Network Working Group
Request for Comments: 2663
Category: Informational

P. Srisuresh
M. Holdrege
Lucent Technologies

August 1999

Транслятор сетевых адресов IP (NAT) - терминология и рассмотрение

IP Network Address Translator (NAT) Terminology and Considerations

Статус документа

Этот документ содержит информацию для сообщества Internet и не определяет каких-либо стандартов. Документ может распространяться свободно.

Авторские права

Предисловие

Мотивом создания документа послужило желание внести ясность в терминологию, используемую в связи с трансляторами сетевых адресов (Network Address Translator). Сам термин «транслятор сетевых адресов» может относиться к разным субъектам в зависимости от контекста. Целью этого документа является определение различных вариантов NAT[1] и стандартизация значений применяемых терминов.

Указанные в списке авторы являются редакторами этого документа и обязаны отметить существенный вклад членов рабочей группы. Значительные фрагменты документа под названием IP Network Address Translator (NAT) были использованы почти дословно и обеспечили стартовую базу для этого документа. Редакторы рады поблагодарить авторов этого документа Pyda Srisuresh и Kjeld Egevang. Редакторы рады поблагодарить Praveen Akkiraju за его вклад в описание сценариев развёртывания NAT. Редакторы также выражают свою признательность членам IESG Scott Bradner, Vern Paxson и Thomas Narten за детальный анализ документа и улучшение текста.

Аннотация

NAT представляет собой метод отображения адресов IP из одного диапазона на адреса из другого диапазона в попытке обеспечить прозрачную маршрутизацию к хостам. Традиционно устройства NAT используются для подключения областей с изолированными приватными (не регистрируемыми) адресами к внешним областям, где применяются зарегистрированные адреса с глобальной маршрутизацией. В этом документе предпринимается попытка описать работу устройств NAT и связанные с этим вопросы, а также определить термины, используемые для идентификации разных вариантов NAT.

1. Введение и обзор

Необходимость трансляции адресов IP возникает в тех случаях, когда внутренние IP-адреса сети не могут использоваться за пределами этой сети по причине того, что они недопустимы для внешнего применения, или требуется скрыть структуру частной сети от внешних сетей.

Трансляция адресов позволяет (во многих случаях, за исключением отмеченных в разделах 8 и 9) хостам частных сетей взаимодействовать с адресатами из внешних сетей и наоборот. Имеется множество вариантов NAT и связанных с ними терминов. Этот документ пытается определить терминологию, используемую для идентификации разных вариантов NAT. Рассматриваются также другие вопросы, относящиеся к устройствам NAT в целом.

Отметим, что документ не является описанием работы отдельных вариантов NAT или применимости устройств NAT.

Устройства NAT пытаются обеспечить прозрачную маршрутизацию для конечных хостов, пытающихся работать из областей с немаршрутизируемыми адресами. Это осуществляется путём замены адресов конечных узлов маршрута и поддержкой информации о таких заменах таким образом, чтобы относящиеся к сессии дейтаграммы корректно маршрутизировались нужным конечным узлам любых областей. Такое решение работает только для приложений, не использующих пространство адресом IP в качестве части самого протокола. Например, идентификация конечных точек с использованием имён DNS вместо адресов делает приложения менее зависимыми от реальных адресов, которые выбирает NAT и избавляет от необходимости преобразования содержимого дейтаграмм при изменении адресов IP с помощью NAT.

Функция NAT сама по себе не может обеспечит прозрачную поддержку всех приложений и часто требует применения дополнительных шлюзов прикладного уровня (ALG[2]). При возникновении потребности развернуть решение на основе NAT следует сначала определиться с требованиями приложений и оценить требуемые для обеспечения прозрачности расширения NAT (например, ALG).

Методы IPsec, предназначенные для сокрытия адресов конечных точек в пакетах IP в большинстве практических ситуаций не будут работать через NAT. Методы типа AH и ESP защищают содержимое заголовков IP (включая адреса отправителей и получателей) от изменения, а основной задачей NAT как раз является изменение адресов в заголовках IP.

[1] Network Address Translation - трансляция сетевых адресов.
[2] Application level gateway.

2. Терминология и используемые концепции

В этом разделе определяются термины, часто используемые в контексте NAT.

2.1. Область адресации (область)

Область адресации (address realm) представляет собой часть сети (домен), в которой обеспечивается уникальная адресация объектов, обеспечивающая возможность маршрутизации дейтаграмм между этими объектами. Используемые внутри домена протоколы маршрутизации отвечают за поиск маршрутов к объектам по сетевым адресам последних. Отметим, что этот документ ограничивается описанием NAT в среде IPv4 и не рассматривает NAT в других типах сред (например, IPv6).

2.2. Прозрачная маршрутизация

Термин «прозрачная маршрутизация» используется в этом документе для обозначения функциональности в части маршрутизации, обеспечиваемой устройством NAT. Это отличается от функциональности обычных маршрутизаторов, которые пересылают пакеты между областями с однотипной адресацией .

Прозрачная маршрутизация выполняется между областями с несовместимой маршрутизацией путём замены адресных полей в заголовках IP значениями, которые будут корректны в той области, куда направляется дейтаграмма. Более подробное описание прозрачной маршрутизации приведено в параграфе 3.2.

2.3. Сессии и потоки трафика

Поток соединения или сессии отличается от просто потока пакетов. Поток сессии показывает направление, в котором сессия была инициирована, относительно сетевого интерфейса. Поток пакетов представляет собой направление, в котором пакеты перемещаются относительно сетевого интерфейса. Рассмотрим в качестве примера исходящую сессию telnet. Такая сессия включает поток пакетов в обоих направлениях (входящие и исходящие). Исходящие пакеты передают информацию о нажатии клавиш, а входящие - содержимое «экрана» на сервере telnet.

В контексте данного документа сессией считается подмножество трафика, управляемое, как единица (элемент) трансляции. Сессии TCP/UDP однозначно идентифицируются квадруплетом (IP-адрес отправителя, порт TCP/UDP отправителя, IP-адрес получателя, порт TCP/UDP получателя). Сессии ICMP определяются тремя параметрами (IP-адрес отправителя, идентификатор запроса ICMP, IP-адрес получателя). Все остальные сессии идентифицируются тройкой параметров (IP-адрес отправителя и получателя, протокол IP).

Выполняемая NAT трансляция адресов происходит на уровне сессии и включает преобразование как входящих, так и исходящих пакетов для данной сессии. Направление сессии определяется направлением передачи первого пакета данной сессии (см. параграф 2.5).

Отметим, что определение сессии в контексте NAT не будет совпадать с представлениями о сессии в приложениях. Приложение может рассматривать группу сессий NAT, как одну прикладную сессию или даже не считать обмен пакетами между партнёрами какой-то сессией. Не все приложения могут работать в несовместимых областях адресации, даже при наличии ALG (определены в параграфе 2.9).

2.4. Порты TU, порты серверов и клиентов

В оставшейся части документа порты TCP/UDP, связанные с адресом IP, будут называться просто «портами TU».

Для большинства хостов TCP/IP диапазон портов TU с номерами 0-1023 используется серверами для прослушивания входящих вызовов. Инициирующие соединения клиенты обычно указывают номер порта-источника из диапазона 1024-65535. Однако это соглашение не является универсальным и выполняется не во всех случаях. Некоторые клиентские станции инициируют соединения, используя номер порта-источника из диапазона 0-1023, а некоторые серверы прослушивают порты TU с номерами из диапазона 1024-65535.

Список выделенных номеров портов TU можно найти в RFC 1700 [Ref 2].

2.5. Начало сессии для TCP, UDP и др.

