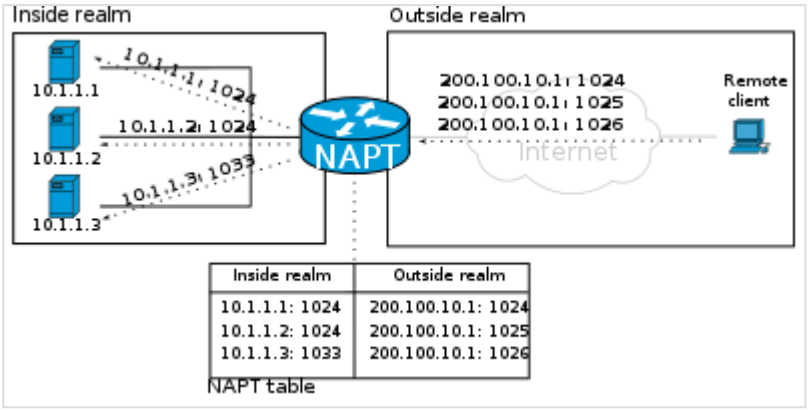
WIKIPEDIA
The Free Encyclopedia

Перенаправление порта

В компьютерных сетях переадресация **портов** или **сопоставление портов** — это приложение преобразования сетевых адресов (NAT), которое перенаправляет запрос на связь с одной комбинации адреса и номера порта на другую, пока пакеты проходят через сетевой шлюз, такой как маршрутизатор или брандмауэр . Этот метод чаще всего используется для того, чтобы сделать службы на хосте , находящемся в защищенной или замаскированной (внутренней) сети, доступными для хостов на противоположной стороне шлюза (внешняя сеть), путем переназначения IP-адреса назначения и номера порта связи на внутренний хост. [1] [2]



Переадресация портов через NAT-маршрутизатор

Цель

Переадресация портов облегчает подключение удаленных компьютеров, например, интернет -хостов, к определенному компьютеру или службе в локальной сети (LAN). [3]

В типичной жилой сети узлы получают доступ в Интернет через DSL или кабельный модем , подключенный к маршрутизатору или транслятору сетевых адресов (NAT/NAPT). Хосты в частной сети подключены к коммутатору Ethernet или взаимодействуют через беспроводную локальную сеть . Внешний интерфейс устройства NAT настроен с использованием публичного IP-адреса. С другой стороны, компьютеры за маршрутизатором невидимы для хостов в Интернете, поскольку каждый из них взаимодействует только с частным IP-адресом.

При настройке переадресации портов сетевой администратор выделяет один номер порта на шлюзе для исключительного использования для связи со службой в частной сети, расположенной на определенном хосте. Внешние хосты должны знать этот номер порта и адрес шлюза для связи с внутренней сетевой службой. Часто номера портов известных интернет-служб, такие как порт номер 80 для веб-служб (HTTP), используются при переадресации портов, чтобы общие интернет-службы могли быть реализованы на хостах в частных сетях.

Типичные области применения включают в себя следующее:

- Запуск публичного HTTP- сервера в частной локальной сети
- Разрешение доступа Secure Shell к хосту в частной локальной сети из Интернета
- Разрешение FTP- доступа к хосту в частной локальной сети из Интернета
- Запуск общедоступного игрового сервера в частной локальной сети

Администраторы настраивают переадресацию портов в операционной системе шлюза. В ядрах Linux это достигается с помощью правил фильтрации пакетов в компонентах ядра iptables или netfilter . Операционные системы BSD и macOS до Yosemite (OS 10.10.X) реализуют ее в модуле Ipfirewall

(ipfw), а операционные системы macOS , начиная с Yosemite, реализуют ее в модуле Packet Filter (pf).

При использовании на шлюзовых устройствах переадресация портов может быть реализована с помощью одного правила для трансляции адреса назначения и порта. (В ядрах Linux это правило DNAT). Исходный адрес и порт в этом случае остаются неизменными. При использовании на машинах, которые не являются шлюзом по умолчанию в сети, исходный адрес должен быть изменен на адрес транслирующей машины, иначе пакеты будут обходить транслятор и соединение не будет установлено.

