**4 Лекция. МЭ. Фильтры.**

**Межсетевой Экран (МЭ)**

**Фильтры**

Фильтры могут работать на разных уровнях модели OSI.

На каждом интерфейсе фильтры могут быть установлены как на входе, так и на выходе. Но оптимальнее фильтры ставить именно на входе, т.к. пакеты предназначенные для уничтожения будут уничтожены сразу, что исключит их лишнею обработку.

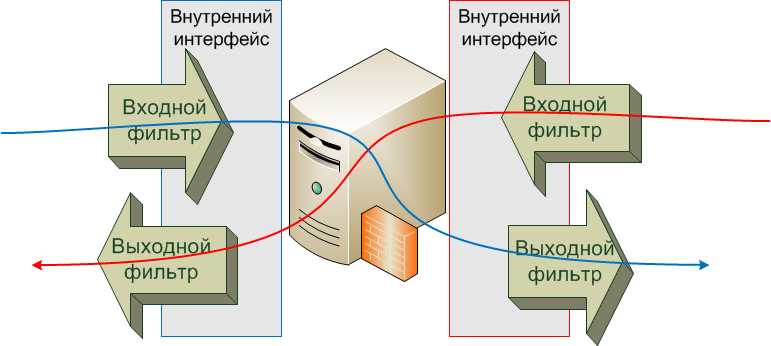


Рис. Фильтры на внешнем и внутреннем интерфейсах

**Два основных подхода составления фильтров:**

1. По умолчанию запретить все и разрешать избранное.
2. По умолчанию разрешить все и запрещать избранное.

Рассмотрим пример сети.

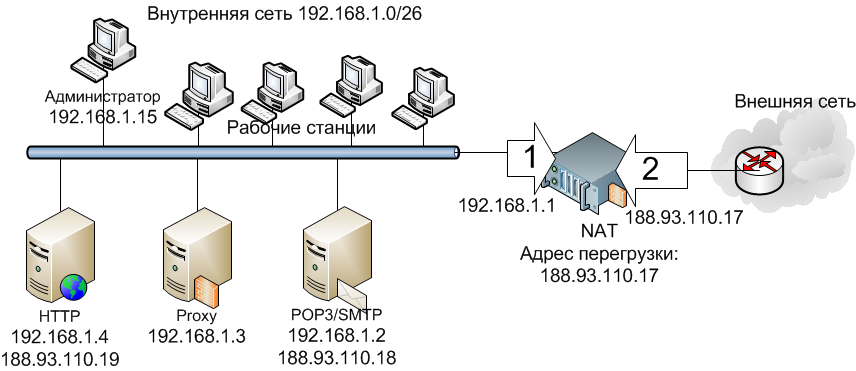


Рис. Пример локальной сети с выходом в Интернет.

Пример входящих фильтров на внутреннем интерфейсе (1) (по умолчанию все запрещено).

разрешить 192.168.1.2/32  0.0.0.0/00  ANY  25-25  (запросы почтового сервера в интернет SMTP)

разрешить 192.168.1.2/32  0.0.0.0/00  UDP  53-53  (запросы почтового сервера в интернет DNS)

разрешить 192.168.1.2/32  0.0.0.0/00  ANY  1025-65535 (ответы почтового сервера в Интернет)

разрешить 192.168.1.3/32  0.0.0.0/00  ANY  80-80  (запросы Proxy в интернет HTTP)

разрешить 192.168.1.3/32  0.0.0.0/00  ANY  20-21  (запросы Proxy в интернет FTP)

разрешить 192.168.1.3/32  0.0.0.0/00  UDP  53-53  (запросы Proxy в интернет DNS)

разрешить 192.168.1.4/32  0.0.0.0/00  ANY  1025-65535 (ответы HTTP сервера в Интернет)

разрешить 192.168.1.0/26  0.0.0.0/00  ICMP 0-0    (Ping в интернет)

разрешить 192.168.1.15/32 0.0.0.0/00  ANY  0-0    (Разрешить все администратору)

сбросить  0.0.0.0/00      0.0.0.0/00  ANY  0-0    (сбросить все)

Пример входящих фильтров на внешнем интерфейсе (2) (по умолчанию все запрещено).

разрешить 0.0.0.0/00  188.93.110.17/32  ANY  1025-65535 (ответы для Proxy и на Ping)

разрешить 0.0.0.0/00  188.93.110.18/32  ANY  1025-65535 (ответы для почтового сервера SMTP от других серверов)

разрешить 0.0.0.0/00  188.93.110.18/32  ANY  25-25  (запросы на почтовый сервер SMTP от других серверов)

разрешить 0.0.0.0/00  188.93.110.19/32  ANY  80-80  (запросы на HTTP сервер от внешних пользователей)

сбросить  0.0.0.0/00  0.0.0.0/00        ANY  0-0    (сбросить все)