Первый пакет каждой сессии TCP пытается организовать сессию и содержит стартовую информацию для соединения. Первый пакет сессии TCP можно распознать по наличию бита SYN и отсутствию бита ACK в поле флагов TCP. Во всех пакетах TCP, за исключением первого, флаг ACK должен быть установлен.

Однако не существует детерминированного метода детектирования начала сессий UDP или других протоколов, отличных от TCP. Эвристический метод будет полагать первый пакет с не существовавшими доселе параметрами сессии (определены в параграфе 2.3), как начальный пакет новой сессии.

2.6. Завершение сессии для TCP, UDP и др.

Завершение сессии TCP детектируется подтверждёнными FIN для обеих сторон или получением одной из сторон сегмента с битом RST в поле флагов TCP. Однако, поскольку устройство NAT не может знать о реальной доставке пакетов другой стороне (они могут быть отброшены на пути), оно не может быть уверенным в том, что сегменты с флагами FIN или RST[1] будут последними в сессии (т. е., возможен повтор передачи). Следовательно, считать сессию завершённой можно лишь по истечение 4 минут с момента обнаружения указанных выше событий. Необходимость столь длительного ожидания описана в RFC 793 [Ref 7], где предложено значение TIME-WAIT в 2 * MSL[2] (4 минуты).

Отметим, что возможны разрывы соединений TCP, которые устройство NAT не сможет детектировать (например, при перезагрузке одной из сторон). Следовательно, на устройствах NAT нужна «сборка мусора» для удаления несуществующих сессий TCP. Однако в общем случае нет возможности отличить простаивающее соединение от разорванного. Для сессий UDP нет однозначного способа детектировать разрыв сессии, поскольку протоколы на основе UDP существенно зависимы от приложений.

[1] В оригинале ошибочно сказано SYN. См. http://www.rfc-editor.org/errata_search.php?eid=400. *Прим. перев.*
[2] Maximum Segment Lifetime - максимальное время жизни сегмента.

Для детектирования завершение сессий применяется множество эвристических методов. Например, можно считать прерванными сессии TCP, бездействующие, более 24 часов, или сессии других протоколов, не используемые в течение нескольких минут. Зачастую такие предположения будут работать, но иногда нет. Интервалы допустимого бездействия очень сильно различаются между приложениями и даже для разных сессий одного приложения. Следовательно, значения тайм-аутов должны быть настраиваемыми. Но даже это не гарантирует удовлетворительного результата. Более того, как отмечено в параграфе 2.3, нет гарантии, что представление NAT о разрыве сессии совпадёт с представлением приложения.

Другим способом обработки разрыва сессий является введение временных меток и их хранение для определения возможных периодов бездействия.

2.7. Публичная/глобальная/внешняя сеть

Глобальная (Global) или публичная (Public) сеть представляет собой адресную область с уникальными для каждого узла адресами, выделенными IANA[1]) или другим регистратором. В контексте NAT такую сеть также будем называть внешней (External).

2.8. Частная/локальная сеть

Частная сеть представляет собой область адресации, которая не зависит от внешних сетевых адресов. Частные (Private) сети называют также локальными (Local). Прозрачная маршрутизация между частной сетью и внешними сетями облегчается за счёт использования NAT-маршрутизаторов.

В RFC 1918 [Ref 1] даны рекомендации по использованию адресного пространства в частных сетях. Агентство IANA выделило 3 блока адресов IP (10/8, 172.16/12, 192.168/16) для использования в частных сетях. В нотации, принятой до CIDR, первый блок является сетью класса A, второй представляет собой непрерывный блок из 16 сетей класса B, а третий - непрерывный блок из 256 сетей класса C.

Организация, решившая использовать в своей сети адреса из перечисленных блоков, может делать это без координации с IANA или иным регистратором, типа APNIC, RIPE и ARIN. Эти блоки адресов могут одновременно использоваться во множестве независимых организаций. Однако, если позднее такая организация пожелает организовать сетевое взаимодействие с другой организацией или подключиться к сети Internet, ей потребуется поменять блок адресов в своей сети или включить NAT на своих граничных маршрутизаторах.

2.9. Шлюзы прикладного уровня

Не все приложения легко перевести на работу через устройства NAT - в частности, это относится к приложениям, которые используют адреса IP и номера портов TCP/UDP в полях данных[2]. Шлюзы прикладного уровня (ALG[3]) обеспечивают функции специфических агентов трансляции, которые позволяют приложениям на хосте с адресом из одной области прозрачно подключаться к системам, работающим на хостах других адресных областей. ALG могут взаимодействовать с NAT для организации состояния, использовать информацию о состоянии NAT, менять содержимое полей данных прикладных пакетов и выполнять иные операции, которые могут потребоваться для работы через разнородные области адресации.

ALG могут использовать информацию о состоянии NAT не во всех случаях. Они могут подбирать данные приложений и просто сообщать NAT о необходимости добавить информацию о состоянии в некоторых случаях. Шлюзы ALG похожи на прокси (Proxy) в том, упрощают специфические для приложения коммуникации между клиентами и серверами. Прокси используют специальный протокол для коммуникаций с клиентами, транслируя данные клиентов на серверы, и наоборот. В отличие от прокси, шлюзы ALG не используют специальных протоколов для коммуникаций с клиентскими приложениями и не требуют внесения изменений в приложения-клиенты.

3. Что такое NAT?

Трансляция сетевых адресов (NAT[4]) представляет собой метод отображения адресов IP из одного блока на адреса из другого блока, обеспечивающий прозрачную маршрутизацию для оконечных хостов. Существует множество вариантов трансляции адресов, предназначенных для решения разных задач. Однако всем устройствам NAT следует поддерживать;

a) прозрачное выделение адресов;

b) прозрачную маршрутизацию через систему трансляции (маршрутизация в данном случае рассматривается, как пересылка пакетов, а не обмен маршрутными данными);

c) трансляция полей данных сообщений ICMP об ошибках.

На рисунке показано использование NAT в оконечном домене, подключённом к сети Internet через региональный маршрутизатор сервис-провайдера.

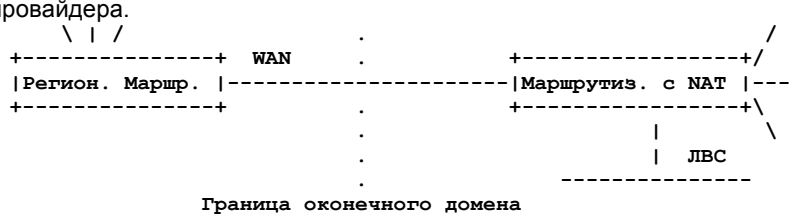


Рисунок 1. Типичный сценарий работы NAT.

[1]Internet Assigned Numbers Authority.
[2]Не в заголовках. *Прим. перев.*
[3]Application Level Gateway.
[4]Network Address Translation.

3.1. Прозрачное выделение адресов

NAT связывает адреса приватной сети с адресами глобальной сети и наоборот для обеспечения прозрачной маршрутизации дейтаграмм через границу адресных областей. В некоторых случаях трансляция может расширяться на идентификаторы транспортного уровня (например, номера портов TCP/UDP). Привязка адресов происходит в начале сессии. Ниже описаны два варианта выделения адресов.

3.1.1. Статическое выделение адресов

При статическом выделении адресов выполняется взаимно-однозначное (one-to-one) отображение между адресами хостов приватной сети и внешними сетевыми адресами на время действия операции NAT. При статическом выделении адресов не требуется управлять этим выделением в зависимости от потоков данных сессий.

