# 9 Межсетевой экран. Введение, NAT, Proxy

## Межсетевой Экран (МЭ)

устройство (программа), которое управляет доступом (выходом) в частную сеть или компьютер.

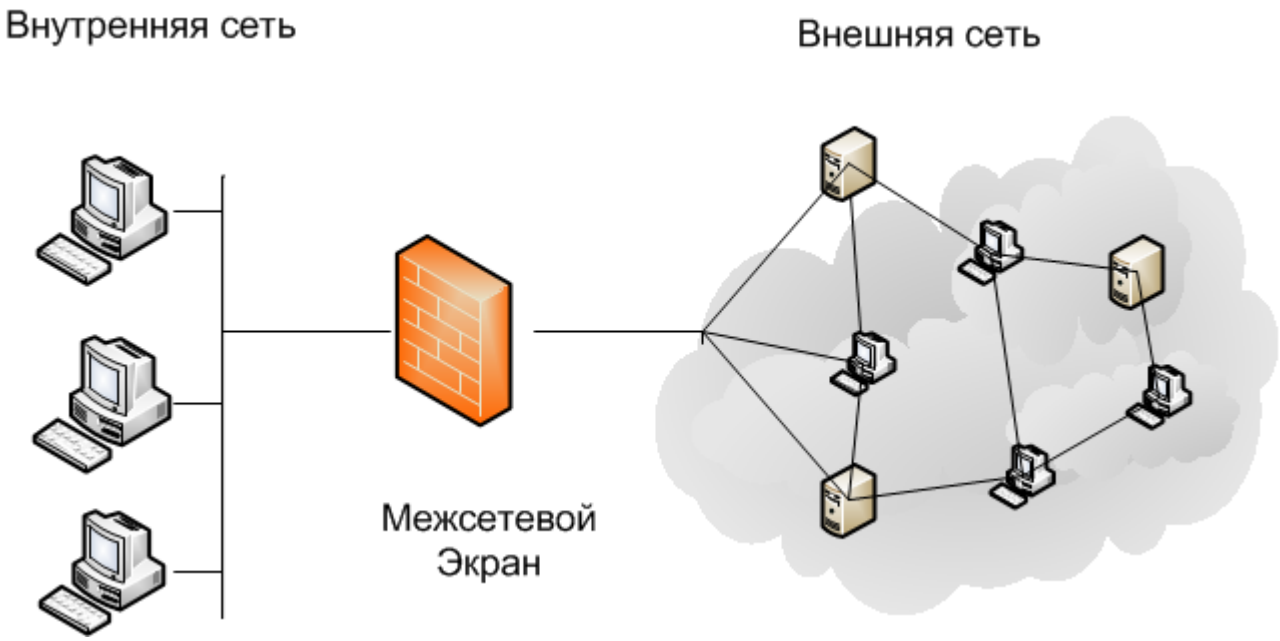



Рис. Межсетевой экран

**Места применения МЭ:**

- На персональном компьютере
- На маршрутизаторе между сегментами локальной сети
- На шлюзе из локальной сети во внешнею (глобальную) сеть
- На сервере удаленного доступа
- На сервер, МЭ уровня приложений (например: ModSecurity для фильтрации запросов (ответов) к HTTP-серверу)


**Функции межсетевого экрана:**

- **Фильтрация** - фильтры отсеивают нежелательные пакеты (запросы), на основе содержимого полей (адресов отправителя и получателя, номерам протоколов, номерам портов прикладных сервисов, флагов управления и т.д.) или запросов на прикладном уровне.
- **Трансляция сетевых адресов NAT (Network Address Translation)** – обеспечивает сокрытие внутренней структуры частной сети.
- **Туннелирование** (VPN - Virtual Private Network) - инкапсуляция IP-датаграмм в транспортные IP-датаграммы позволяет скрыть, с применением шифрования и аутентификации, IP-обмен между виртуальными частными сетями.
- **Proxy-сервер** - полная обработка прикладных данных (например: размер файлов, содержимое файлов).
- **Регистрация событий** - анализ и регистрация трафика и обнаружение фактов нарушения защиты.

