**2 Лекция. МЭ. NAT.**

**NAT** (Network Address Translation — «преобразование сетевых адресов») — позволяет транслировать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation.

Преимущества:

1. Позволяет сэкономить IP-адреса транслируя несколько внутренних IP-адресов в один внешний реальный ("белый") IP-адрес.
2. Позволяет назначать всем абонентам защищаемой сети IP-адреса из частной (фиктивной) адресной зоны (например, **192.168.х.х, 10.х.х.х**), это исключает возможность доступа в защищаемую  сеть из реального адресного пространства внешней сети
3. Обеспечивает полное сокрытие внутренней структуры (адреса и порты) частной сети.

Недостатки:

1. Не все протоколы могут "преодолеть" NAT.  (например, FTP с активным режимом).
2. Из-за трансляции адресов "много в один" появляются дополнительные сложности с идентификацией пользователей, все пользователи работают под одним внешним адресом.
3. Иллюзия DoS-атаки. При подключении многих пользователей к одному и тому же сервису возникает иллюзия DoS-атаки на сервис т.к. все они работают из под одного адреса.
4. В некоторых случаях, необходимость в дополнительной настройки статического NAT или PAD (Port address translation).

Самый простой NAT -**статический NAT**.

Каждому внутреннему локальному адресу присваивается внутренний глобальный адрес.

Преимущества:

1. Простота реализации.
2. Из глобальной сети можно обращаться к компьютерам в локальной сети (серверам).

Недостатки:

1. Каждому компьютеру в локальной сети необходим глобальный адрес.

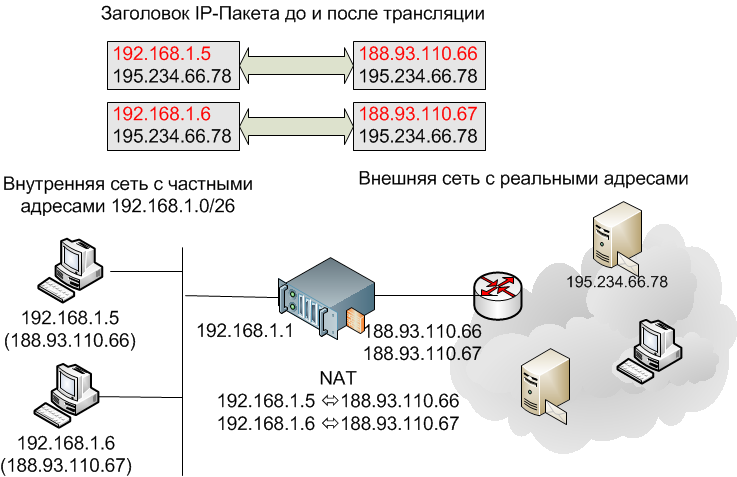


Рис. Статический NAT

Все преобразования делаются с помощью таблицы.

Таблица статического NAT.

|  |  |
| --- | --- |
| **Фиктивный адрес (внутренний локальный)** | **Реальный адрес (внутренний глобальный)** |
| **192.168.1.5** | **188.93.110.66** |
| **192.168.1.6** | **188.93.110.66** |

**Динамический  NAT.**

NAT Overload. NAPT, PAT, masquerading.

Преимущества:

1. Всем компьютерам в локальной сети необходим один глобальный адрес.

Недостатки:

1. Сложнее в реализации.
2. Ограничений на общее количество соединений равное количеству портов (216)
3. Из глобальной сети нельзя обращаться к компьютерам в локальной сети (серверам).

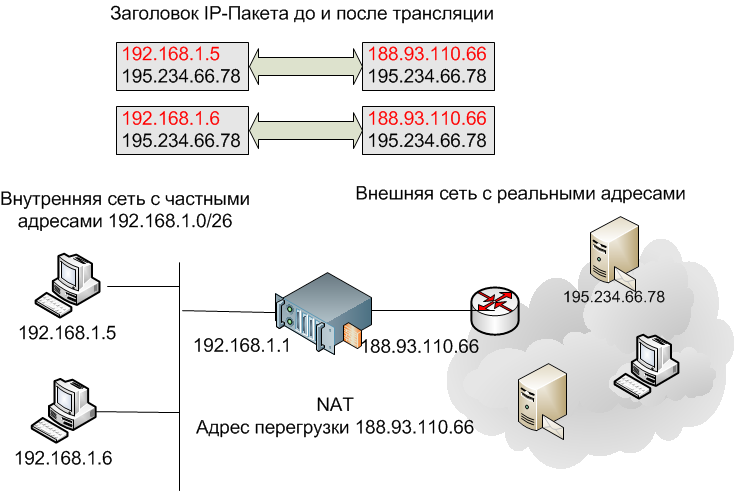
****

Рис. Динамический NAT

Обойтись только адресами в этом случае нельзя, т.к. глобальный адрес один (адрес перегрузки).

Поэтому для идентификации используются порты.

Таблица динамического NAT.

|  |  |  |
| --- | --- | --- |
| **Внутренний локальный адрес:порт** | **Адрес перегрузки:порт** | **Внешний глобальный адрес:порт** |
| **192.168.1.5:1027** | **188.93.110.66:15045** | **195.234.66.78:25** |
| **192.168.1.6:1027** | **188.93.110.66:24576** | **195.234.66.78:80** |
| **192.168.1.5:2023** | **188.93.110.66:23124** | **195.234.66.78:80** |
| **192.168.1.6:2374** | **188.93.110.66:62323** | **195.234.66.78:25** |

**Цепочка прохождения пакетов.**

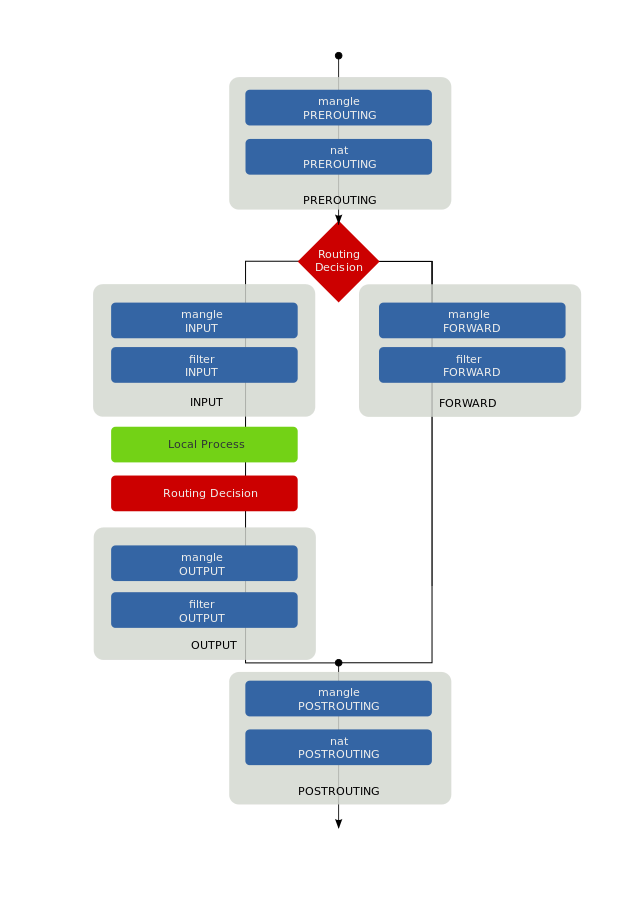


Рис. Цепочка прохождения пакетов в Iptables