3.1.2. Динамическое выделение адресов

В этом случае внешние адреса присваиваются хостам приватной сети (и наоборот) динамически на основе операционных требований и сеансовых потоков, эвристически определённых NAT. При завершении последней сессии, использовавшей привязку NAT будет освобождать данную привязку для последующего использования внешних адресов. Детали процесса выделения адресов зависят от конкретной реализации NAT.

3.2. Прозрачная маршрутизация

Маршрутизатор NAT размещается на границе между двумя адресными областями и транслирует адреса в заголовках пакетов IP так, чтобы при переходе пакета из одной адресной области в другую маршрутизация выполнялась корректно. Поскольку устройства NAT подключаются к нескольким адресным областям, они должны быть аккуратны в части распространения информации (например, через протоколы маршрутизации) о сетях из одной области в другую.

Трансляция адресов включает три фазы, описанные ниже. Суммарно эти три фазы обеспечивают создание, поддержку и удаление состояний для сессий, организуемых через устройства NAT.

3.2.1. Привязка адресов

В фазе привязки адресов локальны адрес IP связывается с внешним адресом (и наоборот) для последующей трансляции. Привязка адресов бывает статической при статическом распределении адресов и динамической (в начале сессии) при динамическом распределении. После связывания пары адресов все последующие сессии, исходящие от данного хоста или входящие к нему, будут использовать данную привязку для трансляции пакетов.

Новая привязка адресов организуется при старте новой сессии, если нужно привязки адресов не было организовано ранее. После того, как локальный адрес связан с внешним адресом, все последующие сессии, организуемые с этого адреса или направленные ему, будут использовать эту же привязку.

Начало каждой сессии будет приводить к организации состояния, позволяющего транслировать дейтаграммы этой сессии. Для одной адресной привязки может быть организовано множество сессий, организованных одним хостом.

3.2.2. Просмотр и трансляция адресов

После организации состояния для сессии для всех относящихся к ней пакетов будет выполняться просмотр адресов (в некоторых случаях идентификаторов транспортного уровня) и их трансляция.

Трансляция адреса и транспортного идентификатора для дейтаграммы будет приводить к соответствующему изменению адресной информации в заголовке.

3.2.3. Отвязывание адресов

Разрыв привязок (освобождение адресов) представляет собой фазу, когда приватный адрес перестаёт быть связанным с глобальным адресом для целей трансляции. NAT будет освобождать адреса по результатам принятия решения о разрыве последней из использовавших данную привязку сессий. Эвристические аспекты обработки разрыва сессий рассмотрены в параграфе 2.6.

3.3. Преобразование пакетов для сообщений об ошибках ICMP

Все сообщения ICMP об ошибках (за исключением сообщений типа Redirect) должны изменяться при прохождении через NAT. Типы сообщений ICMP об ошибках, которые нужно изменять при прохождении через NAT, включают Destination-Unreachable, Source-Quench, Time-Exceeded и Parameter-Problem. NAT не будет пытаться изменить сообщения типа Redirect.

Изменения в сообщениях ICMP будут включать модификацию исходного пакета IP (или его частей), вложенного в поле данных сообщения ICMP об ошибке. Для обеспечения полной прозрачности NAT с точки зрения конечных хостов адрес IP во вложенном в поле данных пакета ICMP заголовке IP должен быть изменён, а поле контрольной суммы этого заголовка IP рассчитано заново. То же самое относится и к заголовку транспортного уровня. Контрольная сумма заголовка ICMP также должна пересчитываться с учётом изменений адреса IP и транспортного заголовка в поле данных. Следовательно, обычный заголовок IP также требует изменений.

4.0. Варианты NAT

Существует множество вариантов трансляции адресов, рассчитанных для разных приложений. Перечисленные ниже варианты NAT не описывают всех ситуаций, но показывают существенные различия между вариантами.

Приведённая на рисунке схема будет служить базовой моделью для иллюстрации вариантов NAT. Host-A с адресом Addr-A размещается в приватной области, представленной сетью N-Pri. Сеть N-Pri отделена от внешних сетей маршрутизатором NAT. Host-X с адресом Addr-X размещается во внешней области, представленной сетью N-Ext. Маршрутизатор NAT с двумя интерфейсами, подключёнными к разным областям, обеспечивает прозрачную маршрутизацию между этими областями. Интерфейс во внешнюю сеть имеет адрес Addr-Nx, а приватный интерфейс - Addr-Np. Следует понимать, что адреса Addr-A и Addr-Np относятся к сети N-Pri, а Addr-X и Addr-Nx - к сети N-Ext.

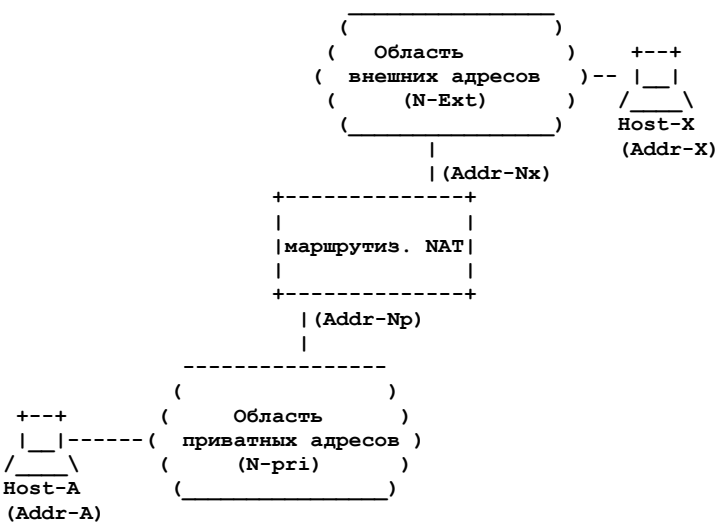


Рисунок 2. Базовая модель для иллюстрации NAT.

4.1. Traditional NAT (или) Outbound NAT

Традиционная (или исходящая) трансляция NAT обеспечивает хостам из приватной сети прозрачный доступ к хостам внешней сети для большинства случаев. В традиционной NAT сессии являются односторонними, исходящими из приватной сети. В отличие от этого Bi-directional NAT (двухсторонняя трансляция) поддерживает как исходящие, так и входящие сессии. Более подробное описание Bi-directional NAT приведено в параграфе 4.2.

Ниже описаны адресные области, поддерживаемые традиционной трансляцией NAT. IP-адреса хостов во внешней сети являются уникальными и корректны как во внешней, так и во внутренней сети. Однако адреса хостов из приватной сети уникальны лишь в рамках данной сети и могут быть не корректны для внешних сетей. Иными словами, NAT не будет анонсировать приватные сети во внешнюю область. Недопустимо перекрытие адресов внутренней сети с адресами из внешних сетей. Любой конкретный адрес должен относиться либо ко внешней, либо к приватной сети, но не может относиться к обеим сразу.

Традиционный маршрутизатор NAT на рисунке 2 будет позволять Host-A инициировать сессии с хостом Host-X, но не будет поддерживать вызовов в обратном направлении. Адреса N-Ext являются маршрутизируемыми внутри N-Pri, но адреса N-Pri не будут маршрутизироваться в N-Ext.

Traditional NAT обычно используется сайтами с адресами из приватных блоков для доступа во внешние сети.

Существует два варианта традиционной NAT - базовый (Basic NAT) и NAPT[1] (трансляция адресов и портов). Оба варианта рассматриваются в двух следующих параграфах.

4.1.1. Basic NAT

В Basic NAT для трансляции адресов хостов приватной сети используется блок внешних адресов при организации соединений из приватной сети со внешними доменами. Для исходящих из приватной сети пакетов IP-адрес отправителя и связанные поля типа контрольных сумм заголовков IP, TCP, UDP и ICMP соответствующим образом транслируются. Для принимаемых пакетов транслируется адрес получателя и указанные контрольные суммы.