# 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.x.x, 10.x.x.x**), 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**.

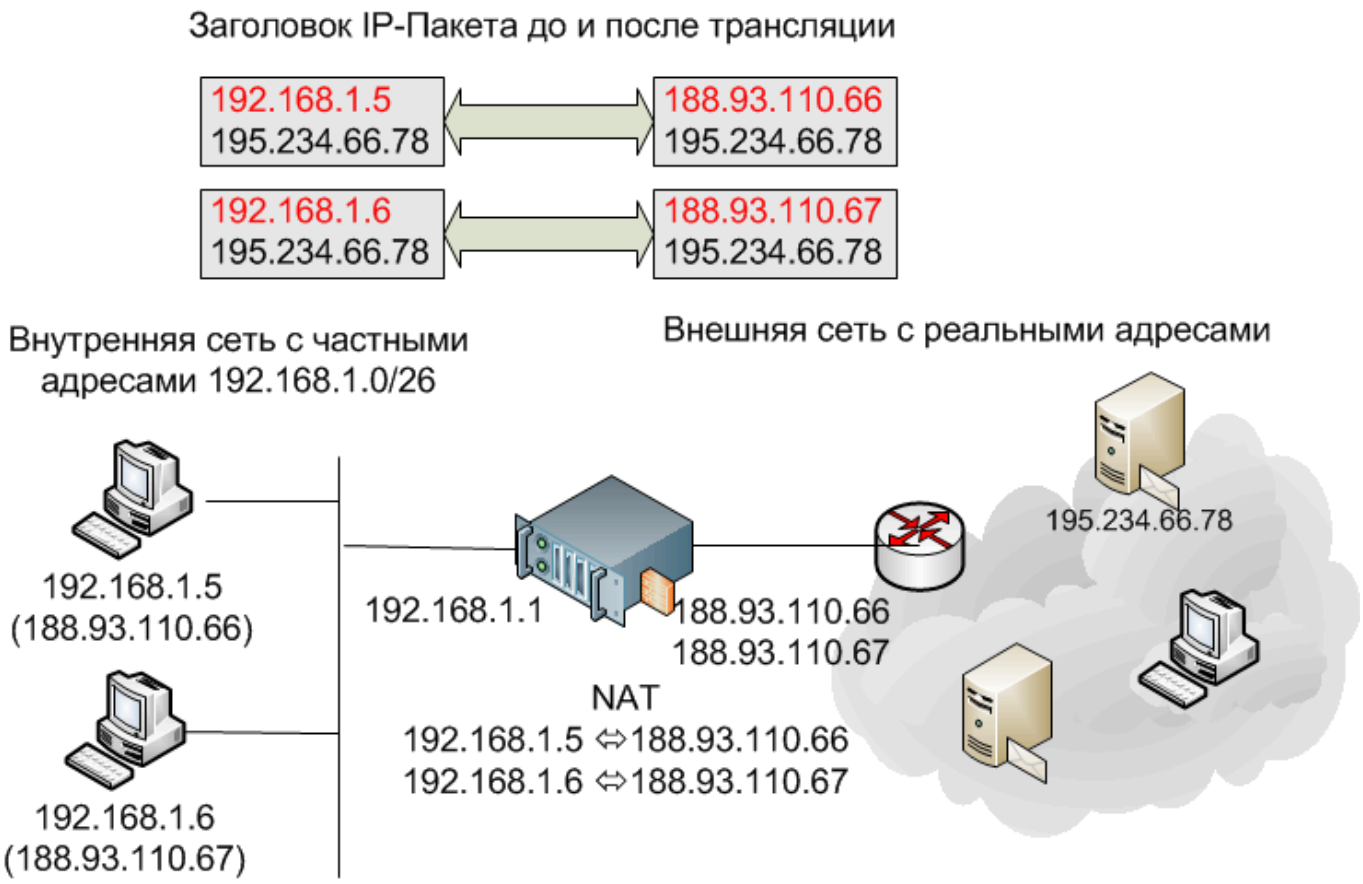
Каждому внутреннему локальному адресу присваивается внутренний глобальный адрес.

