Тема занятия: Что такое NAT, как его настроить и использовать — NAT.

По данной теме, вы можете посмотреть видео, перейдя по ссылке

https://www.youtube.com/watch?v=L1JtmAiSaFQ

Теоретическая часть

Сегодня затронем подробнее тему несколько болезненную и довольно непонятную, но более непонятную, чем болезненную.

В большей степени эта проблема касается тех, кто играет в многопользовательские игры и коротко эта проблема звучит примерно так: "ПОЧЕМУ КО МНЕ НИКТО НЕ ЗАХОДИТ?". Для других эта проблема выглядит несколько иначе, а именно:

- Почему не качает торрент?
- Почему пользователи/друзья/знакомые/неизвестные личности не могут подключиться к **FTP, WEB, VOIP** (**TS, Mamble**, ведро) и прочим серверам, которые вы так долго пытались настроить и даже проверяли что у вас все работает?
- Почему ваш личный домашний сервер пустует? Может это вселенский заговор?

Но, однако, нет никакого заговора, виновник всех этих бед находится рядом с вами и хитро подмигивает вам лампочками, а зовут его... роутер, да-да, тот самый, который раздает вам интернет на все ваши (и может быть соседские) девайсы.

Если коротко, то пользователи из интернета просто не могут к вам подключиться, потому что ваш роутер их не пускает, но он делает это не просто из прихоти, а потому, что не знает о том, что все эти люди хотят подключиться именно к вам. Вот он и думает, что они что-то хотят от него самого.

Да, только что я вам обрисовала для чего нужен **NAT**. А теперь о том, что это такое.

Общее определение

NAT (Network Address Translation) - это такой механизм, который позволяет роутеру определять какие сервисы находятся за роутером и должны быть доступны из интернета, чтобы пользователи оттуда могли этими сервисами пользоваться (определение из вики я брать не стал, т.к. оно заумное и не всем понятное).

NAT присутствует во всех роутерах и серверных операционках в том или ином виде. В роутерах это обычно называется **port forwarding**, в линуксах **iptables**, на виндовых серверах - в специальной оснастке. А теперь давайте поговорим о различных типах **NAT**.

Тип первый, Static NAT

Static NAT не требуется для дома, а нужен в том случае, если провайдер выделил несколько **IP** адресов (внешние или "белые" адреса) вашей компании, и вам нужно, чтобы некоторые серверы всегда были видны из интернета, при этом их адреса бы не менялись.

Т.е. происходит преобразование адресов **1-1** (один внешний **IP** назначается одному внутреннему серверу). При такой настройке ваши серверы всегда будут доступны из интернета на любом порту.

Кстати говоря о **портах**, попробую несколько углубиться в эту тему, но не слишком сильно. Дело в том, что любой сервис, любая программа обращается к компьютеру, серверу, роутеру или сервису (будь то почта, веб-страничка или любой другой сервис) не только по **IP** адресу, но и по порту. Например, чтобы вам открыть страничку **google.com** со своего компьютера, вам надо ввести две вещи: **IP** адрес (**DNS** имя) и.. порт.

Но постойте, возмутитесь вы, ведь никакого порта вы не вводите и все отлично открывается!

Так в чем же дело в статике?

Дело в том, что, нет, в **DNS** записи порт не прячется, как некоторые могли бы подумать, этот самый порт ваш браузер сам подставляет в адресную строку вместо вас. Вы можете легко это проверить. Введите в адресной строке **google.com:80** и увидите, что страничка гугла открылась, но волшебные "**:80**" внезапно исчезли.

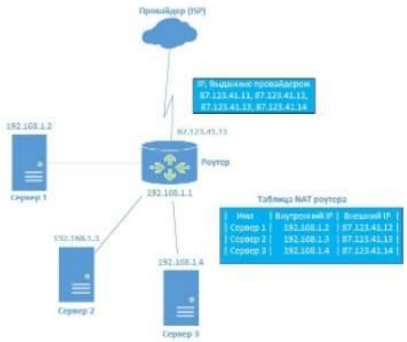
Так вот, чтобы пользователям из интернета вас видеть и иметь возможность к вам подключаться, они должны знать две вещи: ваш **IP адрес** и ваш порт, на котором расположен ваш сервис.

При статическом **NAT** вам будет фиолетово какой порт использует сервер или программа, т.к. сервер становится полностью доступен из интернета. Чтобы уже ограничить используемые порты, настраивается на этом сервере межсетевой экран.

