались неверными.

Понятие сессии

- Период простоя может существенно отличаться как от приложения к приложению, так и от сессии к сессии в одном приложении.
- Следовательно, **таймауты сессии должны быть конфигурируемы**.
- Но даже и в этом случае нет гарантии, что может быть найдено приемлемое значение.
- Не существует также гарантии, что завершенная с **точки зрения NAT** сессия будет завершенной **с точки зрения приложения**.
- Другим способом обработки завершения сессии является использование записей с отметкой времени, которые будут храниться как можно дольше, удаляться в случаи необходимости будет только самая старая простаивающая сессия.

Шлюз прикладного уровня (ALG)

- Не для всех приложений можно использовать NAT без дополнительных преобразований в пакете; в частности, это касается тех приложений, которые используют **IP-адреса и TCP/UDP порты в содержимом пакета**.
- Одним из решений прохождения NAT является использование шлюза прикладного уровня (**ALG**).
- ALG является **прикладным агентом**, который позволяет приложению, выполняющемуся на хосте в одной адресной области, прозрачно взаимодействовать с противоположной стороной, выполняющейся на хосте в другой области.
- **ALG должен взаимодействовать с NAT**, чтобы установить состояние NAT, использовать информацию состояния NAT, модифицировать специфичное для приложения содержимое или выполнить что-то еще, что необходимо для выполнения приложения при пересылке пакетов из одной адресной области в другую.

Шлюз прикладного уровня (ALG)

- **ALG аналогичны прокси** в том смысле, что и тот, и другой расположены между клиентом и сервером.
- Прокси используют специальный протокол для взаимодействия с клиентом и пересылке данных серверу и наоборот.
- В отличие от прокси **ALG не используют специальный протокол** и **не требуют никаких изменений в прикладных клиентах**.

Статическое и динамическое назначение адресов

- NAT является методом, с помощью которого выполняется преобразование IP-адресов при пересылке пакета из одной области адресов в другую, обеспечивая прозрачную маршрутизацию между конечными хостами.
- Существует много различных **способов** преобразования адресов.
- Тем не менее, все технологии NAT должны разделять следующие **характеристики**.

1. **Прозрачное** для протоколов маршрутизации и конечных хостов назначение адресов.
2. Возможность выполнять **обычную маршрутизацию** после преобразования адресов (маршрутизация здесь означает пересылку пакетов, а не обмен информацией маршрутизации).
3. Согласованное преобразование содержимого **пакета ICMP-error**.

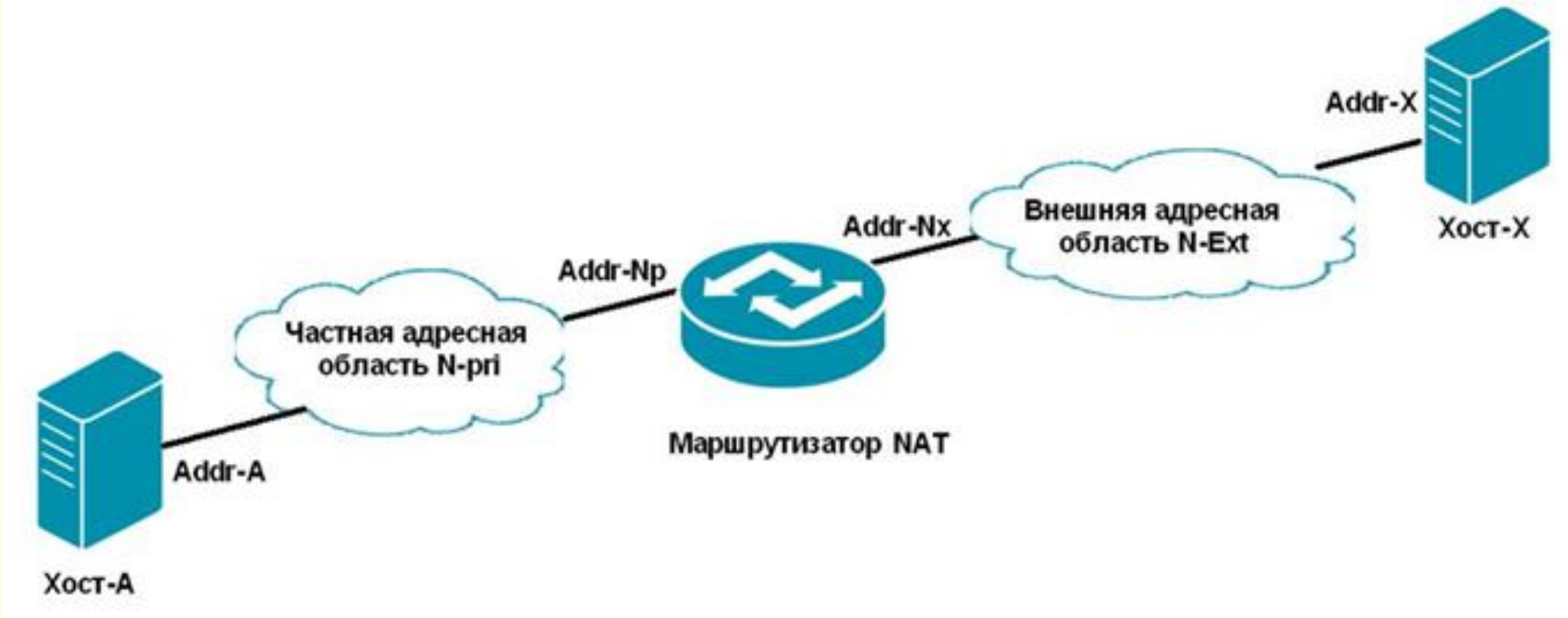
Статическое и динамическое назначение адресов

