10 Межсетевой экран. Фильтры, VPN

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 лишнюю обработку.

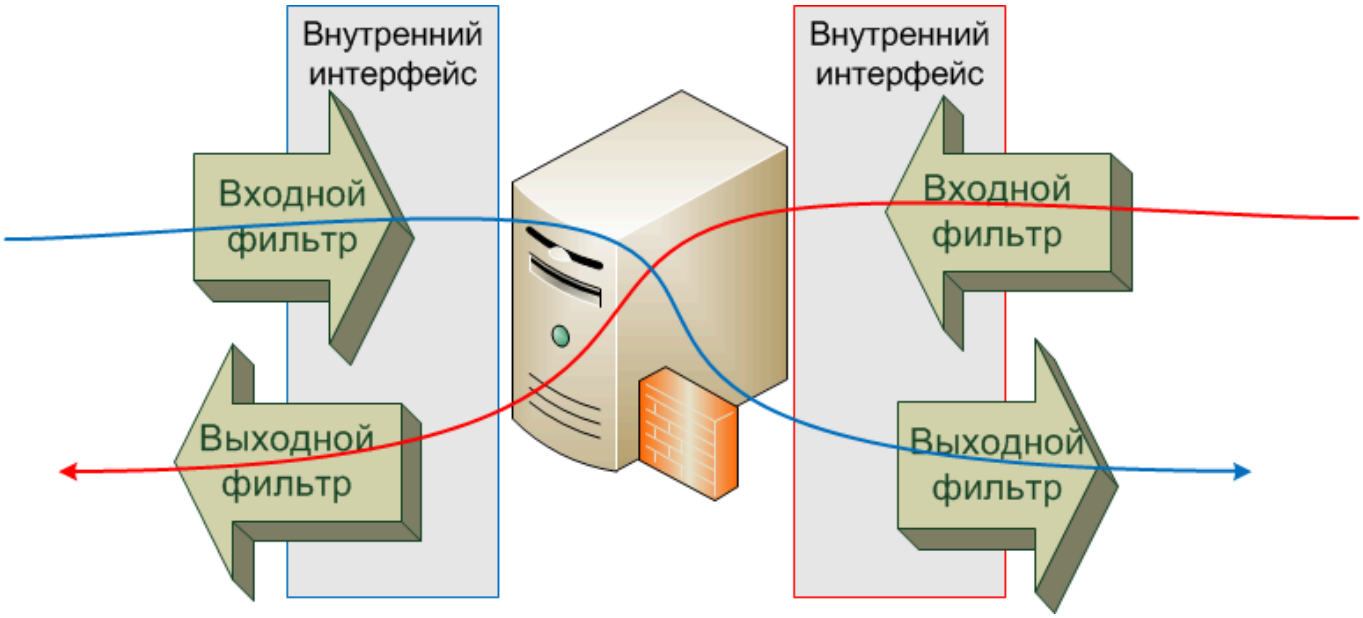


Рис. Фильтры на внешнем и внутреннем интерфейсах

Два основных подхода составления фильтров:

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

Рассмотрим пример сети.

