Министерство образования и науки Украины

Севастопольский национальный технический университет

NETWORK ADDRESS TRANSLATION (NAT) И VIRTUAL PRIVATE NETWORKS (VPN) НА БАЗЕ ОПЕРАЦИОННОЙ СИСТЕМЫ MICROSOFT WINDOWS SERVER 2003

Методические указания
к выполнению лабораторной работы
по дисциплине «Глобальные и корпоративные
компьютерные сети»
для студентов специальности 6.050201
«Системная инженерия»
дневной и заочной форм обучения

Севастополь
2009

УДК 681.3

Network Address Translation (NAT) и Virtual Private Networks(VPN) на базе операционной системы Microsoft Windows Server 2003: Методические указания к выполнению лабораторной работы по дисциплине «Глобальные и корпоративные компьютерные сети» для студентов направления 6.050201 «Системная инженерия» дневной и заочной форм обучения / Сост. П.Л. Светличный, – Севастополь: Изд-во СевНТУ, 2009. – 12 с.

Целью методических указаний является оказание помощи студентам в выполнении лабораторной работы.

Методические указания рассмотрены на заседании кафедры
Технической кибернетики, протокол № 6 от « 26 » ___мая____ 2009 г.

Допущено учебно-методическим центром СевНТУ в качестве методических указаний.

Рецензент
Карапетьян В.А. канд.техн.наук, доцент кафедры ТК

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Изучить принципы построения виртуальных частных сетей (VPN) и объединения с глобальными сетями посредством трансляции сетевых адресов (NAT) на базе операционной системы Microsoft Windows 2003 Server.

2. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

С ростом числа компьютеров, устанавливаемых дома и на предприятиях малого бизнеса, становятся очевидными преимущества сетевой среды, предоставляющей широкие возможности совместного использования компьютерных ресурсов. Подключение к интернету является одним из наиболее ценных ресурсов в сети, и потому естественно стремление организовать общий доступ к нему. Развертывание шлюзов интернета позволяет решить эту задачу и построить недорогую, легко управляемую домашнюю или небольшую офисную сеть. В шлюзах интернета, как правило, используется технология NAT (Network Address Translation - преобразование сетевых адресов), которое обеспечивает подключение нескольких узлов к интернету с использованием одного общего IP-адреса.

NAT. Network Address Translation (сетевое преобразование адреса) – это технология, которая использует маршрутизатор для распределения интернет соединения между компьютерами в частной сети, даже если эти компьютеры не имеют публичного адреса. Существуют как аппаратные, так и программные реализации маршрутизаторов NAT.

Преобразование сетевых адресов представляет собой стандарт IETF (Internet Engineering Task Force - рабочая группа разработки технологий интернета), с помощью которого несколько компьютеров частной сети (с частными адресами из таких диапазонов, как, например, 10.0.x.x, 192.168.x.x, 172.x.x.x) могут совместно пользоваться одним адресом IPv4, обеспечивающим выход в глобальную сеть. Основная причина растущей популярности NAT связана со все более обостряющимся дефицитом адресов протокола IPv4. Средство общего доступа к подключению интернета в операционных системах Windows XP и Windows Me, а также многие шлюзы интернета активно используют NAT, особенно для подключения к широкополосным сетям, например, через DSL или кабельные модемы.

NAT дает немедленное, но временное решение проблемы дефицита адресов IPv4, которая рано или поздно отпадет сама собой с появлением протокола IPv6.

NAT не только позволяет сократить число необходимых адресов IPv4, но и образует дополнительную защиту частной сети, поскольку с точки зрения любого узла, находящегося вне сети, связь с ней осуществляется лишь через один, совместно используемый IP-адрес. NAT – это не то же самое, что брандмауэр или прокси-сервер, но это, тем не менее, важный элемент безопасности.

Общие принципы работы. Клиентам сети, находящимся с внутренней стороны устройства NAT, назначаются частные IP-адреса; обычно это делается через службу DHCP (Dynamic Host Configuration Protocol - протокол динамической настройки узлов) или путем статической настройки, выполняемой администратором. В ходе сеанса связи с узлом, находящимся снаружи этой частной сети, обычно происходит следующее.

На стороне клиента

Приложение, собирающееся установить связь с сервером, открывает сокет, определяемый IP-адресом источника, портом источника, IP-адресом назначения, портом назначения и сетевым протоколом. Эти параметры идентифицируют обе конечные точки, между которыми будет происходить сеанс связи. Когда приложение передает данные через сокет, частный IP-адрес клиента (IP-адрес источника) и клиентский порт (порт источника) вставляются в пакет

в поля параметров источника. Поля параметров пункта назначения будут содержать IP-адрес сервера (IP-адрес назначения - удаленный узел) и порт сервера. Поскольку пункт назначения пакета находится вне частной сети, клиент направляет его в основной шлюз. В данном сценарии роль основного шлюза играет устройство NAT.

Исходящий пакет в устройстве NAT

Устройство NAT перехватывает исходящий пакет и производит сопоставление порта, используя IP-адрес назначения (адрес сервера), порт назначения, внешний IP-адрес устройства NAT, внешний порт, сетевой протокол, а также внутренние IP-адрес и порт клиента.