- NAT преобразует адреса в частной сети в адреса во внешней сети для обеспечения прозрачной маршрутизации дейтаграмм между разными адресными областями.
- В некоторых случаях преобразование может быть сделано и для идентификаторов транспортного уровня (такие как порты TCP/UDP).
- Преобразование адреса выполняется при инициализации сессии.
- Может существовать два способа назначения адресов.
- При **статическом назначении адреса** существует отображение один-к-одному между адресами частной сети и адресами внешней сети в течение всего времени функционирования NAT.

Статическое и динамическое назначение адресов

- Внешние адреса могут назначаться хостам в частной сети **динамически**.
- Когда сессия, для которой используются назначенные адреса, заканчивается, NAT освобождает внешний адрес, чтобы в дальнейшем он мог опять использоваться для другого хоста из частной сети.
- Конкретный способ такого связывания специфичен для каждой реализации NAT.

Варианты выполнения NAT



Варианты выполнения NAT

- **Хост-А** с адресом **Addr-A** расположен в области с частными адресами, которая обозначена как сеть **N-Pri**.
- **N-Pri** изолирована от внешней сети с помощью маршрутизатора NAT.
- **Хост-Х** с адресом **Addr-X** расположен во внешней области, обозначенной как сеть **N-Ext**.
- Маршрутизатор NAT имеет два интерфейса, каждый из которых соединен с соответствующей областью.
- Интерфейсу к внешней области назначен адрес **Addr-Nx**, интерфейсу к частной области назначен адрес **Addr-Np**.
- Адреса **Addr-A** и **Addr-Np** принадлежат сети **N-Pri**, а адреса **Addr-X** и **Addr-Nx** принадлежат сети **N-Ext**.

Традиционный (или исходящий) NAT

- Традиционный NAT позволяет хостам в частной сети прозрачно получать доступ к хостам во внешней сети.
- В традиционном NAT **сессия может существовать только в одном направлении**, исходящим из частной сети.
- Это отличает его от двунаправленного NAT, который допускает сессии как во входящем, так и в исходящем направлениях.
- Рассмотрим свойства области, в которой выполняется традиционный NAT.
- IP-адреса хостов **во внешней сети являются уникальными** и доступными как во внешней, так и в частной сети.
- Однако адреса хостов в частной сети являются **уникальными только внутри этой частной сети** и не являются доступными во внешней сети.
- Другими словами, NAT ничего не сообщает внешней области о частной сети. Но частная сеть может иметь информацию о сетях во внешней области.
- Адреса, используемые в частной сети, не должны перекрываться с внешними адресами. Любой адрес должен являться **либо частным адресом, либо внешним**.

Традиционный (или исходящий) NAT

- Традиционный маршрутизатор NAT разрешает **`Хост-А`** инициировать сессию к **`Хост-Х`**, но не наоборот.
- Также **`N-Ext`** является маршрутизируемой из **`N-Pri`**, в то время как **`N-Pri`** не может быть маршрутизируема из **`N-Ext`**.
- Традиционный NAT первоначально использовался в тех случаях, когда хостам с частными адресами необходимо было разрешить исходящие сессии.
- Существует два варианта традиционного NAT, называемые базовым **NAT и NAPT** (Network Address Port Translation).

Традиционный (или исходящий) NAT

Базовый NAT

- Для исходящих из частной сети пакетов преобразуются IP-адрес источника и относящиеся к этому поля, такие как контрольные суммы заголовков IP, TCP, UDP и ICMP.

