УДК 004.7

СОЕДИНЕНИЕ «СЕРЫХ» КОМПЬЮТЕРОВ ПРИ СИММЕТРИЧНОМ NAT

А. В. Гриценко

Донской государственный технический университет, Ростов-на-Дону, Российская Федерация

express-rus@yandex.ru

Представлен обзор механизма преобразования сетевых адресов NAT (Network Address Translation) по способу преобразования. Приведены данные о том, с какой частотой разные способы используются на практике. Рассмотрены различные схемы обхода NAT.

Ключевые слова: NAT, P2P, публичный адрес, UDP, hole punching.

UDC 004.7

CONNECTION OF PRIVATE IP ADDRESS COMPUTERS WITH SYMMETRIC NAT

A.V.Gritsenko

Don State Technical University, Rostov-on-Don, Russian Federation

express-rus@yandex.ru

The paper presents the review of NAT on the way of address translation. It provides the date on how often different methods are used in practice. Different NAT bypass schemes are considered.

Keywords: NAT, P2P, public address, UDP, hole punching.

Введение. Пиринговые соединения (от узла к узлу) в последнее время все чаще и чаще используются в приложениях и сервисах. Такой подход небезоснователен, так как для дистрибьюторов услуги позволяет экономить ресурсы и повышать отказоустойчивость системы, лишая ее узкого места — сервера. Для конечных клиентов появляется дополнительная гарантия, исключающая прослушку и логгирование трафика третей стороной. На подготовительных стадиях работы по организации распределенных высокопроизводительных вычислений была выявлена проблема создания подобных прямых соединений между клиентами за NAT, в частности, наибольшие сложности вызывают симметричные NAT. Зачастую клиент находится в локальной подсети, имеющей свою адресацию («серые» ip-адреса), которая имеет лишь транслируемый выход во «вне». Клиент может быть как за домашним NAT, т.е. роутером/маршрутизатором, так и за NAT провайдера, а также за двумя и более NAT. Ключевым шагом организации прямых соединений является преодоление NAT.

Виды NAT по способу преобразования адресов.

1) Full Cone (полный конус).

Однозначная (взаимная) трансляция между парами «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт». Любой внешний хост может инициировать соединение с внутренним хостом.

2) Restricted Cone (ограниченный конус).

Постоянная трансляция между парой «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт». Любое соединение, инициированное с внутреннего адреса, позволяет в дальнейшем получать ему пакеты с любого порта того публичного хоста, к которому он отправлял пакет(ы) ранее. Отличие от Full Cone в том, что на узел будут маршрутизироваться только пакеты с того же IP, хотя порты источника могут различаться.

3) Port Restricted Cone (порт ограниченного конуса).

Постоянная трансляция между парой «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт», при которой входящие пакеты проходят на внутренний хост только с одного порта публичного хоста — того, на который внутренний хост уже посылал пакет. Отличие от Full Cone в том, что на узел будут маршрутизироваться пакеты с любого IP, но порт источника должен совпасть с портом назначения первой отправки.

4) Symmetric (симметричный).

Трансляция, при которой каждое соединение, инициируемое парой «внутренний адрес: внутренний порт» преобразуется в свободную уникальную случайно выбранную пару «публичный адрес: публичный порт». При этом инициация соединения из публичной сети невозможна.