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.




Все преобразования делаются с помощью таблицы.

| 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.

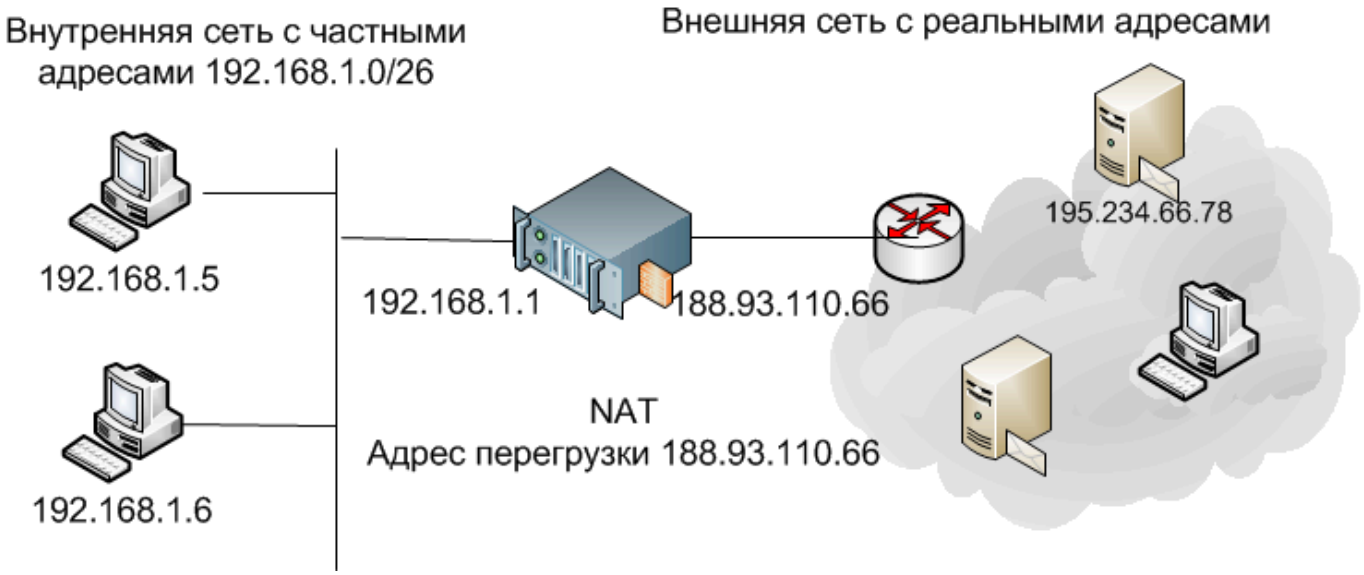
Преимущества:

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).