Если провести параллель, то **IP** адрес - это адрес вашего дома, а порт - это номер вашей квартиры. Таким образом, чтобы люди могли к вам попасть, им нужно знать эти две вещи, иначе они вас просто не найдут.

Схема работы статического NAT

Попробую рассказать о схеме работы статического **NAT**.



Например, провайдер выдал вам
четыре **IP** адреса **87.123.41.11, 87.123.41.12, 87.123.41.13, 87.123.41.14**, а у вас
есть **три** сервера и роутер. Вы назначаете роутеру, например, первый адрес из этого диапазона (**87.123.41.11**), а остальные делите между серверами (сервер **1 - .12,** сервер **2 - .13,** сервер **3 - .14**).

Чтобы пользователи из интернета могли подключаться на эти серверы, им достаточно будет ввести **внешние** IP адреса серверов. Например, когда пользователь подключается на адрес **87.123.41.12**, то роутер перенаправляет его на **сервер 1** и пользователь уже общается с сервером, хотя не знает что реальный адрес сервера на самом деле другой (**192.168.1.2**). Такая запись в **NAT** таблице роутера будет храниться всегда.

Преимущества данного способа:

- реальные адреса серверов будут скрыты;
- Ваши серверы всегда будут видны в интернете.

Недостатки:

- Злоумышленники могут на них попытаться пробиться или осуществлять какие-нибудь атаки;
- Требуется несколько внешних адресов, что может быть затратно.

Тип второй, Dynamic NAT

Динамический **NAT** отличается от статического немногим. Он используется почти также, но с тем лишь исключением, что ваши сервера не видны из интернета, но самим серверам этот интернет нужен. Суть его в том, что вам также выдаются несколько **внешних IP** адресов от провайдера, после чего роутер сам распределяет адреса между "нуждающимися".

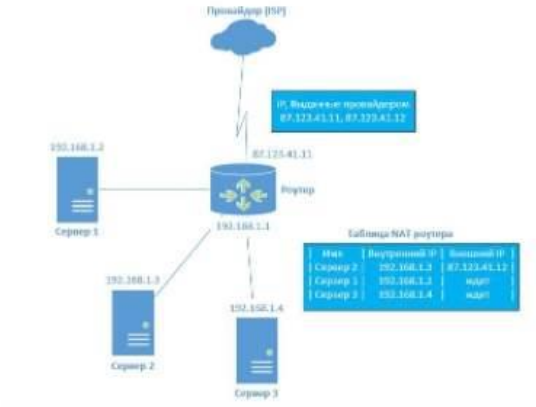
Т.е. как только сервер или компьютер захотел выйти в интернет, роутер смотрит на свой список внешних адресов, выданных провайдером, и выдает один адрес из этого списка, при этом помечает что вот он выдал такой-то внешний адрес такому-то серверу или компьютеру (таблица **NAT**).

При этом срок жизни такой записи длится очень короткое время и как только сервер/компьютер перестал требовать доступ в интернет, этот адрес удаляется из таблицы **NAT** роутера.

Существенный недостаток в том, что количество серверов и компьютеров, которым требуется доступ в интернет, не должен сильно превышать кол-во выданных провайдером внешних адресов.

Недостаток и преимущества динамики

Ведь как только у роутера закончатся адреса в списке, он не сможет пустить новые компьютеры или серверы в интернет, пока не освободится хотя бы один внешний адрес.



В данном примере провайдер выдал нам всего два внешних адреса: **87.123.41.11 и 87.123.41.12**. В этом случае мы IP **87.123.41.11** назначаем роутеру, а оставшийся адрес будет автоматически отдаваться тому серверу, который первым попросит доступ в интернет (в данном примере это был сервер 2), остальные серверы будут ждать, когда первый закончит и этот IP адрес освободится.

Преимущества данного способа:

- Всякие злоумышленники не смогут определить по каким адресам доступны ваши серверы, т.к. их адреса будут все время меняться;
- Не нужно вручную назначать IP адреса, роутер сам распределит.

Недостатки:

- Требуется несколько внешних адресов;
- Кол-во хостов в вашей сети не должно быть сильно больше, чем выданных провайдером IP адресов.

Закрепление материала:

1. Что такое NAT?
2. Что необходимо чтобы пользователи из интернета вас видеть и имели возможность к вам подключаться?
3. Опишите схему работы статического NAT.
4. Опишите схему работы динамического NAT.

Задания выполнить в Word и направить на почту: ignat-880@mail.ru не позднее 13.04.2020г.