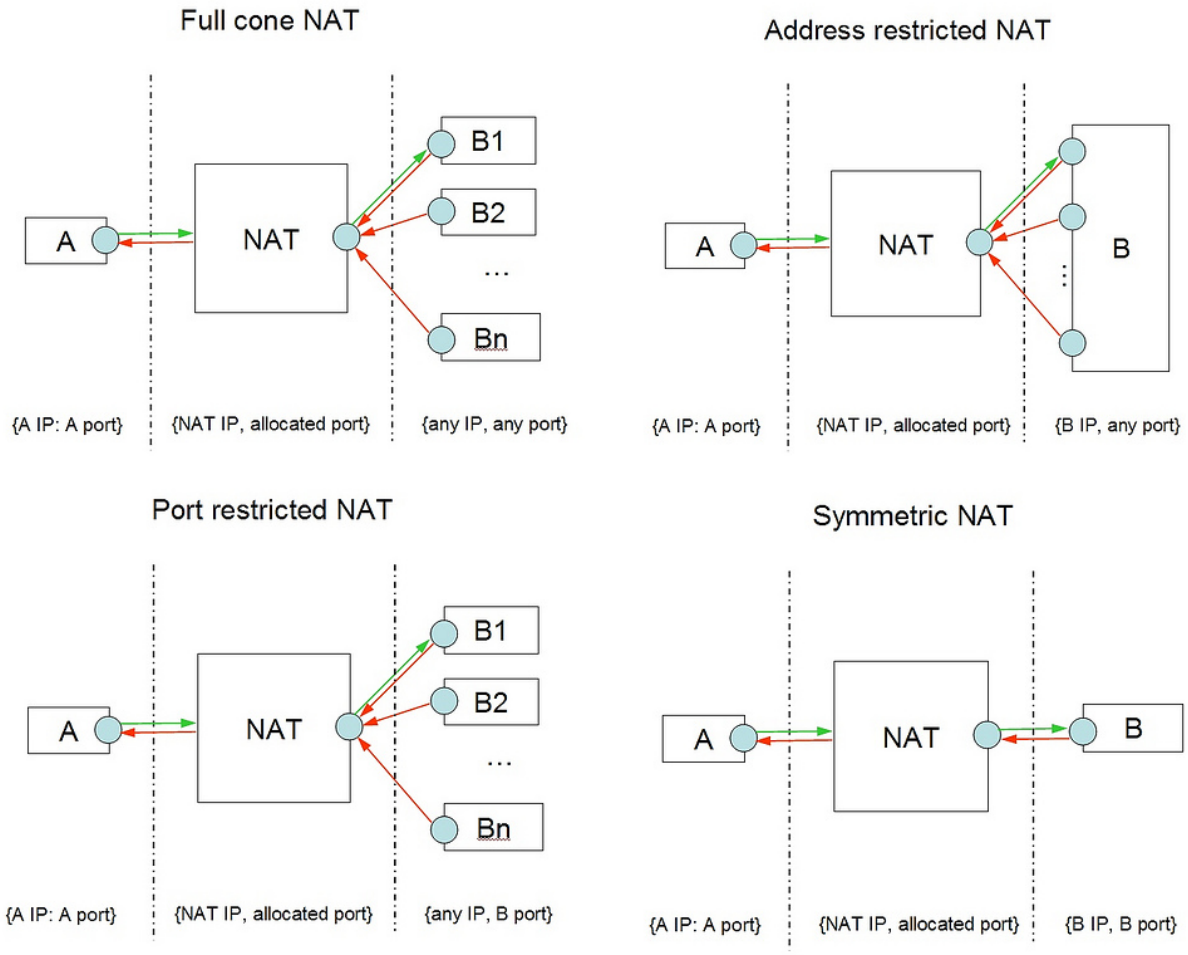

Рис. 1. Виды NAT

По данным сервиса тестирования маршрутизаторов nattest.ne, разработанного Оливером Гассером (Технический университет Мюнхена), в процентном эквиваленте преобладают Port Restricted 50,9%, за ними Symmetric 15,5%, Full Cone: 13%, Restricted Cone 3,3%. Всего выборка содержит 12 182 протестированных узлов.