NAPT

- NAPT дополнительно **преобразует идентификатор транспорта**, такой как **номера портов** TCP и UDP.
- NAPT позволяет большому числу хостов разделять **единственный внешний адрес**.
- NAPT может быть скомбинирован с базовым NAT таким образом, чтобы использовался пул внешних адресов совместно с преобразованием портов.
- Маршрутизатор NAPT может быть сконфигурирован для преобразования сессий из **`N-Pri`** в единственный внешний адрес, например, **`Addr-i`**.
- Очень часто адрес внешнего интерфейса **`Addr-Nx`** маршрутизатора NAPT используется в качестве адреса, в который отображается **`N-Pri`**.

Традиционный (или исходящий) NAT

Использование IP-адреса интерфейса в качестве IP-адреса источника

- При установлении нового соединения для него по таблице маршрутизации определяется выходной интерфейс.
- При выполнении преобразования адресов IP-адрес этого интерфейса используется в качестве нового IP-адреса источника. Этот способ преобразования используется чаще всего.

Традиционный (или исходящий) NAT

Использование выделенного IP-адреса в качестве IP-адреса источника

- В качестве нового IP-адреса источника может быть указан выделенный IP-адрес. Для этого необходимо, чтобы этот IP-адрес был опубликован **протоколом ARP** на выходном интерфейсе, так как в противном случае возвращаемые пакеты не будут получены межсетевым экраном. Этот метод используется, когда **IP-адрес источника должен отличаться от адреса интерфейса**.

Традиционный (или исходящий) NAT

Использование IP-адреса из NAT-пула

- В качестве IP-адреса источника может использоваться NAT-пул – диапазон IP-адресов, определенный администратором сети.
- В этом случае в качестве IP-адреса NAT будет использовать очередной доступный IP-адрес из пула.
- Причем **NAT-пулов** может существовать **несколько**.
- А также один NAT-пул может быть использоваться в более чем одном NAT-правиле.
- NAT-пулы обычно применяются, если требуется создать **много уникальных подключений** используя один порт.

Традиционный (или исходящий) NAT

- Межсетевой экран обычно может поддерживать до 65 000 соединений с уникальной комбинацией из IP-адреса источника и IP-адреса назначения.
- Большее количество портов может потребоваться, если много клиентов одновременно должны иметь доступ в интернет через прокси-сервер.
- Проблема с ограниченным количеством портов решается с помощью выделения **дополнительных внешних IP-адресов** для выхода в интернет и использования NAT-пулов для создания новых соединений с использованием этих IP-адресов.

Традиционный (или исходящий) NAT

Типы NAT-пулов

- Существует три типа NAT-пулов, каждый из которых производит распределение новых подключений разными способами:

- **Stateful (с поддержкой состояния)**
- **Stateless (без поддержки состояния)**
- **Fixed (Фиксированный)**

Традиционный (или исходящий) NAT

NAT-пулы типа Stateful

- При использовании NAT-пула *Stateful*, каждому соединению назначается IP-адрес из пула, через который в настоящий момент осуществляется наименьшее количество соединений.
- Во всех последующих соединениях **с тем же внутренним хостом** будет использоваться **тот же самый IP-адрес**.
- **Преимуществом** данного подхода является обеспечение сбалансированной нагрузки нескольких внешних каналов связи интернет-провайдера по количеству соединений и гарантия того, что информация от внешнего хоста всегда вернется обратно на IP-адрес отправителя, что может быть важно в таких протоколах как HTTP.
- **Недостатком** является требование дополнительных ресурсов памяти для отслеживания соединения в таблице состояний, а также накладные расходы, связанные с обработкой данных в процессе установления нового соединения.

Традиционный (или исходящий) NAT

- Для того чтобы таблица состояний не содержала записей о неактивных соединениях, можно установить время активного состояния соединения (State Keepalive) – **время неактивности подключения** в секундах, по истечении которого, запись об этом подключении будет удалена из таблицы состояний.

- По прошествии данного периода система считает, что исходящих соединений от данного хоста создаваться больше не будет.

- В случае, если запись о состоянии подключения из таблицы удалена, то последующие подключения данного хоста будут заноситься в новую запись таблицы и могут иметь другой внешний IP-адрес из NAT-пула.