Маршрутизатор Basic NAT на рисунке 2 может быть настроен на трансляцию N-Pri в блок адресов (например, Addr-i - Addr-n), выбранных из внешней сети N-Ext.

4.1.2. Трансляция адресов и номеров портов (NAPT)

NAPT расширяет трансляцию, добавляя возможность преобразования идентификаторов транспортного уровня (например, номера порта TCP или UDP, идентификатора запроса ICMP). Это позволяет мультиплексировать транспортные идентификаторы множества приватных хостов в транспортные идентификаторы одного внешнего адреса. NAPT позволяет множеству внутренних хостов пользоваться одним внешним адресом. Отметим, что NAPT может комбинироваться с Basic NAT, чтобы использовать блок внешних адресов вкупе с трансляцией портов.

Для исходящих из приватной сети пакетов NAPT будет транслировать IP-адрес и транспортный идентификатор отправителя, а также такие поля, как контрольные суммы заголовков IP, TCP, UDP и ICMP. Транспортными идентификаторами могут служить номера портов TCP/UDP или идентификаторы запросов ICMP. Для входящих пакетов будут транслироваться IP-адрес и транспортный идентификатор получателя, а также контрольные суммы заголовков.

Маршрутизатор NAPT на рисунке 2 можно настроить на трансляцию сессий, организованных из N-Pri, на один внешний адрес (например, Addr-i).

Зачастую при трансляции адресов N-Pri они отображаются на внешний адрес Addr-Nx маршрутизатора NAPT.

4.2. Bi-directional NAT (или) Two-Way NAT

При двухсторонней трансляции (Bi-directional NAT) сессии могут инициироваться как с хостов приватной сети, так и из внешней сети. Адреса приватной сети привязываются к уникальны в глобальном масштабе адресам статически или динамически при организации сессий в обоих направлениях. В пространстве имён (т. е., FQDN[2]) для хостов приватной и внешних сетей предполагается уникальность каждого имени. Хосты из внешней области получают доступ к хостам внутренней области, используя для преобразования имён в адреса систему DNS. В дополнение к Bi-Directional NAT требуется развёртывание DNS-ALG для корректного отображения адресов. В частности, с помощью DNS-ALG должна

[1]Network Address Port Translation.
[2]Fully Qualified Domain Name - полное доменное имя.

обеспечиваться возможность трансляции адресов из приватной области в запросах и откликах DNS на внешние привязки для этих адресов (и обратно) при прохождении пакетов DNS между приватной и внешней областями.

Требования к адресному пространству, отмеченные для Traditional NAT, применимы и в данном случае.

Маршрутизатор Bi-directional NAT на рисунке 2 позволит Host-A инициировать сессии с Host-X, а Host-X, в свою очередь - инициировать сессии с Host-A. Как и для традиционной трансляции NAT, адреса N-Ext будут маршрутизироваться в N-Pri, но адреса N-Pri не будут маршрутизироваться из N-Ext.

4.3. Twice NAT

Двойная трансляция (Twice NAT) - это вариант NAT, в котором устройство NAT при прохождении дейтаграммы через границу между сетями меняет адреса как отправителя, так и получателя. Этим данный вариант отличается от Traditional-NAT и Bi-Directional NAT, где преобразуется лишь один из адресов (отправителя или получателя, в зависимости от направления). Отметим, что термин Once-NAT (однократная трансляция) не используется.

Twice NAT требуется использовать в тех случаях, когда адресные пространства внешней и внутренней сети конфликтуют между собой[1]. Наиболее вероятно возникновение такой ситуации при некорректном применении во внутренней публичных адресов из блока, выделенного другой организации. Аналогичная ситуация может возникнуть и при смене организацией провайдера без замены внутренних адресов, выделенных прежним провайдером. Основной проблемой в таких случаях является совпадение части адресов внутренней и внешней сетей. При указании такого адреса в заголовке пакета этот пакет будет направлен скорей всего внутреннему хосту, а не на устройство NAT для трансляции. Twice-NAT пытается организовать мост между двумя областями путём трансляции адресов отправителя и получателя в пакетах IP при пересечении пакетом границы между областями.

Twice-NAT работает следующим образом. Когда Host-A инициирует сессию с Host-X, он отправляет запрос DNS для имени Host-X. Система DNS-ALG перехватывает запрос DNS и в отклике возвращаемом на хост Host-A меняет адрес Host-X на адрес, для которого обеспечивается корректная маршрутизация на локальном сайте (например, Host-XPRIME). После этого Host A инициирует взаимодействие с Host-XPRIME. Когда пакеты проходят через устройство NAT, IP-адрес отправителя транслируется (как в Traditional NAT), а адрес получателя транслируется в адрес Host-X. Аналогичные преобразования выполняются для пакетов, приходящих от Host-X.

Далее описываются свойства адресных областей, поддерживаемых Twice-NAT. Адреса хостов внешней сети уникальны в рамках этой сети, но могут иметь совпадения с адресами внутренней сети. Аналогично, адреса хостов приватной сети уникальны внутри этой сети, но могут совпадать со внешними адресами. Иными словами, по адресам хостов нет возможности определить принадлежность ко внутренней или внешней сети. Трансляция Twice NAT не допустима для анонсирования локальных сетей во внешние и обратно.

Маршрутизатор Twice NAT на рисунке 2 будет позволять Host-A инициировать сессии с Host-X, а Host-X - инициировать сессии с Host-A. Однако сеть N-Ext (или подмножество N-Ext) не будет маршрутизироваться из сети N-Pri, а сеть N-Pri не будет маршрутизироваться из N-Ext.

Twice NAT обычно используется в тех случаях, когда адресное пространство внутренней сети пересекается с адресным пространством внешней сети. Например, на приватном сайте, использующем блок адресов 200.200.200.0/24, официально выделенный другому сайту во внешней сети. Предположим, что Host_A (200.200.200.1) из приватной сети Private пытается связаться с Host_X (200.200.200.100) во внешней сети Public. Для организации такого соединения адрес Host_X отображается на другой адрес для Host_A (и обратно). Двойную трансляцию на граничном маршрутизаторе сети Private можно настроить следующим образом:

```
Private -> Public : 200.200.200.0/24 -> 138.76.28.0/24
Public <- Private : 200.200.200.0/24 -> 172.16.1.0/24
Поток дейтаграмм  : Host_A(Private) ->  Host_X(Public)
```

a) В приватной сети

```
DA: 172.16.1.100      SA: 200.200.200.1
```

b) После трансляции twice-NAT

```
DA: 200.200.200.100    SA: 138.76.28.1
```

Поток дейтаграмм Host_X (Public) -> Host_A (Private)

a) В публичной сети

```
DA: 138.76.28.1       SA: 200.200.200.100
```

b) В приватной сети после трансляции twice-NAT

```
SA: 200.200.200.1     DA: 172.16.1.100
```

4.4. Multihomed NAT

При использовании NAT возникают некоторые ограничения. Например, запросы и отклики, относящиеся к одной сессии, должны маршрутизироваться через одно устройство NAT, поскольку маршрутизатор NAT поддерживает информацию о состоянии организованных через него сессий. По этой причине часто предполагается, что маршрутизатор NAT является единственным краевым маршрутизатором оконечного домена и все пакеты IP при междоменных коммуникациях проходят через этот маршрутизатор NAT.

Для того, чтобы обеспечить приватной сети доступ во внешние сети даже при отказе одного из каналов NAT, желательно сделать приватную сеть многодомной с каналами к одному или нескольким провайдерам. Такие соединения могут быть организованы через одно или разные устройства NAT.