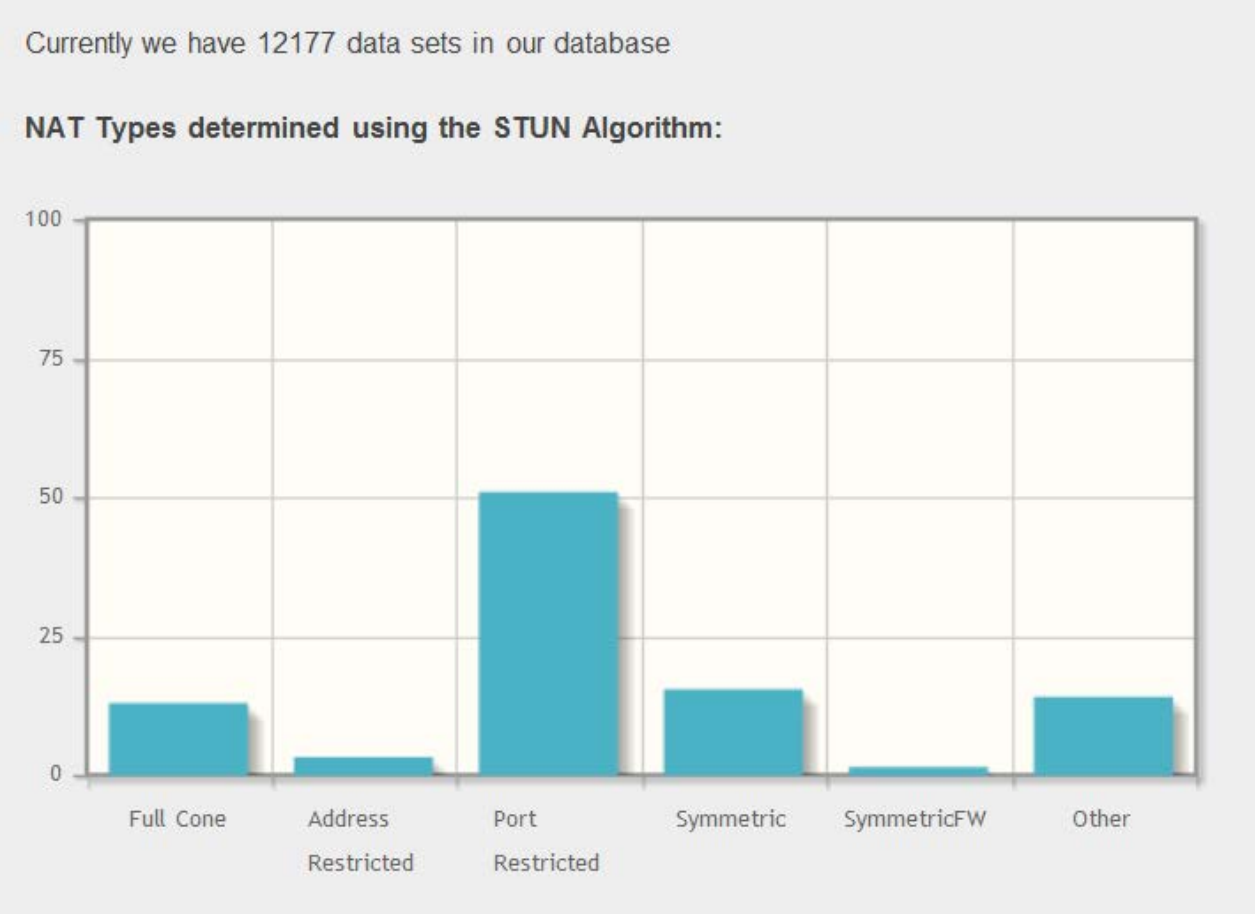

Рис. 2. Статистика существования NAT по типам

Обход NAT. Существующие механизмы позволяют обходить все конусные NAT, например, специально разработанный для этого высокоуровневый протокол STUN, подробно описан и закреплен в рекомендации RFC 5389. Рабочее предложение RFC (Request for Comments) — документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети. Однако, наибольшие трудности вызывает обход Symmetric (симметричного) NAT. У данного типа трансляции внешний порт меняется при каждом соединении, либо по истечении некоторого времени (обычно 20–60 секунд). Симметричный NAT принимает пакеты с ip:port только от узла с которым самостоятельно установил соединение. До отправки во вне какого-либо пакета, сопоставления «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт» не существует в таблице маршрутизации NAT.

Способы обхода NAT:

1) Ретрансляция подключения через сторонний публичный сервер. Способ позволяет добиться 100% обхода любого NAT, однако переносит накладные расходы на сервер и снижает отказоустойчивость. Готовая реализация подобной ретрансляции — это протокол TURN.

2) Supernode — это ретрансляция через других клиентов сети, имеющих публичный адрес или конусный NAT [1].

