Межсетевые экраны и proxy-серверы

Межсетевой экран, брандмауэр (firewall) – средство контроля доступа.

- Компьютер,
- маршрутизатор,
- специализированное устройство

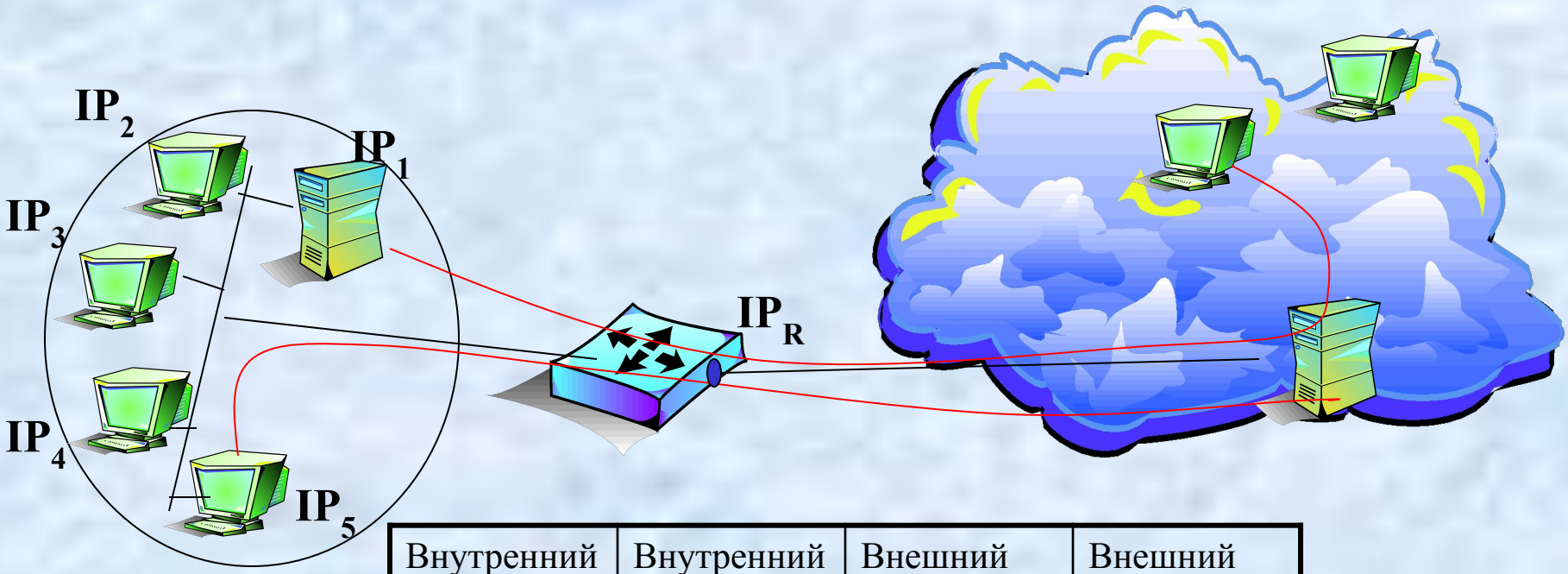
с установленным на нем специальным программным обеспечением, защищающим от попыток злоумышленников вторгнуться в сеть

Экран может разграничивать части корпоративной сети

Экраны базируются на двух основных приемах защиты:

- 1. пакетной фильтрации,
- 2. серверах-посредниках (proxy-server)

Технология трансляции сетевых адресов



Внутренний IP-адрес	Внутренний порт	Внешний IP-адрес	Внешний порт
IP_1	1025	IP_R	3451
IP_2	1080	IP_R	3452
IP_3	1334	IP_R	3453
IP_4	1080	IP_R	3454

Типы межсетевых экранов

Уровень архитектуры TCP/IP	Протоколы	Категория межсетевого экрана
Прикладной	Telnet, FTP, DNS, NFS, PING, SMTP, HTTP	Шлюз прикладного уровня, (application-level gateway), брандмауэр экспертного уровня (stateful inspection firewall)
Транспортный	TCP	Шлюз сеансового уровня (circuit-level gateway)
Уровень межсетевого взаимодействия	IP	экран с фильтрацией пакетов (packet-filtering firewall)

Packet filtering firewall

Брандмауэр с фильтрацией пакетов

Принцип работы:

- Фильтрует по заданному правилу на основе заголовков IP, TCP и UDP (IP- омера портов)
- Кроме адреса. Н заголовка пакета, никакая информация не проверяется