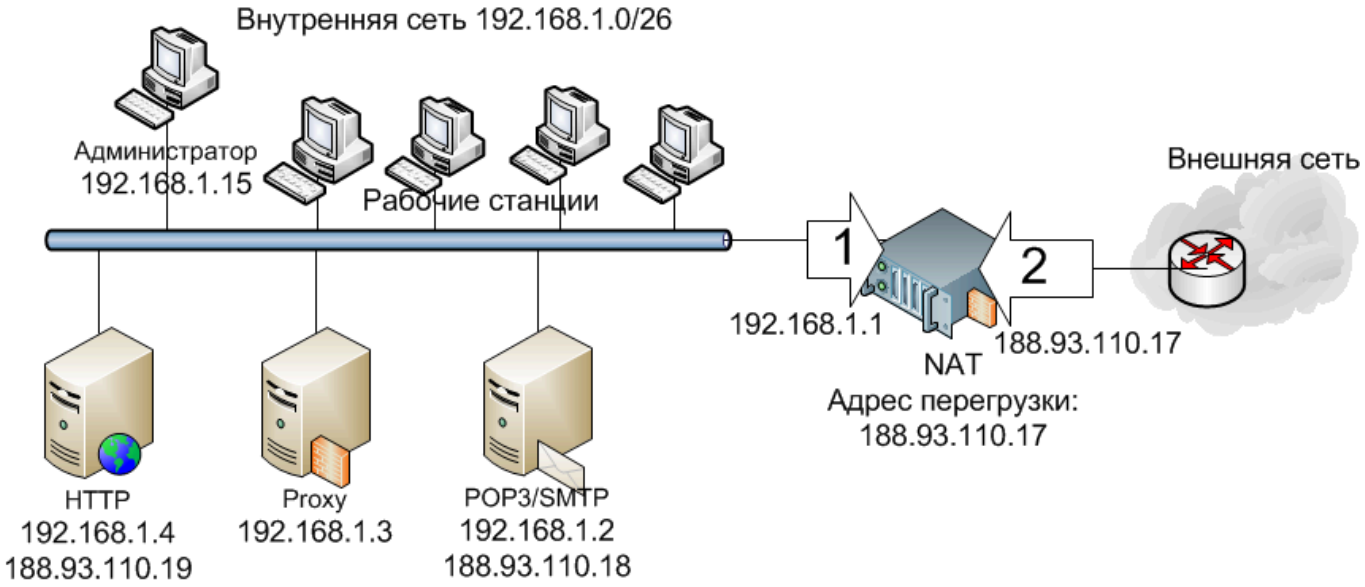


Рис. Пример локальной сети с выходом в Интернет.

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)

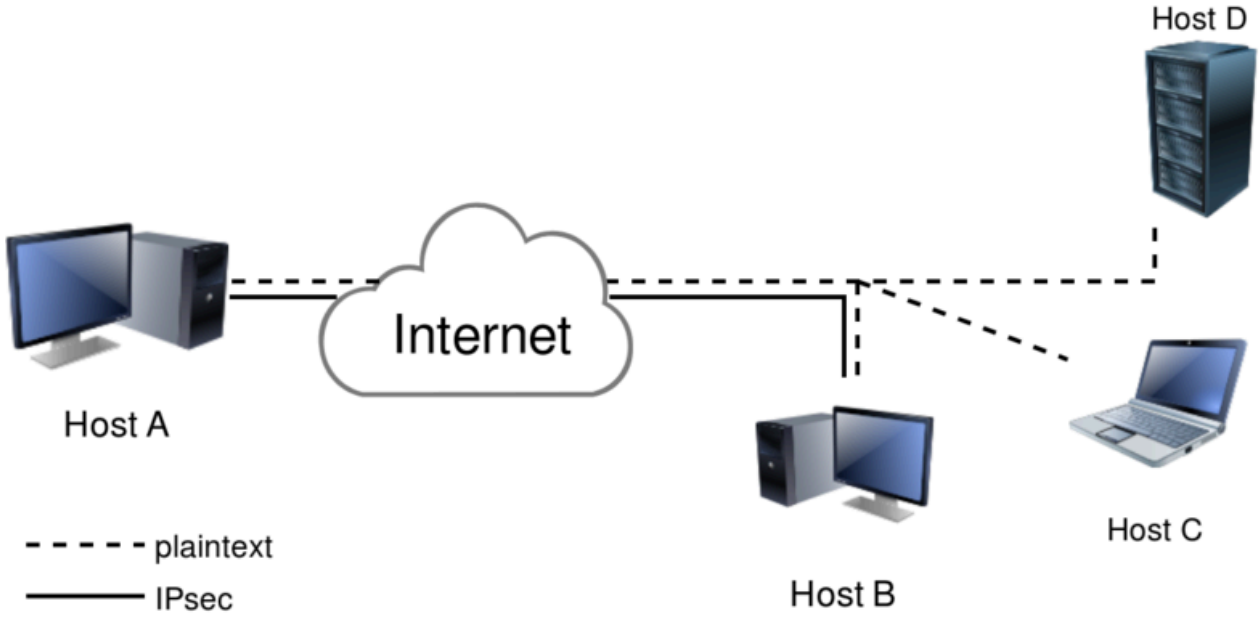
сбросить 0.0.0.0/00 0.0.0.0/00 ANY 0-0 (сбросить все)