Когда переадресация портов реализуется прокси-процессом (например, на брандмауэрах прикладного уровня, брандмауэрах на основе SOCKS или через прокси-серверы TCP-цепи), то на самом деле пакеты не транслируются, проксируются только данные. Обычно это приводит к изменению исходного адреса (и номера порта) на адрес прокси-машины.

Обычно только один из частных хостов может использовать определенный перенаправленный порт в один момент времени, но иногда возможна настройка для дифференциации доступа по исходному адресу исходного хоста.

Unix-подобные операционные системы иногда используют переадресацию портов, где номера портов меньше 1024 могут быть созданы только программным обеспечением, работающим от имени пользователя root. Запуск с привилегиями суперпользователя (для привязки порта) может представлять угрозу безопасности для хоста, поэтому переадресация портов используется для перенаправления порта с низким номером на другой порт с высоким номером, чтобы прикладное программное обеспечение могло выполняться от имени обычного пользователя операционной системы с ограниченными привилегиями.

Протокол Universal Plug and Play (UPnP) предоставляет функцию автоматической установки экземпляров переадресации портов в домашних интернет-шлюзах. UPnP определяет протокол шлюзового устройства Интернета (IGD), который является сетевой службой, с помощью которой интернет-шлюз объявляет о своем присутствии в частной сети через протокол Simple Service Discovery Protocol (SSDP). Приложение, предоставляющее интернет-службу, может обнаружить такие шлюзы и использовать протокол UPnP IGD для резервирования номера порта на шлюзе и заставить шлюз пересылать пакеты на свой прослушивающий сокет .

Типы

Переадресацию портов можно разделить на следующие типы: локальная, удаленная и динамическая переадресация портов. [4]

Локальная переадресация портов

Локальная переадресация портов является наиболее распространенным типом переадресации портов. Она используется для того, чтобы позволить пользователю подключаться с локального компьютера к другому серверу, т. е. безопасно пересылать данные из другого клиентского приложения, запущенного на том же компьютере, что и клиент Secure Shell (SSH). Используя локальную переадресацию портов, можно обойти брандмауэры, блокирующие определенные веб-страницы. [5]

Подключения от клиента SSH перенаправляются через сервер SSH на предполагаемый сервер назначения. Сервер SSH настроен на перенаправление данных с указанного порта (который является локальным для хоста, на котором запущен клиент SSH) через защищенный туннель на определенный

хост и порт назначения. Локальный порт находится на том же компьютере, что и клиент SSH, и этот порт является «перенаправленным портом». На том же компьютере любой клиент, который хочет подключиться к тому же хосту и порту назначения, может быть настроен на подключение к перенаправленному порту (а не напрямую к хосту и порту назначения). После того, как это соединение установлено, клиент SSH прослушивает перенаправленный порт и направляет все данные, отправленные приложениями на этот порт, через защищенный туннель на сервер SSH. Сервер расшифровывает данные, а затем перенаправляет их на хост и порт назначения. [6]

Некоторые варианты использования локальной переадресации портов:

- Использование локальной переадресации портов для получения почты [7]
- Подключитесь с ноутбука к веб-сайту с помощью SSH-туннеля.

Удалённая переадресация портов

Эта форма переадресации портов позволяет приложениям на стороне сервера соединения Secure Shell (SSH) получать доступ к службам, находящимся на стороне клиента SSH. [8] В дополнение к SSH существуют фирменные схемы туннелирования, которые используют удаленную переадресацию портов для той же общей цели. [9] Другими словами, удаленная переадресация портов позволяет пользователям подключаться со стороны сервера туннеля, SSH или другого, к удаленной сетевой службе, расположенной на стороне клиента туннеля.

Для использования удаленной переадресации портов необходимо знать адрес сервера назначения (на стороне клиента туннеля) и два номера портов. Выбранные номера портов зависят от того, какое приложение будет использоваться.