Преимущества:

- невысокая стоимость
- минимальное влияние на производительность сети

Недостатки:

- может оказаться достаточно сложной процедура настройки правил фильтрации пакетов
- уступают по уровню защиты другим типам межсетевых экранов
- злоумышленник может воспользоваться возможностью подмены полей IP-заголовка IP-spoofing

К брандмауэрам с фильтрацией пакетов может быть отнесен обычный маршрутизатор, поддерживающий функции фильтрации -
в Internet 80% маршрутизаторов
пакетных фильтров работают на базе

Шлюз сеансового уровня

- следит за установлением и допустимостью TCP-соединений
- После этого просто копирует и перенаправляет пакеты в обе стороны

Шлюз прикладного уровня

- функционирует в качестве посредника **(proxy-сервера)**
- пропускает только пакеты, сгенерированные теми приложениями, которые ему поручено обслуживать
- проверяет содержимое каждого проходящего через шлюз пакета

Достоинство:

высокий уровень защиты

Недостатки:

- обработка трафика требует больших вычислительных затрат
- наличие посредника между клиентом и сервером часто не является полностью незаметным для пользователей

Примеры

Black Hole компании Milkyway Networks

Eagle компании Raptor Systems

Брандмауэры экспертного уровня

- могут фильтровать трафик на основании данных полученных из заголовков пакетов
- могут контролировать установление сеансов
- могут работать на прикладном уровне, выполняя отбраковку пакетов, анализируя их содержимое.
- устанавливают **прямые соединения** между клиентами и внешними хостами
- вместо proxy-серверов используют специальные алгоритмы распознавания и обработки данных на уровне приложений
- "прозрачны" для пользователей
- не требуют внесения изменений в клиентское ПО

Один из самых популярных коммерческих брандмауэров экспертного уровня **FireWall-1** компании Check Point Software Technologies

Взаимное расположение Firewall’a и VPN-шлюза

A) VPN-шлюз перед firewall’ом

Недостаток:

VPN-шлюз принимает на себя все внешние атаки по незашифрованному трафику

Взаимное расположение Firewall’a и VPN-шлюза

B) VPN-шлюз позади firewall’a

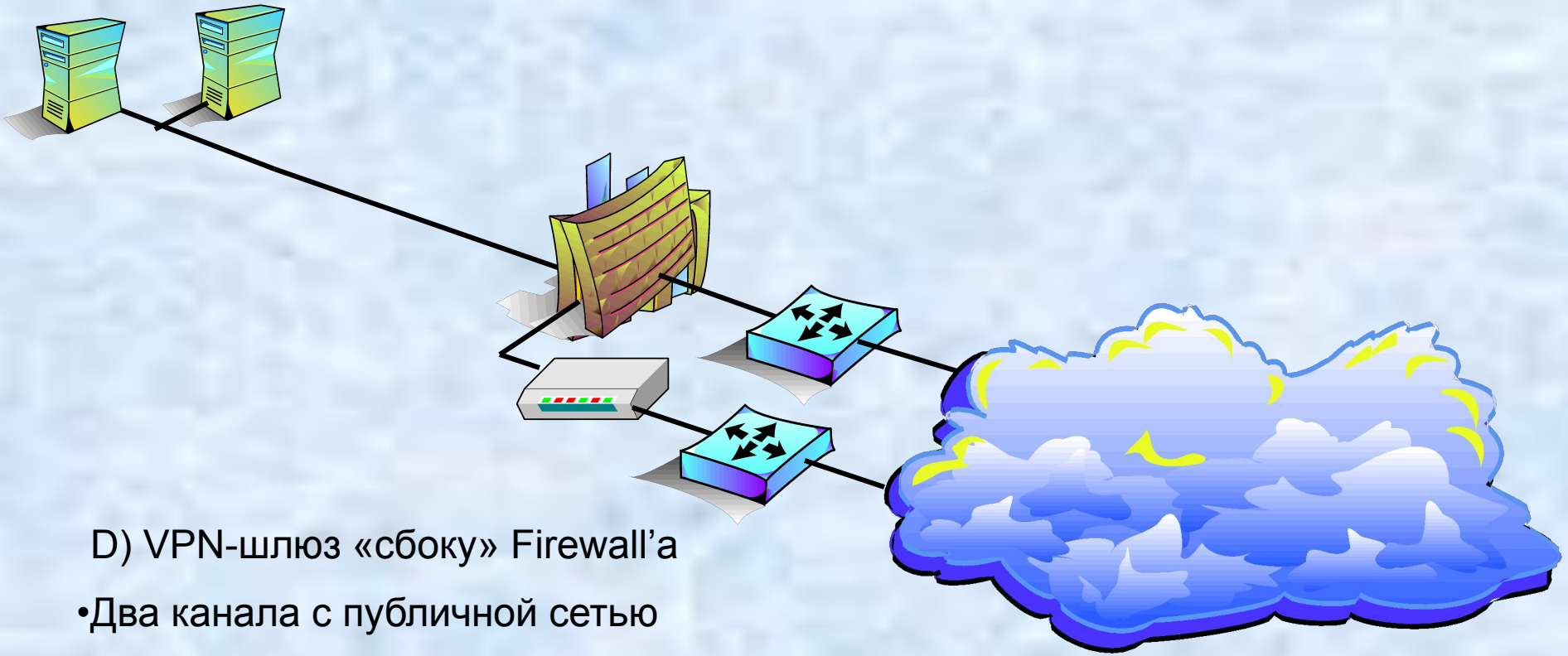
- Защищенность улучшается
- Firewall отражает все внешние атаки
- Firewall должен пропускать зашифрованный трафик