3) STUN — это высокоуровневый сетевой протокол, который позволяет клиенту, находящемуся за сервером трансляции адресов (или за несколькими такими серверами),

определить свой внешний IP-адрес, способ трансляции адреса и порта во внешней сети, связанный с определённым внутренним номером порта [2].

4) ICE — это STUN + TURN. Пытается напрямую соединить клиентов по STUN, в случае неудачи начинает ретрансляцию посредством TURN.

5) Universal Plug and Play (UPnP) — набор сетевых протоколов, публикуемых форумом UPnP. Цель UPnP — универсальная автоматическая настройка сетевых устройств, как дома, так и в корпоративной среде. Состоит из набора сопутствующих протоколов, построенных на открытых интернет-стандартах. Позволяет открыть и перенаправить внешние порты, в том числе конфигурация передается NAT автоматически программным способом (внутри локальной сети) без физического доступа к NAT или его панели администратирования.

6) DMZ (англ. Demilitarized Zone — демилитаризованная зона, ДМЗ) — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. Позволяет открыть и перенаправить внешние порты. Настройка осуществляется вручную при непосредственном доступе к маршрутизатору.

7) Port triggering/forwarding где статическое перенаправление портов это Port Forwarding, а динамическое перенаправление портов Port Triggering. Обе функции позволяют открыть и перенаправить внешние порты. Настройка осуществляется вручную при непосредственном доступе к маршрутизатору.

8) UDP hole punching — метод установления прямого соединения между двумя клиентами спрятанными за NAT [3]. Для инициации соединения требуется третья сторона — сервер, который виден обоим клиентам. Он позволяет определить клиентам свои внешние адреса и порты, по которым в дальнейшем будет инициировано соединение.

9) ICMP hole punching — метод установления прямого соединения между двумя клиентами спрятанными за NAT [4]. В отличии от обычного UDP hole punching, метод не требует третьего сервера для определения внешних адресов. Алгоритм отправляет ICMP ECHO REQUEST запросы в UDP виде, с низким значением TTL (Time to live — предельный период времени или число итераций или переходов, за который набор данных (пакет) может существовать до своего исчезновения) инкрементируя TTL от 1 в надежде, что, где-то посередине между NAT клиента и другими промежуточными сетями (или близко к клиенту) TTL истечет. Тогда произойдет возврат сообщения TTL_EXPIRED. Но так как был использован UDP-протокол, источник спалит свой внешний порт, по которому, собственно, в дальнейшем можно установить общение. ICMP UDP поддерживается не всеми маршрутизаторами.

10) Подмена источника — в случае с симметричным NAT, входящие пакеты могут быть доставлены только от ip:port источника, которому клиент отправлял запрос самостоятельно. Подмена источника пакета другим клиентом позволит соответствовать этому требованию. Однако существуют механизмы распознавания фальсификации данных, некоторые сети, файерволы, провайдеры, которые блокируют подобные пакеты.

Заключение. Способы обхода NAT имеют каждый свои особенности. Ни один способ (кроме ретрансляции) не дает 100% гарантии преодоления симметричных NAT, однако их совокупное использование позволяет максимизировать успех.

Библиографический список.

1. IT Administrators Guide [электронный ресурс] / Skype Limited 2010. — Режим доступа : https://download.skype.com/share/business/guides/skype-it-administrators-guide.pdf (дата обращения: 12.05.2017).

2. RFC 3489 - STUN - Simple Traversal of User Datagram Protocol (UDP). Network Address Translators (NATs). J. Rosenberg, J. Weinberger, dynamicsoft, C. Huitema, Microsoft, R. Mahy, Cisco, March 2003. 47 с.

3. A New Method for Symmetric NAT Traversal in UDP and TCP (Yuan Wei, Daisuke Yamada, Suguru Yoshida, Shigeki Goto) — Режим доступа :

https://www.goto.info.waseda.ac.jp/~wei/file/wei-apan-v10.pdf (дата обращения: 10.05.2017).

4. Extended UDP Multiple Hole Punching Method to Traverse Large Scale NATs (Kazuhiro Tobe, Akihiro Shimoda, and Shigeki Goto) APAN Network Research Workshop 2010 at the 30th APAN Meeting August 9, 2010 Hanoi, Vietnam. 23 с.