Традиционный (или исходящий) NAT

- Так как таблица состояний расходует ресурсы памяти, существует возможность ограничить ее размер, используя параметр **`Max States`** объекта NAT-пул.
- Таблица состояний формируется не сразу, она увеличивается в размере по мере необходимости.
- Одна запись в таблице состояний отображает все соединения одного хоста за межсетевым экраном, независимо от того, к какому внешнему хосту данное соединение относится.
- Если размер таблицы состояний достиг значения параметра **`Max States`**, в таблице перезаписывается то состояние, у которого самое длительное время неактивности.
- Если все состояния из таблицы активны, тогда новое соединение игнорируется.
- Значение параметра **`Max States`** должно быть не меньше количества локальных хостов или клиентов, имеющих доступ к интернету.

- В каждом NAT-пуле есть только одна таблица соответствий, поэтому, если один NAT-пул несколько раз используется в разных IP-правилах NAT, то они будут совместно использовать одну и ту же таблицу состояний.

Традиционный (или исходящий) NAT

NAT-пулы типа Stateless

- Если выбран тип NAT-пула *Stateless*, это означает, что таблица состояний не формируется, для каждого нового соединения будет использоваться новый IP-адрес из пула, через который осуществляется наименьшее количество соединений.
- В результате этого два разных соединения от одного внутреннего хоста к одному и тому же внешнему хосту могут использовать два разных внешних IP-адреса источника.
- **Преимуществом** NAT-пула с типом *Stateless* является то, что он обеспечивает эффективное распределение новых соединений между внешними IP-адресами без лишних затрат памяти на формирование таблицы состояний.
- Помимо этого, время на обработку данных при установлении каждого нового соединения сокращается.
- **К недостаткам** способа относится то, что он не подходит для подключений, требующих наличия постоянного внешнего IP-адреса.

Традиционный (или исходящий) NAT

NAT-пулы типа Fixed

- Если выбран тип NAT-пула *Fixed*, то каждому внутреннему хосту поставлен в соответствие один из внешних IP-адресов.
- Такое соответствие создается с помощью алгоритма хеширования.
- Хотя администратор не имеет возможности контролировать, какое из внешних подключений будет использоваться, такой подход гарантирует, что определенный внутренний хост всегда будет обмениваться информацией через один и тот же внешний IP-адрес.

- **Преимуществом** типа *Fixed* является то, что он не требует ресурсов памяти на создание таблицы состояний и обеспечивает очень высокую скорость обработки данных при установлении нового соединения.

Двунаправленный (Two-Way) NAT

- При двунаправленном NAT сессии могут инициализироваться как с хостов из внешней сети, так и с хостов из частной сети.
- Прозрачная маршрутизация для сессий, начинающихся с хостов из внешней сети, может быть реализована несколькими способами.

Первый способ. NAT должен быть сконфигурирован таким образом, чтобы отображать определенный порт получателя на конкретный хост и порт за NAT.

Например, все HTTP-запросы, которые приходят на NAT, могут быть перенаправлены на один хост, расположенный в защищенной межсетевым экраном сети.

Данная технология иногда называется ***pinholing*** или ***проброс портов***.

Например, если политикой требуется, чтобы все HTTP-сервера, доступные извне, были расположены в DMZ, то один из способов сделать – это определить в NAT возможность pinholing на TCP-порт 80.

Второй способ. Хосту в частной сети (**`Хост-А`**) может быть назначен IP-адрес, доступный из внешней сети.

Двунаправленный (Two-Way) NAT

- Двунаправленный маршрутизатор NAT позволяет **Хост-А** инициировать сессию к **Хосту-Х**, и **Хост-Х** инициировать сессию к **Хосту-А**, если **Хост-А** доступен либо первым, либо вторым способом.
- Также как и в случае традиционного NAT **N-Ext** является маршрутизируемой из **N-Pri**, но **N-Pri** остается не маршрутизируемой из **N-Ext**.
- Рассмотрим особенности реализации второго способа создания двунаправленного NAT, когда хост в частной сети имеет IP-адрес из внешней сети.

Двунаправленный (Two-Way) NAT

- NAT-маршрутизатор является узлом, который расположен на границе между частной и внешней областями и имеет возможность выполнять маршрутизацию пакетов из внешней области в частную область.
- В случае двунаправленного NAT пакеты могут как исходить от **Хоста-А**, так и быть направлены к **Хосту-А**.
- **Хост-А** при соединении с хостом во внешней области имеет IP-адрес из внешнего пространства адресов.
- После этого никакой другой хост в частном или внешнем домене не может иметь тот же самый адрес.

Двунаправленный (Two-Way) NAT

Обсудим возможные способы маршрутизации, которые могут иметь место внутри частной области.