Устройство NAT ведет таблицу сопоставлений портов и сохраняет созданное сопоставление в этой таблице. Внешние IP-адрес и порт – это общие IP-адрес и порт, которые будут использоваться в текущем сеансе передачи данных вместо внутренних IP-адреса и порта клиента.

Затем устройство NAT транслирует пакет, преобразуя в пакете поля источника: частные, внутренние IP-адрес и порт клиента заменяются общими, внешними IP-адресом и портом устройства NAT.

Преобразованный пакет пересылается по внешней сети и в итоге попадает на заданный сервер.

На стороне сервера

Получив пакет, сервер полагает, что имеет дело с каким-то одним компьютером, IP-адрес которого допускает глобальную маршрутизацию. Сервер будет направлять ответные пакеты на внешние IP-адрес и порт устройства NAT, указывая в полях источника свои собственные IP-адрес и порт.

Входящий пакет в устройстве NAT

NAT принимает эти пакеты от сервера и анализирует их содержимое на основе своей таблицы сопоставления портов. Если в таблице будет найдено сопоставление порта, для которого IP-адрес источника, порт источника, порт назначения и сетевой протокол из входящего пакета совпадают с IP-адресом удаленного узла, удаленным портом и сетевым протоколом, указанным в сопоставлении портов, NAT выполнит обратное преобразование. NAT заменяет внешний IP-адрес и внешний порт в полях назначения пакета на частный IP-адрес и внутренний порт клиента.

Затем NAT отправляет пакет клиенту по внутренней сети. Однако если NAT не находит подходящего сопоставления портов, входящий пакет отвергается и соединение разрывается.

Благодаря устройству NAT клиент получает возможность передавать данные в глобальной среде интернета, используя лишь частный IP-адрес; ни от приложения, ни от клиента не требуется никаких дополнительных усилий. Приложению не приходится обращаться к каким-либо специальным API-интерфейсам, а клиенту не нужно выполнять дополнительную настройку. В данном случае механизм NAT оказывается прозрачным по отношению к клиенту и к серверному приложению - все работает просто и четко.

Однако не все сетевые приложения пользуются протоколами, способными взаимодействовать с NAT. В этом-то и заключается проблема.

Проблемы взаимодействия NAT и приложений

Средство NAT успешно обеспечивает совместное использование единого глобального IP-адреса, когда клиент инициирует контакт и принимает ответ через один и тот же порт. Однако многие приложения используют стратегии, основанные на предположениях, которые становятся неверными, если для доступа в интернет применяется устройство NAT. Некоторые из подобных проблем обсуждаются ниже.

Службы во внутренней сети

Многие сетевые службы и серверы исходят из того, что если они установили прослушивающий сокет, то любой клиент в интернете сможет инициировать с ними контакт. Если на периферии сети размещено устройство NAT, то для прохождения входящего трафика к службам внутренней сети потребуется наличие соответствующего сопоставления портов. Поэтому такая служба будет доступна только клиентам частной сети, но не остальным узлам интернета.

Чаще всего эту проблему обходят, вручную настраивая сопоставление портов, которое позволяет устройству NAT передавать трафик, адресованный в NAT с указанием неких внешних IP-адреса и порта, на внутренние IP-адрес и порт, используемые службой.

Когда такое сопоставление установлено, служба может получать входящие пакеты и становится доступной для клиентов, внешних

по отношению к частной сети. Пока сопоставление портов не выполнено, связь с сетью не поддерживается.

Настроить сопоставление портов вручную, как правило, довольно сложно; это требует определенного опыта. Поэтому многие индивидуально работающие пользователи и сотрудники небольших офисов не могут работать с нужными им приложениями и службами без посторонней помощи и вынуждены в поисках решения проблемы обращаться в службу технической поддержки своего интернет-провайдера, производителя компьютера, торговой фирмы или производителя шлюза интернета. К тому же такое сопоставление накладывает меньше ограничений ? любой внешний клиент сможет воспользоваться им для инициирования контакта с сервером.

Вложенные адреса и порты

Некоторые сетевые приложения предполагают, что IP-адрес и порт, назначенные клиенту, всегда будут доступны для глобальной маршрутизации и смогут непосредственно использоваться в интернете. Во многих случаях эти адреса являются частными IP-адресами из диапазонов, зарезервированных группой IETF. Приложение включает такой частный IP-адрес или порт в содержащую полезные данные часть пакета, посылаемого на сервер. Сервер может использовать этот вложенный адрес для связи с клиентом.

Если сервер попытается ответить, используя вложенные IP-адрес и порт вместо сопоставленных значений адреса и порта, предоставленных средством NAT, то пакет будет отброшен при передаче. Это происходит потому, что вложенный IP-адрес нельзя маршрутизировать. Если сетевое приложение обнаружило бы устройство NAT и получило у него внешний IP-адрес и внешний порт, оно смогло бы поместить в пакет правильные данные.