VPN

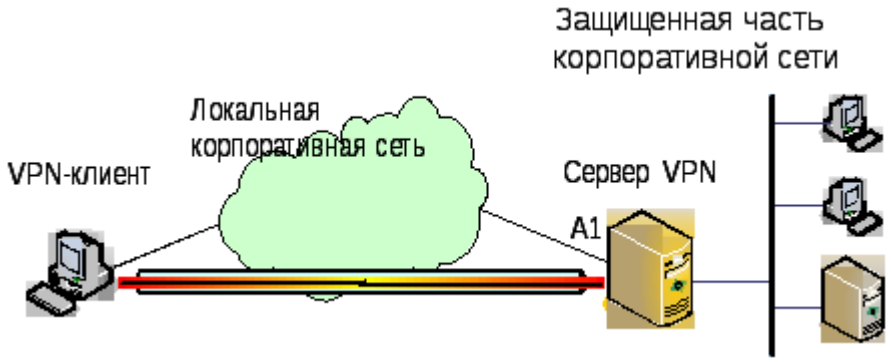
VPN (Virtual Private Network — виртуальная частная сеть)

С точки зрения задач можно разделить на:

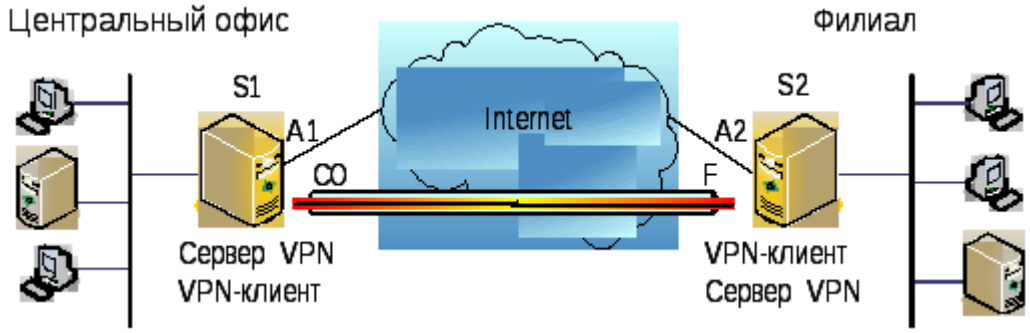
- **узел-узел** **(динамический)**
  (пример: создать VPN с другом)



- **узел-сеть (динамический)**
  (пример: командировочный подключается по VPN к корпоративной сети)



- **сеть-сеть (статический)**
  (пример: два здания одной организации соединены по VPN)



С точки зрения технологии построения можно разделить на:

- ***динамический - не фиксированный IP адрес МЭ***
- **статический** ****- фиксированные IP адреса МЭ

Основные технологии:

- IPsec
- OpenVPN

IPsec (IP Security)

IPSec работает на 3 уровне OSI (IP).