1. На маршрутизаторе должен быть явно прописан маршрут к **Хосту-А**.
2. Если указание такого маршрута вызывает проблемы, то может быть использовано туннелирование.

Один из возможных подходов состоит в установке туннеля между **Хостом-А** и NAT-маршрутизатором, соединяющим две адресные области.

Пакеты к **Хосту-А** и от **Хоста-А** могут быть туннелированы, но пакеты между NAT-маршрутизатором и удаленным получателем будет пересылаться в обычном виде.

Туннель от **Хоста-А** к пограничному маршрутизатору может и не требоваться.

Как правило туннель бывает необходим, если межсетевой экран фильтрует пакеты, в которых адрес получателя принадлежит внешней сети.

- Например, если **Хост-А** имеет адрес **Addr-k** из внешней области, что означает возможность создания сессий от **Addr-X** к **Addr-k**.
- Если **Addr-k** не маршрутизируется внутри частной сети, то для прохождения пакетов внутри частной области можно создать туннель.

Двунаправленный (Two-Way) NAT

Могут существовать и другие подходы.

1. **Хосту-А** назначается адрес из внешней области для взаимодействия с хостами из этой области.

Такой адрес может быть связан статически или получаться динамически (с помощью заранее определенного протокола) от узла, который может назначать адреса из внешней области.

Маршрутизатору NAT назначен адрес внешней области.

2. Выполняется маршрутизация пакетов к внешним хостам, используя маршрутизатор NAT в качестве шлюза. **Хосту-А** может потребоваться возможность функционирования в качестве конечной точки туннеля для инкапсуляции пакетов для их пересылки и выполнять обратную де-туннелирование при получении.

   - Маршрутизатор NAT принадлежит адресному пространству как в частной, так и во внешней областях и выполняет маршрутизацию пакетов из внешней области в частную область.

Двунаправленный (Two-Way) NAT

- Маршрутизатор NAT должен иметь следующие характеристики:

1. Должен быть маршрутизатором, соединенным как с частной, так и с внешней областью адресов.
2. Должен иметь возможность обеспечивать маршрутизацию пакетов из внешней области в частную область.
3. Маршрутизатор должен иметь возможность быть конечной точкой туннеля с **Хостом-А**.

Он будет де-туннелировать исходные пакеты, исходящие от **Хоста-А**, и перенаправлять их внешним хостам.

На обратном пути он создает туннель для **Хоста-А**, основываясь на адресе получателя исходного пакета, и инкапсулировать пакет в туннель для перенаправления его к **Хосту-А**.

Двунаправленный (Two-Way) NAT

- Возможен другой вариант, при котором несколько частных хостов используют единственный внешний адрес, но имеют различные идентификаторы транспортного уровня (т.е. номера портов TCP/UDP и ICMP Query ID).
- В этом случае **Хост-А** может быть определен аналогично предыдущему случаю с той разницей, что **Хост-А** указывает пару (внешний адрес, идентификатор транспорта) при соединении с хостом во внешней области.
- При этом взаимодействие с внешними узлами для **Хоста-А** может быть ограничено TCP-, UDP- и ICMP-сессиями.
- Маршрутизатор NAT аналогичен предыдущему случаю в том, что он должен маршрутизировать пакеты из внешней области к **Хосту-А** внутри частной области.
- Обычно маршрутизатор NAT также назначает параметры транспорта для **Хоста-А**.

Двунаправленный (Two-Way) NAT

- В примере **Хост-А** получает параметры (**Addr-Nx**, TCP-порт **T-Nx**) от маршрутизатора NAPT.
- Пересылка пакетов между конечными точками внутри частной области может быть проиллюстрирована следующим образом.
- При использовании первого метода внешний заголовок исходящего пакета от **Хоста-А** использует (частный адрес **Addr-A**, порт источника **T-Na**) в качестве параметров источника для взаимодействия с **Хостом-Х**.
- Маршрутизатор NAPT преобразует эти параметры в (**Addr-Nx**, порт **T-Nxa**).

Двойной NAT

- Двойной NAT является вариантом NAT, в котором **адреса как источника, так и получателя модифицируются NAT** при пересечении дейтаграммой границы пространства адресов.
- Это отличает его от традиционного NAT и двунаправленного NAT, в которых преобразуется только один адрес.
- Двойной NAT необходим, когда в частной и внешней областях есть коллизия адресов.
- В большинстве случаев это происходит, когда внутренние хосты имеют внешние адреса, которые не являются уникальными во внешней области.