Например, приватная сеть может иметь соединения с двумя провайдерами и сессии хостов этой сети будут проходить через маршрутизаторы NAT с выбором лучшей метрики на пути к адресату. При отказе одного из маршрутизаторов NAT оставшийся может маршрутизировать трафик для всех соединений.

[1] Не обеспечивается уникальности адресов. *Прим. перев.*

Множество устройств NAT или множество каналов на одном устройстве NAT, использующих общие настройки NAT, могут обеспечивать резервирование один для другого. В таких случаях резервное устройство NAT должно обмениваться данными с активным маршрутизатором NAT, чтобы при возникновении в том отказа сессии автоматически переносились на резервное устройство. Работа с резервным устройством NAT упрощается при использовании статических отображений.

5.0. Специфические для области адреса IP (RSIP)

Аббревиатура RSIP[1] используется для обозначения функциональности (осведомленного о наличии областей) хоста из приватной сети принимать специфический для области адрес IP для взаимодействия с хостом приватной или внешней области.

Клиентом RSIP считается хост в приватной сети, принимающий адрес из внешней области при соединении с хостами из этой области. Пакеты, генерируемые хостами с обеих сторон такого соединения, будут использовать адреса, являющиеся уникальными для внешней области и не требующие трансляции.

Сервером RSIP считается узел, который входит как в приватную, так и во внешнюю сеть и может маршрутизировать пакеты из внешней сети в приватную сеть. Такие пакеты могут исходить от клиента RSIP или быть направленными клиенту RSIP. Сервер RSIP может также служить узлом, выделяющим адреса из внешней области клиентам RSIP.

Существует два варианта RSIP - RSA-IP[2] и RSAP-IP[3], которые описаны ниже.

5.1. Специфический для области адрес (RSA-IP)

Клиент RSA-IP принимает адрес IP из внешнего адресного пространства при соединении с хостом из внешней области. После того, как клиент RSA-IP примет внешний адрес, ни один другой хост приватной или внешней сети не сможет принимать этот адрес, пока он не будет освобождён клиентом RSA-IP.

Ниже приводится обсуждение вариантов маршрутизации, с помощью которых может быть реализована сквозная маршрутизация пакетов RSA-IP в приватной сети. Одним из вариантов является туннелирование пакетов до адресата. Внешний заголовок может транслироваться NAT, как обычно, не оказывая влияния на адресацию во внутреннем заголовке. Другим вариантом является организация двухстороннего туннеля между клиентом RSA-IP и граничным маршрутизатором, соединяющим две адресных области. Пакеты к клиенту и от него будут туннелироваться, но пересылка пакетов между граничным маршрутизатором и удаленным получателем будет происходить, как обычно. Отметим, что туннель от клиента к граничному маршрутизатору не является обязательным. Можно просто пересылать пакеты напрямую. Это будет работать, если во внутренней сети не используется фильтрации пакетов по адресам отправителей (которые в данном случае будут из внешней сети).

Например, Host-A на рисунке 2 может принять адрес Addr-k из внешней области и действовать, как клиент RSA-IP, чтобы обеспечить возможность организации сквозных сессий между Addr-k и Addr-X. Прохождение пакетов через приватную область можно проиллюстрировано ниже.

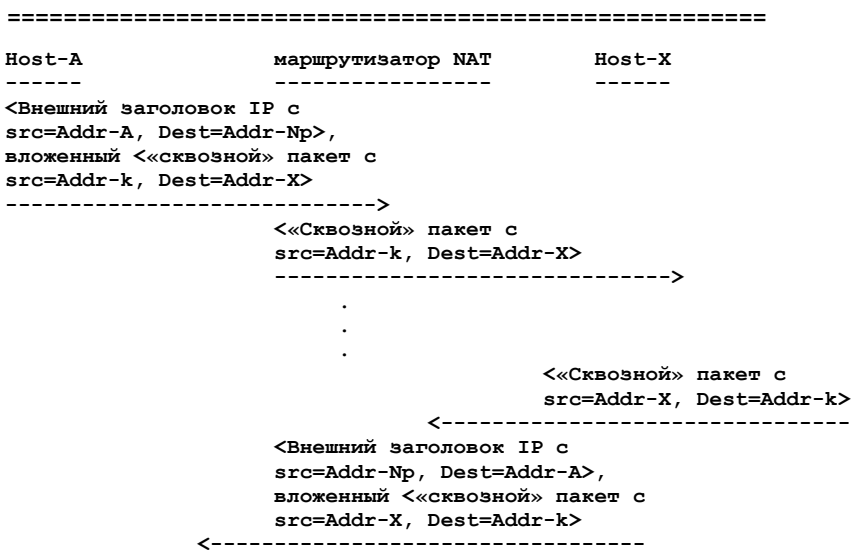
Первый метод использует трансляцию на маршрутизаторе NAT.

```
=======================================================

Host-A               маршрутизатор NAT        Host-X
------               -----------------        ------
<Внешний заголовок IP с
src=Addr-A, Dest=Addr-X>,
вложенный <«сквозной» пакет с
src=Addr-k, Dest=Addr-X>
------------------------------>
                     <Внешний заголовок IP с
                     src=Addr-k, Dest=Addr-X>,
                     вложенный <«сквозной» пакет с
                     src=Addr-k,  Dest=Addr-X>
                     --------------------------->
                          .
                          .
                          .
                                      <Внешний заголовок IP с
                                      src=Addr-X, Dest=Addr-k>,
                                      вложенный <«сквозной» пакет с
                                      src=Addr-X, Dest=Addr-k>
                                <---------------------------------
                     <Внешний заголовок IP с
                     src=Addr-X, Dest=Addr-A>,
                     вложенный <«сквозной» пакет с
                     src=Addr-X, Dest=Addr-k>
            <---------------------------------------
```

[1]Realm Specific IP.
[2]Realm Specific Address IP.
[3]Realm Specific Address and port IP.

Второй метод использует туннель внутри приватной области.



Могут использоваться и другие варианты.

Ниже приведены характеристики клиента RSA-IP. Набор выполняемых клиентом RSA-IP операций может быть обозначен термином RSA-IP.

1. Осведомлен об областях, в которых могут размещаться партнерские узлы.
2. Принимает адрес из внешней области при взаимодействии с хостами из данной области. Адрес может присваиваться статически или выделяться динамическими (протокол будет определён) узлом, способным выделять адреса из внешней области. Распределение адресов из внешней области может координировать сервер RSA-IP.
3. Маршрутизирует пакеты внешним хостам, используя подходящий сервер RSA-IP. В любом случае клиент RSA-IP будет служить конечной точкой туннеля, инкапсулирующей пакеты для сквозной пересылки и декапсулирующей возвращаемые пакеты.

Сервер RSA-IP представляет собой узел, подключенный к приватной и внешней сети, который обеспечивает маршрутизацию пакетов из внешней области клиентам RSA-IP в приватной области. Сервер RSA-IP можно описать следующими характеристиками.

1. Может обеспечивать статическое или динамическое выделение адресов из внешней области клиентам RSA-IP.
2. Должен быть маршрутизатором, подключённым к приватной и внешней области адресов.
3. Должен обеспечивать механизм маршрутизации пакетов из внешней области внутри приватной области. Описаны два варианта такой маршрутизации.

   В первом варианте сервер RSA-IP должен быть устройством NAT с прозрачной маршрутизацией по внешним заголовкам. В этой модели внешний партнёр должен быть конечной точкой туннеля.

