**NAT** (Network Address Translation) – процесс трансляции лок.адресов во внешн.

Благодаря этому – доступ в интернет.

Существует 3 базовых концепции трансляции адресов:

\*статическая (Static NAT)

\*динамическая (Dynamic NAT)

\*маскарадная (NAPT, NAT Overload, PAT)

**Стат.NAT –** отображ.незарег.IP на зарег. IP на осн.1к1.

**Динам.NAT** – отображ.незарег.IP на зарег.IP от группы зарег. IP.

**Перегруж.NAT** – форма динам.NAT, кот.отображ.неск незарег.IP в единств.зарег.IP, исп-я порты (известен как PAT)

**Ф-ции NAT:**

1. Экономия IP-адресов
2. Предотвр/огран.обращ.снаружи ко внутр.хостам, оставляя возм-сть обращения изнутри наружу
3. Позвол.скрыть опред.внутр.сервисы внутр.хостов/сервисов.

**Недостатки:**

1. При его ис-нии хосты интернет взаимод.напрямую с нат-ус-вом, не с реальным хостом в частной сети
2. Исп-ние NAT усложняет работу админов
3. Не все протоколы могут «преодолеть» NAT

**Межсетевой экран (сетевой) –** комплекс аппаратных или ПС, осущ-щий контроль и фильтрацию проходящий через него сетевых пакетов в соотв.с зад.правилами. Защищает соединяемую с интернет корпорат.сеть от проникновения извне и сключ.возм-сть доступа к конфид.инфе.

**Межсетевой экран:**

* Пакетный фильтр
* Шлюз сеансового уровня
* Шлюз прикладного уровня
* Stateful Packet Inspection

Браундмауэр типа **пакетный фильтр** явл.наиб.простыми. Они раб.на сет.ур. модели OSI или на IP-уровне стека протоколов TCP/IP

**Шлюзы сеансового уровня** – брандмауэр, кот раб.на сеанс.ур.модели OSI или на TCP стека протоколов TCP/IP. Отслеживают процессы установл.TCP-соед.и позвол.опред., явл ли д-й сеанс легитимным.

**Шлюзы прикладного ур (proxy-сервер) –** функционир на прикл.ур модели OSI . Прикладной ур.отвеч.за доступ приложений в сеть. К задачам относ: перенос файлов, обмен почт.сообщ и упр-ние сетью.

**Stateful Packet Inspection** – объединяет в себе преим.пакетных фильтров, шлюзов сеанс.ур-ня и шлюзов прикладного ур. Т.е.фактически речь идет о многоур.брандмауэрах, кот.раб.одноврем.на сетевом, сеан и прикл.ур-нях.

**Прокси-сервер** – служба в комп.сетях, позволяющая К вып-ть косв.запросы к др.сетевым службам.

**Исп-ние:**

1. Обеспечение доступа с компьютеров локальной сети в Интернет
2. Кэширование данных
3. Сжатие данных
4. Защита локальной сети от внешнего доступа
5. Ограничение доступа из локальной сети к внешней
6. Анонимизация доступа к различным ресурсам.

**Ремейлер** – сервер, кот.получ.сообщэл.почты и перенапрвл.его по адресу, указанному отправителем. В проц.переадресации вся инфа об отправителе уничтож., поэтому конечн.получатель лишен возм-сти выяснить, кто явл. автором сообщ.

**2 типа ремейлеров:**

\*псевдо-анонимные

Его оп-р знает адрес эл.почты, кот.необх.для получ.ответа на письмо. Тайна связи полностью завис.от оператора, кот.м.стать жертвой угорз, шантажа или соц.инженерии. Преимущество – юзабилити.

\*анонимные

Им.гораздо более выс.секретность, но при этом сложнее в исп-нии. Операторы не м.знать какие д-е пересыл.через них, а поэтому нет гарантии своеврем.доставки сообщ, кот.м.затеряться. Преимущество – надежно скрывают реальный адрес и содержимое сообщ.

**Moxminion –** стандарт реализации 3 типа протокола анон.пересылки эл.почты. М.отсыл.и приним.анон.сообщ.эл.почты.