Двойной NAT

- В качестве примера можно привести случай, когда внешний адрес хоста должен был бы измениться при переходе от одного провайдера к другому, но при этом желательно иметь возможность оставить этот внешний адрес прежним.
- Основной проблемой в этом случае является то, что адрес некоторого хоста во внешней области может быть точно таким же, что и адрес нашего хоста внутри частной области.
- Если данный адрес появляется в пакете в частной сети, он должен быть в определенных случаях перенаправлен внутреннему хосту, а не через преобразование NAT во внешнюю область.
- Двойной NAT является мостом для подобных областей, преобразуя как адрес источника, так и адрес получателя в IP-пакете.
- Маршрутизатор двойного NAT будет позволять **`Хосту-A`** инициировать сессии к **`Хосту-X`**.
- Тем не менее **`N-Ext`** (или подмножество **`N-Ext`**) не маршрутизируемо внутри **`N-Pri`**, и **`N-Pri`** не маршрутизируемо из **`N-Ext`**.

Ограниченность NAT

- Существует много **ограничений** на использование NAT.
- Например, запросы и ответы, относящиеся к сессии, **должны маршрутизироваться через один и тот же маршрутизатор NAT**, так как маршрутизатор NAT поддерживает информацию о состоянии сессий, установленных через него.
- По этой причине часто предполагается, что маршрутизаторы NAT расположены на границе в том месте, где все IP-пакеты выходят из домена и поступают в домен.
- Однако такая конфигурация означает, что маршрутизатор **NAT является единой точкой отказа**.
- Для того чтобы гарантировать в частной сети, что соединение с внешней сетью будет поддерживаться, даже если один из маршрутизаторов NAT откажет, часто требуется иметь несколько соединений частной сети с одним или несколькими сервис-провайдерами.
- Причем реализация NAT на каждом маршрутизаторе может быть как одинаковой, так и разной.

Ограниченность NAT

- Например, частная сеть может иметь связь с двумя различными провайдерами, и сессии от частных хостов могут проходить через маршрутизатор NAT с лучшей метрикой до получателя.
- Когда происходит сбой в одном из маршрутизаторов NAT, другой может выполнять маршрутизацию трафика для всех соединений.
- NAT от нескольких производителей или несколько экземпляров от одного и того же производителя NAT, разделяя общую конфигурацию NAT, могут обеспечивать **отказоустойчивость** друг для друга.
- В этом случае необходимо выполнять **резервное копирование NAT** для обмена информацией о состоянии таким образом, чтобы можно было прозрачно загружать сессию при сбоях первичного NAT.
- Резервное копирование NAT выполняется проще, когда конфигурация основана на статическом отображении.

Сеть с частными адресами и туннели

- Рассмотрим случай, когда сеть с частными адресами должна быть соединена с внешней сетью через туннель.
- В этом случае туннель инкапсулирует трафик, который может как содержать, так и не содержать преобразованные пакеты, в зависимости от характеристик адресных областей, с которыми соединен туннель.
- Обсудим два сценария, когда туннели используются

1. **Совместно с преобразованием адресов.**
2. **Без преобразования адресов.**

Туннелирование преобразованных пакетов

- Все варианты преобразования адресов, которые обсуждались ранее, могут применяться не только к прямым соединениям, но и к туннелям и VPN.
- Например, сеть, соединяющая локальные сети деловых партнеров через **VPN**, может использовать традиционный NAT.
- Также возможно использовать двойной NAT, если адресные пространства локальных сетей перекрываются.
- Преобразование NAT может выполняться на одном конце туннеля или на обоих концах.
- Во всех случаях трафик через VPN может быть для обеспечения безопасности зашифрован. Безопасность здесь означает только безопасность при передаче по VPN.
- Безопасность между конечными точками не обеспечивается. Это означает, что частные сети должны быть доверяемыми.

Магистральные (Backbone) разделенные на сегменты частные сети

- Существует много примеров, когда частная сеть (такая как сеть корпорации) состоит из отдельных подсетей, расположенных в разных местах, и использует публичную сеть для взаимодействия между ними.

- В таких случаях нежелательно выполнять преобразование адресов, как потому что большому числу хостов может потребоваться взаимодействие через основную сеть, что потребует большой таблицы адресов, так и потому, что будет большое число приложений, которые зависят от сконфигурированных адресов, что затруднит работу **DNS-сервера**.

- Будем называть такую частную сеть магистральной, разделенной на сегменты, (backbone-partitioned) частной сетью.

- Тупиковые сети, соединенные с магистральной сетью, разделенной на сегменты, должны быть построены точно также, как если бы они были соединены с обычной магистральной сетью.