   Во второй модели сервером RSA-IP может служить любой маршрутизатор (независимо от NAT), который может быть конечной точкой туннеля к клиенту RSA-IP. Маршрутизатор будет детуннелировать сквозные пакеты, идущие наружу от клиентов RSA-IP, и пересылать их внешним хостам. На пути возврата маршрутизатор будет находить туннель с клиентом RSA-IP по адресу получателя в сквозном пакете и инкапсулировать пакеты для пересылки клиенту RSA-IP.

Клиенты RSA-IP могут применять любые методы IPsec (а именно, транспортный или туннельный режим с поддержкой аутентификации и шифрования на основе заголовков AH и ESP во вложенных пакетах). Для инкапсуляции между клиентом RSA-IP и сервером RSA-IP или внешним хостом могут применяться любые методы туннелирования. Например, инкапсуляция в туннельном режиме IPsec является корректным типом инкапсуляции, которая обеспечивает аутентификацию и шифрование IPsec для вложенных сквозных пакетов.

5.2 Специфический для области адрес и порт (RSAP-IP)

RSAP-IP является вариантом RSIP, в котором множество хостов приватной области может использовать один внешний адрес с мультиплексированием по идентификаторам транспортного уровня (номерам портов TCP/UDP, ICMP Query ID).

Клиент RSAP-IP может быть определён по аналогии с клиентом RSA-IP, но при соединении с хостами внешней области он получает не только адрес, но и идентификатор транспортного уровня. В связи с этим коммуникации клиентов RSAP-IP с внешними областями могут быть ограничены сессиями TCP, UDP и ICMP.

Сервер RSAP-IP похож на сервер RSA-IP в том, что он обеспечивает маршрутизацию внешних пакетов, адресованных клиентам RSAP-IP в приватной области. Обычно сервер RSAP-IP будет также присваивать клиентам пары адрес-транспортный идентификатор.

Маршрутизатор NAPT может работать в качестве сервера RSAP-IP, когда внешняя инкапсуляция основана на TCP/UDP и пакеты передаются между клиентом RSAP-IP и внешним партнёром. В этой модели внешний партнёр должен быть конечной точкой туннеля TCP/UDP. Клиенты RSAP-IP могут использовать любые методы IPsec (а именно, транспортный или туннельный режим с поддержкой аутентификации и шифрования на основе заголовков AH и ESP во вложенных пакетах). Отметим, однако, что туннельный режим IPsec не является подходящим типом инкапсуляции, поскольку маршрутизатор NAPT не может обеспечить прозрачной маршрутизации для протоколов AH и ESP.

В другом варианте пакеты могут туннелироваться между клиентом и сервером RSAP-IP, а сервер будет детуннелировать пакеты от клиентов RSAP-IP и пересылать их внешним хостам. На обратном пути сервер RSAP-IP будет находить туннель с клиентом RSAP-IP по паре (адрес - порт получателя) и инкапсулировать исходный пакет в туннель для пересылки клиенту RSAP-IP. В этом варианте не возникает ограничений на методы туннелирования между клиентом и сервером RSAP-IP. Однако здесь возникают ограничения на сквозное использование защиты на основе IPsec. В транспортном режиме может быть обеспечена аутентификация и защита целостности. Однако конфиденциальность защитить не удастся, поскольку сервер RSAP-IP должен иметь доступ к транспортному идентификатору получателя для определения туннели RSAP-IP. По этой причине через сервер RSAP-IP в этом варианте могут проходить только пакеты TCP, UDP и ICMP в транспортном режиме IPsec с защитой AH и ESP.

Прохождение пакетов через приватную область проиллюстрировано ниже. В первом варианте внешний уровень исходящего от Host-A пакета использует пару (приватный адрес Addr-A, порт отправителя T-Na) для взаимодействия с Host-X. Маршрутизатор NAPT транслирует эту пару в (Addr-Nx, Port T-Nxa). Трансляция не зависит от параметров адресации клиента RSAP-IP, указанных во вложенном пакете.

В первом варианте используется маршрутизатор NAPT для трансляции:

```
=======================================================

Host-A               маршрутизатор NAT        Host-X
------               -----------------        ------
<Внешний пакет TCP/UDP с
src=Addr-A, Src Port=T-Na, Dest=Addr-X>,
вложенный <«сквозной» пакет с
src=Addr-Nx, Src Port=T-Nx, Dest=Addr-X>
---------------------------->
                     <Внешний пакет TCP/UDP с
                     src=Addr-Nx, Src Port=T-Nxa, Dest=Addr-X>,
                     вложенный <«сквозной» пакет с
                     src=Addr-Nx, Src Port=T-Nx, Dest=Addr-X>
                     ---------------------------------------->
                          .
                          .
                          .
                                        <Внешний пакет TCP/UDP с
                                        src=Addr-X, Dest=Addr-Nx, Dest Port=T-Nxa>,
                                        вложенный <«сквозной» пакет с
                                        src=Addr-X, Dest=Addr-Nx, Dest Port=T-Nx>
                                  <---------------------------------
                     <Внешний пакет TCP/UDP с
                     src=Addr-X, Dest=Addr-A, Dest Port=T-Na>,
                     вложенный <«сквозной» пакет с
                     src=Addr-X, Dest=Addr-Nx, Dest Port=T-Nx>
            <-----------------------------------
```

Во втором варианте организуется туннель в приватной области:

```
=======================================================

Host-A               маршрутизатор NAT        Host-X
------               -----------------        ------
<Внешний заголовок IP с
src=Addr-A, Dest=Addr-Np>,
вложенный <«сквозной» пакет с
src=Addr-Nx, Src Port=T-Nx, Dest=Addr-X>
---------------------------->
                     <«сквозной» пакет с
                     src=Addr-Nx, Src Port=T-Nx, Dest=Addr-X>
                     ------------------------------->
                          .
                          .
                          .
                                        <«сквозной» пакет с
                                        src=Addr-X, Dest=Addr-Nx, Dest Port=T-Nx>
                                  <---------------------------------
                     <Внешний заголовок IP с
                     src=Addr-Np, Dest=Addr-A>,
                     вложенный <«сквозной» пакет с
                     src=Addr-X, Dest=Addr-Nx, Dest Port=T-Nx>
            <-----------------------------------
```

6.0. Приватные сети и туннели

Рассмотрим ситуацию с подключением приватной сети к внешнему миру через туннель. В этом случае инкапсулированный в туннель трафик может включать транслированные пакеты в зависимости от параметров соединяемых туннелем областей адресации.

Ниже рассмотрены использования туннелей (a) с трансляцией адресов и (b) без таковой.

6.1. Туннелирование транслированных пакетов

Все рассмотренные выше варианты трансляции адресов могут применяться как для физических каналов, так и для туннелей или VPN[1].

Например, приватная сеть, подключённая к деловому партнёру через облако VPN, может применять традиционную NAT для обмена информацией с партнёром. При пересечении адресных пространств в сетях партнёров можно

[1]Virtual private network - виртуальная частная сеть.

воспользоваться Twice NAT. Устройство NAT может быть установлено как на одной стороне туннеля, так и на обоих его концах. Во всех случаях трафик через VPN может шифроваться для обеспечения его защиты в сети VPN. Для сквозной защиты трафика потребуется использование в приватной сети доверенного устройства NAT.

6.2. Приватные сети, сегментированные магистралями

Во многих случаях приватная сеть (например, сеть компании) территориально распределена и использует публичные сетевые магистрали для связи между разнесёнными фрагментами сети. В таких случаях трансляция адресов нежелательна поскольку через магистрали могут взаимодействовать многочисленные хосты (это потребует поддержки очень больших таблиц состояний), а также по причине того, что многие приложения настраиваются на работу с конкретными адресами без использования серверов имён. Такие сети будем называть «сегментированными магистралями приватными сетями».