Удаленная переадресация портов позволяет другим компьютерам получать доступ к приложениям, размещенным на удаленных серверах. Два примера:

- Сотрудник компании размещает FTP-сервер у себя дома и хочет предоставить доступ к FTP-сервису сотрудникам, использующим компьютеры на рабочем месте. Чтобы сделать это, сотрудник может настроить удаленную переадресацию портов через SSH на внутренних компьютерах компании, включив адрес своего FTP-сервера и используя правильные номера портов для FTP (стандартный порт FTP — TCP/21) [10]
- Открытие сеансов удаленного рабочего стола — это распространенное использование удаленной переадресации портов. Через SSH это можно сделать, открыв виртуальный сетевой вычислительный порт (5900) и включив адрес конечного компьютера. [6]

Динамическая переадресация портов

Динамическая переадресация портов (DPF) — это метод обхода брандмауэра или NAT по требованию с использованием отверстий брандмауэра. Цель состоит в том, чтобы позволить клиентам безопасно подключаться к доверенному серверу, который выступает в качестве посредника для отправки/получения данных на один или несколько целевых серверов. [11]

DPF можно реализовать, настроив локальное приложение, например SSH, как прокси-сервер SOCKS, который можно использовать для обработки передачи данных через сеть или через Интернет. Программы, например веб-браузеры, должны быть настроены индивидуально для направления трафика через прокси, который действует как безопасный туннель на другой сервер. После того, как прокси больше не нужен, программы должны быть перенастроены на их первоначальные настройки. Из-за ручных требований DPF он нечасто используется. [6]

После установления соединения DPF может использоваться для обеспечения дополнительной безопасности для пользователя, подключенного к ненадежной сети. Поскольку данные должны пройти через защищенный туннель на другой сервер, прежде чем будут перенаправлены в исходное место назначения, пользователь защищен от перехвата пакетов, который может произойти в локальной сети. [12]

DPF — мощный инструмент со множеством применений; например, пользователь, подключенный к Интернету через кофейню, отель или иную минимально защищенную сеть, может захотеть использовать DPF как способ защиты данных. DPF также можно использовать для обхода брандмауэров, которые ограничивают доступ к внешним веб-сайтам, например, в корпоративных сетях.

См. также

- Протокол управления портами (PCP)
- Протокол сопоставления портов NAT (NAT-PMP)
- Отверстие в брандмауэре
- Обход NAT
- Пересылка пакетов
- Трансляция адреса порта (PAT)
- Запуск порта
- Адрес помощника UDP

Ссылки

1. "Определение: переадресация портов" (https://web.archive.org/web/20120603230244/http://www.pcmag.com/encyclopedia_term/0%2C1237%2Ct%3Dport+forwarding%26i%3D49509%2C00.asp) . PC Magazine . Архивировано из оригинала (https://www.pcmag.com/encyclopedia_term/0%2C1237%2Ct%3Dport+forwarding%26i%3D49509%2C00.asp) 2012-06-03 . Получено 2008-10-11 .
2. Рори Краузе. "Использование переадресации портов ssh для печати в удаленных местах" (http://www.linuxjournal.com/article/5462) . Linux Journal . Получено 11 октября 2008 г. (http://www.linuxjournal.com/article/5462)
3. Джефф "Крэш" Голдин. "Как настроить домашний веб-сервер" (https://web.archive.org/web/20081004123716/http://www.redhat.com/magazine/022aug06/features/webserver/) . Red Hat . Архивировано из оригинала (http://www.redhat.com/magazine/022aug06/features/webserver/) 2008-10-04 . Получено 2008-10-11 . (https://web.archive.org/web/20081004123716/http://www.redhat.com/magazine/022aug06/features/webserver/) (http://www.redhat.com/magazine/022aug06/features/webserver/)
4. Переадресация портов OpenSSH (https://help.ubuntu.com/community/SSH/OpenSSH/PortForwarding)
5. "Локальная и удаленная переадресация портов и отражение для защищенного ИТ-клиента 7.1 или выше - Техническая записка 2433" (http://support.attachmate.com/techdocs/2433.html) . Support.attachmate.com. 2012-11-09 . Получено 2014-01-30 . (http://support.attachmate.com/techdocs/2433.html)
6. "SSH/OpenSSH/PortForwarding - Community Ubuntu Documentation" (https://help.ubuntu.com/community/SSH/OpenSSH/PortForwarding). Help.ubuntu.com. 2013-12-13. Получено 2014-01-30 . (https://help.ubuntu.com/community/SSH/OpenSSH/PortForwarding)