Взаимное расположение Firewall’a и VPN-шлюза

C) VPN-шлюз совмещен с Firewall’ом

- Наиболее привлекательное решение
- Просто администрировать - единая аутентификация
- Высокие требования к производительности интегрированного устройства
- Нельзя применить для standalone VPN-шлюзов

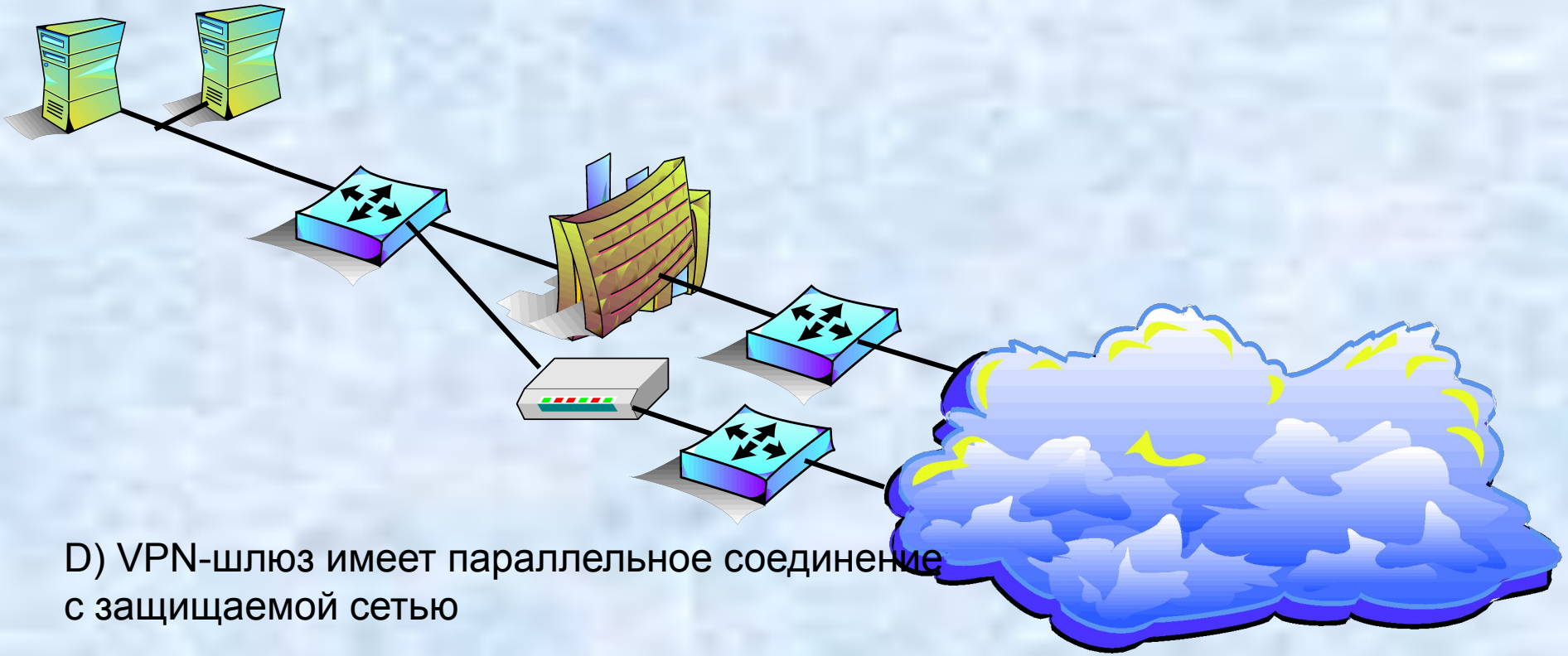
Взаимное расположение Firewall’a и VPN-шлюза