Сегментированным магистралями оконечным сетям следует вести себя так, как будто они не сегментированы. Т. е., маршрутизаторам в каждом сегменте следует поддерживать маршруты к адресным блокам всех сегментов. Маршруты к этим адресам не будут, естественно, поддерживаться (публичными) магистралями. Следовательно, граничным маршрутизаторам следует поддерживать туннели (с помощью VPN) через магистрали, используя инкапсуляцию. Для решения этой задачи каждому устройству NAT будет нужен внешний адрес, через который будут создаваться туннели.

Когда NAT-устройство x в оконечном сегменте X желает доставить пакет в оконечный сегмент Y, оно будет инкапсулировать пакет с указанием во внешнем заголовке глобального IP-адреса NAT-устройства y. Когда NAT-устройство y получит пакет со своим адресом во внешнем заголовке, оно будет декапсулировать пакет и пересылать его адресату в своей локальной сети. Отметим, что в этом случае трансляция адресов не используется и пакеты приватной сети просто туннелируются через магистраль.

7.0. Рабочие характеристики NAT

Устройства NAT не осведомлены о приложениях, поскольку трансляции ограничены заголовками IP/TCP/UDP/ICMP и сообщениями ICMP об ошибках. Устройства NAT не меняют данных в пакетах, поскольку содержимое полей данных зависит от приложений.

Устройства NAT (не включая ALG) не проверяют и не меняют данные транспортного уровня. По этой причине во многих случаях устройства NAT прозрачны для приложений. Однако существуют две области, в которых использование устройств NAT может создавать сложности: 1) данные приложений включают адреса IP и 2) требуется сквозное обеспечение защиты. Отметим, что могут быть и другие задачи, где трансляция создаёт проблемы.

Методы защиты на прикладных уровнях, не использующие адресов IP и не зависящие от них, будут корректно работать через NAT (например, TLS, SSL и ssh). Напротив, методы защиты на транспортном уровне (например, транспортный режим IPSec или TCP MD5 Signature Option RFC 2385 [17]) не будут работать при трансляции адресов.

В транспортном режиме IPSec контроль целостности для AH и ESP целиком включает поле данных (payload) пакета. Если данные относятся к протоколу TCP или UDP, контроль целостности учитывает и поле контрольной суммы TCP/UDP. Когда устройство NAT меняет адрес, контрольная сумма с учётом нового адреса становится иной. Обычно NAT обновляет и поле контрольной суммы, но этого сделать нельзя при использовании AH или ESP. Следовательно, получатели будут отбрасывать пакеты по результатам проверки целостности IPSec (если устройство NAT изменяет контрольную сумму) или по причине некорректности контрольной суммы (если NAT её не меняет).

Отметим, что IPsec в туннельном режиме ESP можно применять, пока на содержимое вложенных пакетов не оказывает влияния трансляция внешнего заголовка IP. Хотя этот метод не работает с традиционной NAT (где хосты просто не знают о наличии NAT), он применим к трансляции Realm-Specific IP, описанной в параграфе 5.0.

Отметим также сквозная аутентификация и защита конфиденциальности в транспортном режиме на основе ESP может использоваться для таких пакетов, как ICMP, где содержимое поля данных IP не меняется в результате трансляции внешнего заголовка IP.

Устройства NAT также нарушают фундаментальные допущения инфраструктур распределения открытых ключей типа Secure DNS RFC 2535 [18] и сертификатов X.509 с подписанными открытыми ключами. В случае Secure DNS каждый набор DNS RRset подписывается ключом зоны. Кроме того, аутентичность конкретного ключа проверяется по цепочке доверия до корня DNS. Когда DNS-ALG меняет адреса (например, в случае Twice-NAT), проверка подписи завершается отказом.

Будет интересно отметить, что IKE (протокол согласования сеансовых ключей) представляет собой основанный на UDP протокол сеансового уровня и не защищён с помощью IPsec. Защищена лишь часть данных IKE. По этой причине сессии IKE могут проходить через NAT, пока данные IKE не включают адресов или транспортных идентификаторов, специфичных для одной области и не известных другой. С учётом того, что IKE используется для организации защищённых связей IPSec и в настоящее время не известно способов организации работы IPSec через NAT, следует вести работу в направлении использования IKE через NAT.

Одно из популярных Internet-приложений FTP не работает с NAT, как описано выше. В следующем параграфе описана поддержка FTP в устройствах NAT. FTP ALG является встроенной частью большинства реализаций NAT. Некоторые разработчики могут включать дополнительные ALG для поддержки работы других приложений через NAT.

7.1. Поддержка FTP

Команда PORT и отклик на команду PASV в данных управления сеансом FTP идентифицируют IP-адрес и номер порта TCP, которые должны использоваться для передачи данных в этой сессии. Аргументами команды PORT и отклика на команду PASV являются адрес IP и номер порта TCP в формате ASCII. Шлюз FTP ALG должен контролировать и обновлять данные управления сеансом FTP, чтобы содержащаяся в них информация относилась к нужным оконечным узлам. Шлюз ALG должен также обновлять NAT с учётом пар адрес-порт и направления сессии, чтобы устройство NAT могло поддерживать состояние для сессий передачи данных FTP.

Поскольку адреса и номера портов TCP указываются в формате ASCII, изменение этих параметров может приводить к изменению размера пакетов. Например, последовательность 10,18,177,42,64,87 имеет размер 18 символов ASCII, а

193,45,228,137,64,87 - 20 символов. Если размер пакета сохраняется, требуется лишь заново рассчитать контрольную сумму TCP. Однако при изменении размера пакета требуется менять порядковые номера TCP с учётом изменения размера управляющих данных FTP. В устройствах ALG могут применяться специальные таблицы для корректировки порядковых номеров и номеров подтверждений TCP. Корректировка порядковых номеров и номеров подтверждений должна выполняться и для всех последующих пакетов данного соединения.

8.0. Ограничения NAT

8.1. Приложения с адресами IP в поле данных

Не все приложения легко можно адаптировать для работы через устройства NAT. В частности, сложности возникают с приложениями, которые передают адрес IP (и номер порта в случае NAPT) в поле данных пакетов. Для таких приложений требуется использовать специализированные шлюзы прикладного уровня (ALG[1]). Шлюзы ALG могут предоставлять адреса (и номера портов), подобно NAT, а также выполнять специфическую трансляцию, нужную для работы приложения. Комбинация функций NAT и ALG не позволяет организовать сквозную защиту с помощью IPsec. Однако можно воспользоваться туннельным режимом IPsec с маршрутизатором NAT в качестве окончания туннеля.

Приложения SNMP[2] относятся к числу передающих адреса в поле данных пакетов. Маршрутизаторы NAT не будут транслировать такие адреса IP в пакетах SNMP. Зачастую для SNMP применяются специализированные ALG (на маршрутизаторе NAT) для трансляции SNMP MIB[3] в приватной сети.

8.2. Приложения со связанными сессиями для управления и данных

Устройства NAT работают в предположении независимости каждой сессии. Параметры сессии (направление, адреса и транспортные идентификаторы отравителя и получателя, сеансовый протокол) определяются независимо при организации каждой сессии.

Однако существуют приложения (например, H.323), которые используют одну или несколько сессий для управления характеристиками сеанса обмена данными. Для таких приложений нужны специализированные шлюзы ALG, способные анализировать и интерпретировать данные сессии. Такая интерпретация будет помогать NAT в обработке связанных сессий передачи данных.