Приложения, использующие различные сокеты

Некоторые сетевые приложения отправляют трафик на сервер или в другой узел, используя сокет в одном порте X, а ожидают ответа с сервера на другом, прослушивающем сокете в порте Y. NAT изучает исходящий трафик и производит сопоставление порта X, но не знает о том, что нужно еще выполнить сопоставление портов для возвращающихся пакетов, адресованных в порт Y. Входящие пакеты, адресованные в порт Y, отбрасываются.

Ожидание доступа к портам

Некоторые сетевые протоколы исходят из того, что нужный им порт, широко известный и допускающий глобальную маршрутизацию, всегда будет для них доступен. Когда несколько клиентов сообща используют один IP-адрес, в каждый момент времени только один клиент имеет доступ к стандартному порту. Например, только одна веб-служба может в каждый момент времени пользоваться внешним портом 80 в локальной сети. Если бы это было не так, устройство NAT не смогло бы определить, к какому клиенту относится внешний запрос. Необходимо, помимо настройки пользователем сопоставления портов, принять специальные меры к тому, чтобы разные клиенты могли быть распознаны извне локальной сети.

При выполнении лабораторной работы и подготовке к защите рекомендуется использовать учебную и справочную литературу [1–3].

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Выполнение лабораторной работы состоит из следующих шагов:

1. Изучение теоретических сведений.
2. Добавление нового протокола (NAT).

Для добавления протокола NAT необходимо в пункте меню «Общие» оснастки «Маршрутизация и удалённый доступ» выбрать соответствующий пункт из контекстного меню.

3. Добавление интерфейсов для сетевого преобразования адресов.

Выбрав в контекстном меню пункта «NAT/Простой брандмауэр» в разделе «IP-маршрутизация» оснастки «Маршрутизация и удалённый доступ» опции «Новый интерфейс», необходимо добавить один из сетевых интерфейсов, через который осуществляется выход в Интернет (см. Приложение А). В свойствах необходимо отметить этот интерфейс как Общий и отметить галочками пункты меню «Включать NAT на данном интерфейсе» и «Включить основной брандмауэр для этого интерфейса».

Затем следует вернуться к пункту меню «NAT/Простой брандмауэр», в контекстном меню выбрать «Новый интерфейс» и в

появившимся окне выбрать интерфейс локальной сети. В свойствах отметить этот интерфейс как частный. Ту же операцию проделываем с оставшимся интерфейсом.

4. Добавление внутренних сервисов сети.
5. Настройка службы маршрутизации и удалённого доступа на работу в качестве сервера удалённого доступа.

В свойствах сервера необходимо установить галочки напротив параметров «локальной сети и вызова по требованию» и «сервер удалённого доступа».

6. Добавление пула IP-адресов.

В закладке «IP» свойств сервера нужно выбрать в качестве адаптера внутренний сетевой интерфейс и добавить статический или динамический пул IP-адресов в зависимости от структуры сети. Эти адреса будут назначаться подключающимся клиентам.

7. Конфигурирование портов PPTP.

Для конфигурирования портов необходимо зайти в свойства «Порты». По умолчанию служба RRAS создаст 5 портов PPTP, 5 L2TP и 1 прямой параллельный порт. В рамках данной лабораторной работы необходимо отключить все порты, кроме PPTP. Нужных портов необходимо создать столько, сколько планируется одновременных подключений по VPN с небольшим запасом.

Для удаления портов нужно в свойствах этих портов указать максимальное количество равное нулю и снять все галочки.

8. Создание клиентов

Для подключения по VPN необходимо наличие пользователя с соответствующими правами. Для создания такого пользователя нужно зайти в оснастку «Управление компьютером», открыть меню «Локальные пользователи и группы» и в разделе «Пользователи» добавить нового клиента. В настройках клиента в закладке «Входящие звонки» необходимо разрешить доступ на удалённый доступ.

9. Защита работы.

Для защиты работы необходимо предоставить подробный отчёт, включающий пошаговое описание выполнения задания и содержащий скриншоты основных настроек. При защите за рабочим местом необходимо продемонстрировать практические навыки и повторить ход выполнения заданий.

4. ЗАДАНИЕ НА РАБОТУ

Взяв за основу сетевые настройки из предыдущей лабораторной работы («Изучение основ программной маршрутизации на базе операционной системы Microsoft Windows Server 2003») настроить сетевую трансляцию адресов (NAT) и сервер виртуальной частной сети (VPN) для приёма клиентских подключений.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое сетевая трансляция адресов?
2. Назовите основные сферы применения сетевой трансляции адресов.
3. Какие оснастки отвечают за функционирование NAT?
4. Что такое виртуальная частная сеть?
5. Для чего применяется VPN?
6. Сколько одновременных подключений по VPN может быть активно на сервере?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Камер, Дуглас, Э. Сети TCP/IP, том 1. Принципы, протоколы и структура, 4-е изд. / Дуглас Э. Камер. – М.: «Вильямс», 2003. – 880 с.
2. Гук М. Аппаратные средства локальных сетей. Энциклопедия / М. Гук. – СПБ.: «Питер», 2005. – 573 с.
3. Электронная энциклопедия www.ru.wikipedia.org