Санкт-Петербург, ул. Седова, 80, телефон (812) 449-0770, факс (812) 449-0771, E-mail: info@bilim.com

Настройка доступа в Internet с использованием двух асимметричных каналов

Николай Малых

nmalykh@bilim.com

Достаточно часто на различных форумах приходиться сталкиваться с обсуждением вопроса о настройке шлюзов при организации доступа в Internet с использованием двух асимметричных каналов. Обычно один из этих каналов обычно связан с приемной спутниковой антенной (в дальнейшем будем этот канал называть спутниковым) и может использоваться только для приема данных. Второй канал (назовем его наземным) служит для передачи трафика из сети пользователя в направлении Internet. В общем случае этот канал может быть симметричным, но без снижения общности задачи можно предположить асимметрию и для этого канала (т. е., канал передает пакеты, но не может их принимать или прием через этот канал нецелесообразен по каким-либо причинам). Этот канал служит для передачи пользовательских запросов к серверам, откликов TCP на полученные от сервера пакеты и т. п. Решение подобных задач не представляет особой сложности, но, как показывает опыт, у большинства пользователей и администраторов небольших сетей возникают проблемы с настройкой оборудования и программ. Постараюсь описать ниже разные варианты организации такого подключения, подробно рассмотрев основные параметры настройки.

Для начала давайте рассмотрим задачу в общем виде, это позволит более глубоко понять происходящие процессы и разобраться в параметрах настройки. Предположим, что у пользователя есть локальная сеть, которая через те или иные устройства (устройство) связана с наземным и спутниковым каналом, идущим к провайдерам Internet (как правило, наземный и спутниковый канал предоставляют разные провайдеры, что и порождает дополнительные проблемы с настройкой). Предположим также, что в локальной сети используются адреса одного из приватных блоков (см. RFC 1918). Пусть наземный канал использует IP-адрес $IP_{earth,}$ а спутниковый канал – IP_{sat}.

Адреса из приватных блоков не будут маршрутизироваться за пределами сети компании, поэтому в исходящих пакетах эти адреса так или иначе должны быть преобразованы в публичный адрес IP_{earth} для исходящих пакетов, а при получении откликов из сети Internet должно быть выполнено обратное преобразование адреса получателя (публичного адреса приемного интерфейса IP_{sat} в приватные адрес локальной сети). Преобразование адресов может выполняться в явном виде (NAT – Network Address Translation) или с помощью прокси сервера, который будет принимать клиентские запросы и передавать их серверу с использованием своего публичного адреса IP. Очевидно, что преобразования адресов в исходящих и входящих пакетах должны быть согласованы, поэтому могут выполняться только в рамках одного хоста. Отметьте в памяти это обстоятельство, оно пригодится нам в дальнейшем.

Рассмотрим теперь процесс взаимодействия клиента из локальной сети с неким сервером Internet. В соответствии с запросом клиента будет сформирован запрос на соединение TCP и передан через интерфейс наземного канала с адресом IP_{earth} с поле отправителя заголовка IP. Получив этот запрос, сервер отправит отклик на него по адресу, указанному в поле отправителя, т. е., IP_{earth}. Поскольку наш наземный канал асимметричен, адресованные IP_{earth} по пакеты просто не попадут к получателю и клиент никогда не дождется отклика от сервера. Мы же хотим получить от внешних серверов отклики через спутниковый канал, т. е. Они должны быть направлены по адресу IP_{sat}. Для решения этой задачи на станции (маршрутизаторе), к которой подключен физический интерфейс наземного канала должна осуществляться подмена значения адреса отправителя в исходящих пакетов IP. Такая подмена называется трансляцией адресов или NAT. В нашем случае взамен адреса IP_{earth} в заголовки исходящих пакетов должно помещаться значение IP_{sat}. После такого преобразования все серверы в ответ на клиентские запросы будут направлять отклики в адрес интерфейса спутникового канала IP_{earth} и клиенты смогут нормально получать отклики на свои запросы.

Но приемный интерфейс спутникового канала еще должен узнать, на с какого из клиентских адресов пришел запрос и соответствующим образом направить отклик. Вспомним, сказанное выше о том, что сведения о трансляции адресов должны быть доступны на станции с приемным интерфейсом и перейдем к рассмотрению реальных конфигураций, которые могут возникать при использовании такой схемы подключения.