- Это означает, что пограничный маршрутизатор должен поддерживать маршруты к частным сетям во всех сегментах. При этом публичные основные сети могут не поддерживать маршруты ко всем локальным адресам.

- Следовательно, при использовании NAT пограничные маршрутизаторы должны туннелировать трафик, используя VPN, через основные сети.

- Чтобы сделать это, преобразование NAT следует выполнять для частных адресов, а глобальные адреса использовать для туннелирования.

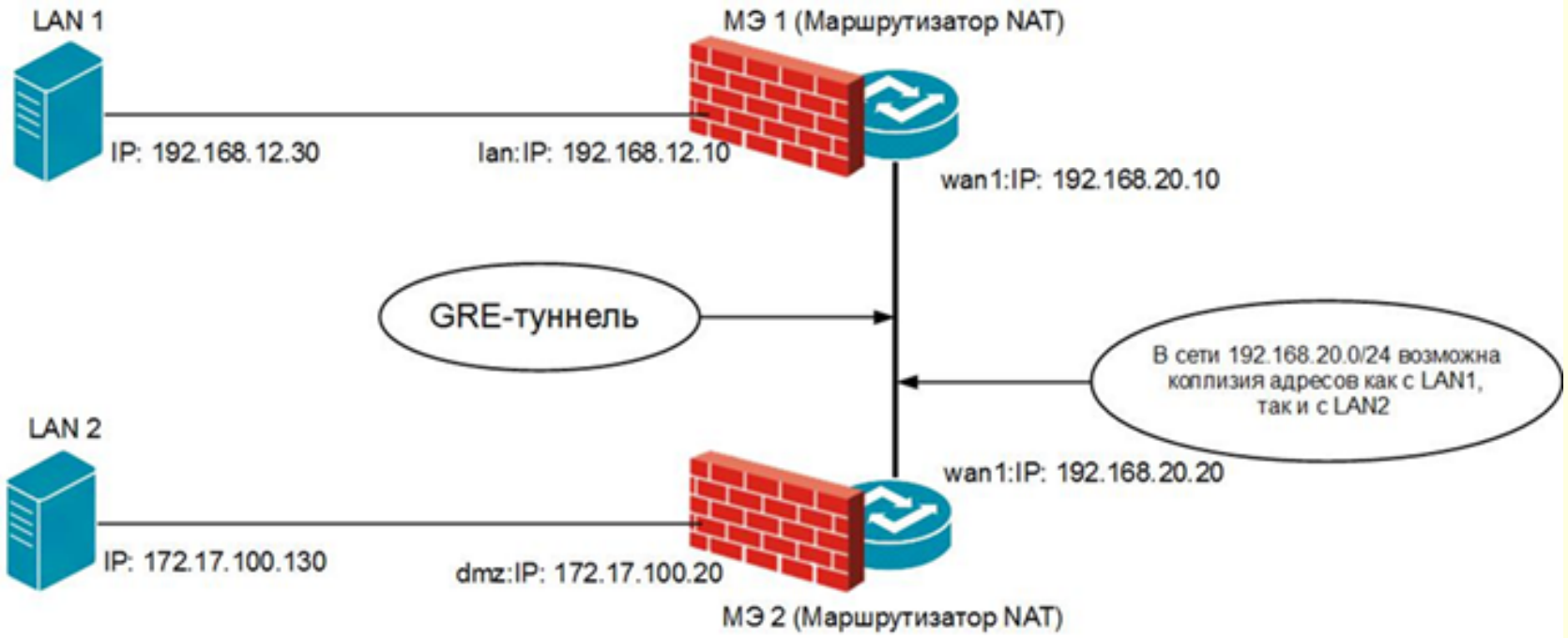
Магистральные (Backbone) разделенные на сегменты частные сети

- Если необходимо доставить пакет из тупикового сегмента **X** в тупиковый сегмент **Y**, то преобразование NAT для сегмента **X** инкапсулирует пакет в IP-заголовок с адресом получателя, установленным в глобальный адрес устройства, выполняющего NAT для сегмента **Y**.

- Когда преобразование NAT для сегмента **Y** получает пакет с этим адресом получателя, NAT де-капсулирует IP-заголовок и перенаправляет пакет во внутреннюю сеть.

- В этом случае может как происходить преобразование адреса, так и не происходить, т.е. будет выполняться простая пересылка пакетов из одной частной сети в другую по внешней сети посредством туннеля.

Магистральные (Backbone) разделенные на сегменты частные сети



Необходимо соединить две локальные сети через магистральную сеть, в которой возможна коллизия адресов как с локальной сетью **LAN 1**, так и с локальной сетью **LAN 2**.