8.3. Отладка

NAT повышает вероятность ошибочной адресации. Например, тот или иной локальный адрес может оказаться связанным с разными внешними адресами в разное время, а один внешний адрес - с разными внутренними. В результате рассмотрение трафика на основе лишь глобальных адресов и номеров портов может приводить к путанице и ошибочным трактовкам.

Если хост в том или ином смысле некорректно ведёт себя в сети Internet (например, попытка атаки другого хоста или рассылка спама), идентифицировать такой хост сложнее, если он скрыт за маршрутизатором NAT.

8.4. Трансляция фрагментированных пакетов управления FTP

Трансляция фрагментированных пакетов управления FTP, содержащих команду PORT или отклик на команду PASV, достаточно сложна. Ясно, что в этом (патологическом) случае маршрутизатору NAT может потребоваться сборка фрагментов до трансляции и пересылки пакета.

Другая ситуация возникает когда каждый символ пакета с командой PORT или откликом на команду PASV передаётся в отдельной дейтаграмме (без фрагментирования). В этом случае NAT будет просто пропускать пакеты без трансляции данных TCP. Если для приложения такая трансляция нужна, неизбежно возникнет отказ в его работе. В редких случаях приложение будет работать, если содержимое данных корректно в обеих адресных областях. Например, сеанс FTP с хоста приватной сети будет работать при прохождении после традиционной или двухсторонней трансляции NAT, пока у управляющей сессии FTP используется команда PASV для организации сессий передачи данных. Причина этого заключается в том, что адрес и номер порта, заданные сервером FTP в отклике на команду PASV (переданном во множестве пакетов без фрагментирования), будут корректны для приватного хоста без их трансляции. Устройство NAT будет просто рассматривать сессию передачи данных (с того же приватного хоста), как независимый сеанс TCP.

8.5. Вычислительные ресурсы

NAT требует достаточно больших вычислительных ресурсов (даже при использовании эффективного алгоритма пересчёта контрольных сумм), поскольку устройство NAT должно просматривать и изменять все пакеты. В результате производительность маршрутизатора может заметно снижаться. Однако, пока производительность NAT выше скорости обработки пакетов на линейных интерфейсах, проблем возникать не должно.

9.0. Вопросы безопасности

Многие люди рассматривают традиционные маршрутизаторы NAT, как односторонние (сеансовые) фильтры трафика, ограничивающего доступ внешних хостов к ресурсам внутренней сети. В дополнение к этому динамически выделяющий адреса маршрутизатор NAT осложняет организацию атак на любой конкретный хост в домене NAT. Маршрутизаторы NAT могут использоваться совместно с межсетевыми экранами для фильтрации нежелательного трафика.

Если устройства NAT и ALG не находятся в доверенной зоне, это вызывает существенные проблемы безопасности, поскольку ALG могут просматривать данные из пользовательского трафика. Данные сеансового уровня можно зашифровать, если эти данные не содержат адресов IP и транспортных идентификаторов, которые требуют трансляции. За исключением случая RSIP, сквозная защита на уровне IP с помощью IPsec не может применяться при

[1]Application Level Gateway.
[2]Simple Nework Management Protocol - простой протокол сетевого управления. *Прим. перев.*
[3]Management Information Base - база управляющей информации. *Прим. перев.*

наличии NAT. Одной из конечных точек должно быть устройство NAT. В параграфе 7.0 было показано, почему сквозная защита IPsec не может быть реализована при наличии в пути устройств NAT.

Совместное использование NAT, ALG и межсетевых экранов будет обеспечивать прозрачную среду для приватного сетевого домена. За исключением случая RSIP, сквозная защита на сетевом уровне с помощью IPsec не может быть обеспечена для хостов приватной сети (работа RSIP описана в параграфе 5.0). В остальных случаях для сквозной защиты IPsec на пути передачи не должно быть устройств NAT. Если устройства NAT находятся в доверенной зоне, можно реализовать туннельный режим IPsec с использованием в качестве конечной точки туннеля устройства NAT (или комбинации NAT, ALG и межсетевого экрана).

Устройства NAT при совместном использовании с ALG будут предотвращать попадание из сети Internet дейтаграмм с приватными адресами в заголовках или полях данных. Пакеты приложений, не соответствующие этим требованиям можно отбрасывать с помощью фильтров на межсетевом экране. Поэтому зачастую функции NAT, ALG и межсетевого экрана используются совместно для защиты на периметре приватной сети. Шлюзы NAT могут служить конечными точками туннелей для организации защищённого транспорта (VPN) пакетов через внешние сети.

Ниже перечислены некоторые проблемы безопасности, связанные с маршрутизаторами NAT.

1. Сессии UDP не защищены по своей природе. Отклики на дейтаграммы могут приходить с адреса, отличающегося от указанного отправителем в исходном пакете [4]. В результате входящие пакеты UDP могут лишь частично соответствовать исходящим сессиям традиционной трансляции NAT (адрес и порт получателя будут соответствовать, адрес и порт отправителя - не будут). В таких случаях могут возникать проблемы безопасности, если устройство NAT будет принимать пакеты с частичным соответствием. Проблемы безопасности UDP присущи и межсетевым экранам.

   Традиционные устройства NAT не отслеживают дейтаграммы по сессиям, а взамен объединяют множество сессий UDP с одинаковой адресной привязкой в одну унифицированную сессию, что дополнительно снижает уровень безопасности. Это связано с тем, что проверка соответствия пакетов сессии ограничена лишь совпадением адреса получателя во входящих пакетах UDP.

2. Групповые адреса (для UDP) создают другую проблему безопасности для традиционных маршрутизаторов NAT. Снова подчеркнём, что такая же проблема присуща межсетевым экранам.

   Предположим, что хост приватной сети инициирует групповую сессию. Отправленные этим хостом дейтаграммы могут вызвать отклики множества внешних хостов. Традиционные маршрутизаторы NAT, использующие одно состояние для групповой сессии, не могут определить, относится входящий пакет UDP к существующей групповой сессии UDP или является частью атаки извне.

3. Устройства NAT могут быть целью атак.

   Поскольку устройства NAT являются хостами Internet, они могут подвергаться различным атакам, включая лавинную передачу пакетов SYN или ping. Устройства NAT должны поддерживать те или иные методы защиты себя, как это делается на серверах Internet.

Литература

[1] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot,G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[2] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700[1], October, 1994.

[3] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[4] Braden, R., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

[5] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[6] Postel, J. and J. Reynolds, "File Transfer Protocol (FTP)", STD 9, RFC 959, October 1985.

[7] Postel, J., "Transmission Control Protocol (TCP) Specification", STD 7, RFC 793, September 1981.

[8] Postel, J., "Internet Control Message Protocol Specification" STD 5, RFC 792, September 1981.

[9] Postel, J., "User Datagram Protocol (UDP)", STD 6, RFC 768, August 1980.

[10] Mogul, J. and J. Postel, "Internet Standard Subnetting Procedure", STD 5, RFC 950, August 1985.

[11] Carpenter, B., Crowcroft, J. and Y. Rekhter, "IPv4 Address Behavior Today", RFC 2101, February 1997.

[12] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[13] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[14] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[15] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[16] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[17] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[18] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

Адреса авторов

Pyda Srisuresh

Lucent Technologies

[1] В соответствии с RFC 3232 документ Assigned Numbers утратил силу. Данные сейчас доступны по ссылке.

4464 Willow Road

Pleasanton, CA 94588-8519

U.S.A.

Phone: (925) 737-2153

Fax: (925) 737-2110

EMail: srisuresh@lucent.com

Matt Holdrege

Lucent Technologies

1701 Harbor Bay Parkway

Alameda, CA 94502

Phone: (510) 769-6001

EMail: holdrege@lucent.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.