1. **Интерфейсы спутникового и наземного канала подключены к одной станции (маршрутизатору).**

   Этот случай более прост в настройке, поскольку приемному интерфейсу доступны информация о трансляции адресов и не составляет большого труда выполнить обратное преобразование для принимаемых через спутниковый канал пакетов. Опишем далее настройки граничного шлюза и клиентских машин в предположении, что шлюз соединен с локальной сетью через интерфейс, имеющий адрес IP_{gate}.

   a) Параметры настройки граничного шлюза

   - Default Gateway – адрес интерфейса маршрутизатора у провайдера, обеспечивающего наземный канал (IP_{earth})
   - NAT – IP SRC -> IP_{sat} для всех исходящих пакетов.
     Ниже приведено правило трансляции адресов для iptables. Если вы используете иные средства трансляции, создайте аналогичное правило в соответствии с синтаксисом используемой NAT
     iptables -A POSTROUTING -j SNAT --to-source IP_{sat}

   b) Параметры настройки станций ЛВС

   - Default Gateway - IP_{gate}

   Если вы используете на граничном шлюзе или другом компьютере прокси-сервер, достаточно транслировать только адрес этого сервера.

2. **Интерфейсы наземного и спутникового канала подключены к разным станциям (маршрутизаторам).**

Этот случай несколько сложнее, но также не требует никаких особых хитростей. Как уже обсуждалось выше приемная станция для корректного отслеживания соединений и преобразования адреса отправителя в принятых должна обладать информацией о преобразовании адресов в исходящих пакета, поэтому система трансляции адресов (NAT) или сервер прокси должна быть установлена на этой машине (прокси можно установить и на другом компьютере, но не на том, который связан с наземным каналом). Обозначим внутренние (приватные) адреса шлюзов с интерфейсами наземного и спутникового каналов как IP_{gate} и IP_{gate1}, соответственно. Оба эти интерфейса подключаются к локальной сети.

a) Параметры настройки передающего шлюза (наземный канал)

- Default Gateway – адрес интерфейса маршрутизатора у провайдера, обеспечивающего наземный канал (IP_{earth})
- NAT – IP SRC -> IP_{sat} для всех исходящих пакетов.
  Ниже приведено правило трансляции адресов для iptables. Если вы используете иные средства трансляции, создайте аналогичное правило в соответствии с синтаксисом используемой NAT
  iptables -A POSTROUTING SNAT --to-source IP_{sat}

b) Параметры настройки для приемной станции (спутниковый канал)

- Default Gateway - Ip_{gate} (внутренний адрес станции, подключенной к наземному каналу)
- NAT – IP SRC -> IP_{sat} для всех исходящих пакетов.
  Ниже приведено правило трансляции адресов для iptables. Если вы используете иные средства трансляции, создайте аналогичное правило в соответствии с синтаксисом используемой NAT
  iptables -A POSTROUTING -j SNAT --to-source IP_{sat}

c) Параметры настройки станций ЛВС

- Default Gateway - Ip_{gate1} (внутренний адрес станции, подключенной к спутниковому каналу)

Если вы используете на граничном шлюзе прокси-сервер, можно не транслировать адресов на этом шлюзе. Если же прокси-сервер установлен на другом компьютере, достаточно транслировать только адрес этого сервера.

В заключении следует отметить еще один нюанс, связанный с организацией таких соединений. Провайдер, обеспечивающий наземный канал, в соответствии с RFC 2827 (на сайте www.protocols.ru имеется перевод этого документа на русский язык) может фильтровать пакеты на границе своей сети по адресам отправителя. Поскольку в описываемой ситуации из вашей сети будут передаваться пакеты с адресом IP_{sat} в поле отправителя, эти пакеты могут быть отброшены фильтрами, т. к. не относятся к выделенным провайдеру и его клиентам блокам адресов IP. Дабы такой проблемы не возникало, следует обратиться в службу технической поддержки провайдера наземного канала самим или попросить это сделать технических специалистов компании, которая предоставляет вам спутниковый канал.