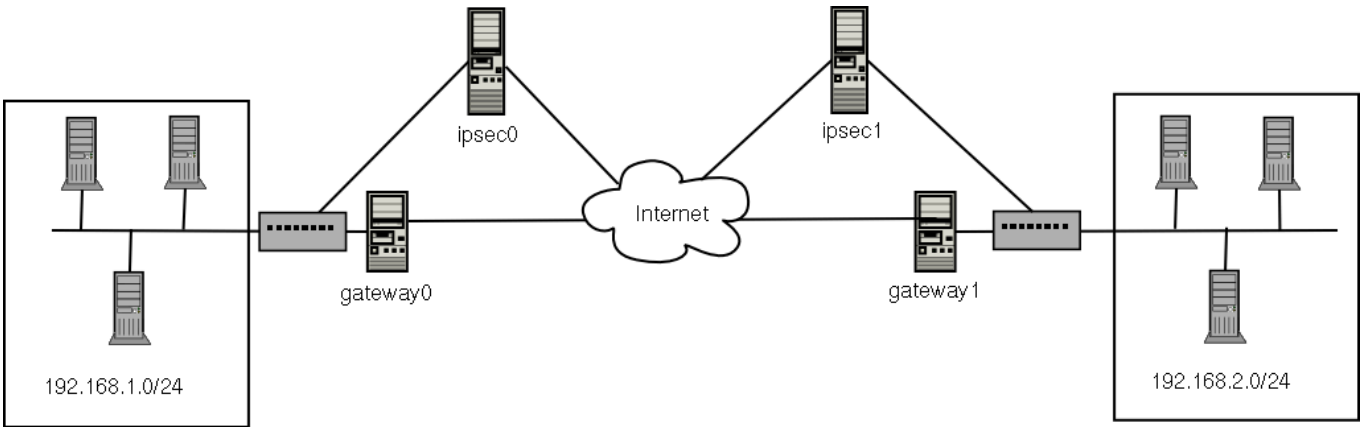


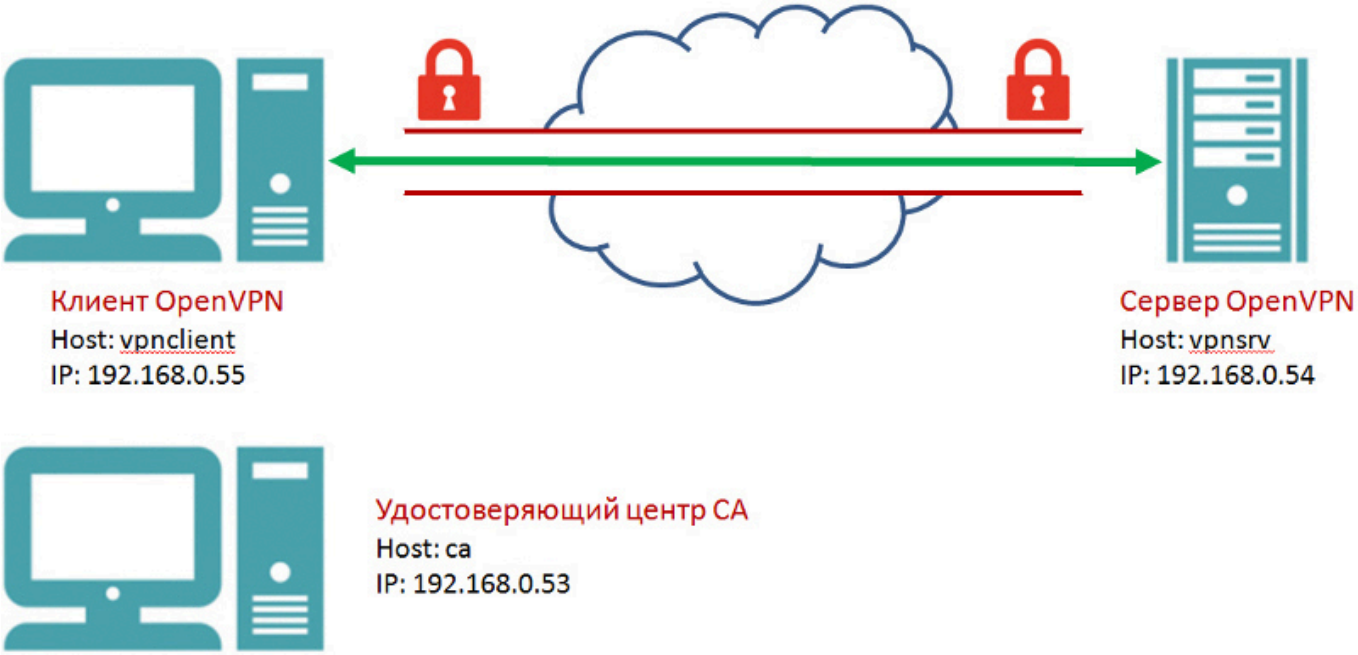
Рис. VPN "сеть-сеть" на IPSec.

Особенности:

- безопасен (зависит от выбранного алгоритма шифрования)
- стандартизирован (RFC, ГОСТ)
- проверен временем
- встроен в современных операционных системах
- работает в режиме ядра (быстрее, менее требователен к ресурсам)

OpenVPN

OpenVPN работает на уровне приложений (7-й модели OSI, 4-й TCP/IP) и инкапсулируя свои пакеты в TCP/UDP.



Особенности:

- безопасен (зависит от выбранного алгоритма шифрования)
- лучше возможности работы сквозь МЭ
- работает в режиме приложений
- необходимо стороннее программное обеспечение
- менее опробованный