Самым простым решением в этом случае является использование GRE-туннеля.

Свойства NAT

- При преобразовании NAT должны изменяться только заголовки IP/TCP/UDP/ICMP и ICMP-сообщения **`error`**.
- Преобразование NAT (за исключением ALG) не анализирует и не изменяет содержимое прикладного уровня. По этой причине в большинстве случаев **преобразование NAT прозрачно для приложений**.
- Тем не менее существуют **две проблемы**, из-за которых преобразование NAT может вызывать трудности:

1) Если содержимое транспортного уровня содержит IP-адрес.
2) Когда необходимо обеспечить безопасность до конечных точек.

Свойства NAT

- **Технологии безопасности прикладного уровня**, которые не зависят от IP-адресов (т.е. TLS и SSH), работают корректно вместе с NAT.
- В отличие от этого **технологии безопасности на транспортном уровне**, такие как IPSec, могут иметь проблемы при использовании NAT.
- В транспортном режиме IPSec как AH, так и ESP обеспечивают проверку целостности всего содержимого. Если преобразование NAT модифицирует адрес, то проверка целостности не пройдет.

Свойства NAT

- Заметим, что ESP в туннельном режиме допустимо, так как преобразование не затрагивает внешний IP-заголовок.
- Преобразование NAT также влияет на инфраструктуры открытых ключей, такие как DNSSec и сертификаты X.509. В случае DNSSec каждый **`RRset`** DNS подписан ключом своей зоны.
- Аутентичность ключа проверяется с помощью цепочки доверия, которая устанавливается от корневого DNS.
- Когда DNS-ALG модифицирует адреса (например, как в случае двойного NAT), проверка подписей не проходит.
- Интересно заметить, что IKE является протоколом уровня сессии, основанном на UDP и не защищенном IPSec.
- Защищены только отдельные части содержимого внутри IKE. Как результат IKE-сессии проходят через NAT, кроме того, также содержимое IKE не содержит адресов или идентификаторов транспорта, специфичных для той или иной области.

Поддержка FTP

- Рассмотрим, как FTP может поддерживаться NAT. FTP ALG является составной частью большинства реализаций NAT.
- Некоторые производители включают дополнительные ALG для поддержки других приложений.
- Команда **`PORT`** и ответ **`PASV`** в содержимом сессии протокола FTP содержит IP-адрес и TCP-порт, который участники должны использовать при передаче данных.
- Для успешного прохождения NAT требуется FTP ALG для просмотра и изменения содержимого управляющей сессии таким образом, чтобы информация содержимого соответствовала параметрам конечных точек.
- ALG должен также взаимодействовать с NAT таким образом, чтобы NAT мог установить информацию о состоянии FTP-сессии для данных.

Поддержка FTP

- Так как адрес и TCP-порт представлены в ASCII кодировке, в результате может измениться размер пакета.
- Например, «**`10,18`**»– это 5 символов ASCII, а «**`110,118`**»– это 7 символов ASCII.
- Если новый размер совпадает с тем, который был до преобразования, то необходимо только изменить контрольную сумму TCP.
- Если же новый размер меньше или больше, чем до преобразования, то необходимо также поменять последовательный номер TCP, чтобы отобразить изменение длины в управляющем потоке FTP.
- ALG может использовать специальную таблицу, чтобы корректировать последовательный номер и номер подтверждения в TCP.
- Причем это необходимо делать **для всех последующих пакетов в соединении**.

Приложения с несколькими взаимозависимыми сессиями

- Преобразование NAT выполняется в предположении, что каждая сессия является независимой.
- Такие характеристики сессии, как ориентация сессии, IP-адреса источника и получателя, протокол сессии, идентификаторы отправителя и получателя транспортного уровня определяются независимо в начале каждой новой сессии.
- Однако существуют приложения, такие как **H.323**, которые используют одну или более управляющих сессий для установки характеристик последующих сессий.
- Такие приложения требуют специальных ALG, которые интерпретируют и при необходимости преобразуют содержимое.

Анализ логов

- При использовании NAT существует возможность неправильной интерпретации адресов, которые будут записаны в логи.
- Например, один и тот же частный адрес может быть связан в разное время с разными внешними адресами и наоборот, один и тот же внешний адрес может быть в разное время связан с разными частными хостами.
- В результате этого анализ трафика, основанный исключительно на внешних адресах и номерах портов, может привести к неправильным выводам.
- Если некоторый хост атакует другие хосты в интернете, может быть трудно определить его источник, потому что IP-адрес хоста скрыт за маршрутизатором NAT.