**

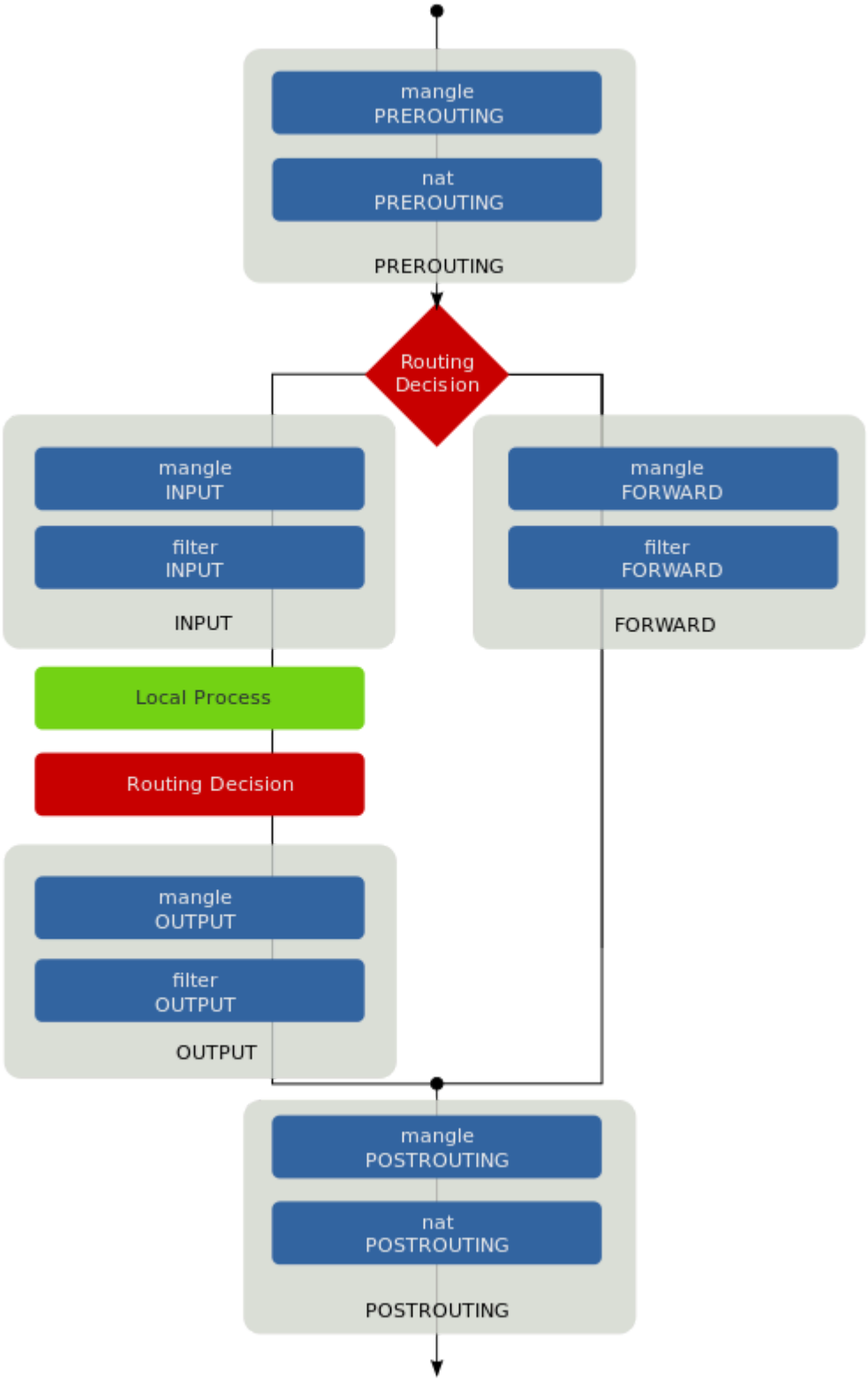




Обойтись только адресами в этом случае нельзя, т.к. глобальный адрес один (адрес перегрузки).

Поэтому для идентификации используются порты.

| 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.


mangle
PREROUTING
nat
PREROUTING
PREROUTING
Routing
Decision
mangle
INPUT
filter
INPUT
INPUT
mangle
FORWARD
filter
FORWARD
FORWARD
Local Process
Routing Decision
mangle
OUTPUT
filter
OUTPUT
OUTPUT
mangle
POSTROUTING
nat
POSTROUTING
POSTROUTING

**PROXY**

Proxy делает полную обработку прикладных данных при их передаче от одного интерфейса к другому.

Достоинства:

- Полный контроль данных на прикладном уровне (например: проверка на вирусы и т.д.)

Недостатки:

- Медленная работа.
- Реализован не для всех протоколов.