D) VPN-шлюз «сбоку» Firewall’a

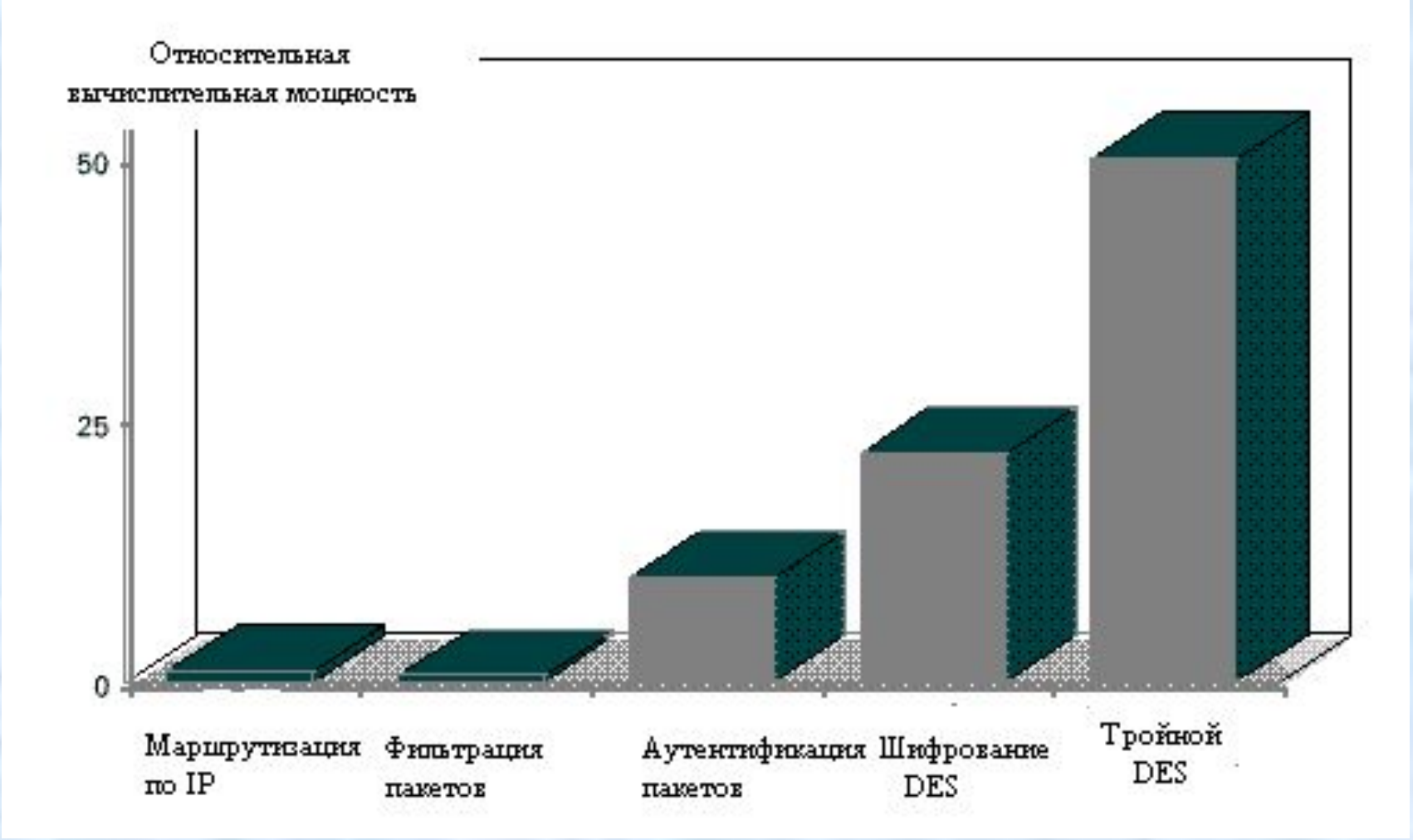
- Два канала с публичной сетью
- Зашифрованный трафик обрабатывается VPN-шлюзом, а затем - Firewall’ом
- Высокая надежность защиты
- Высокая надежность соединения с публичной сетью (резервирование каналов)

Взаимное расположение Firewall'а и VPN-шлюза



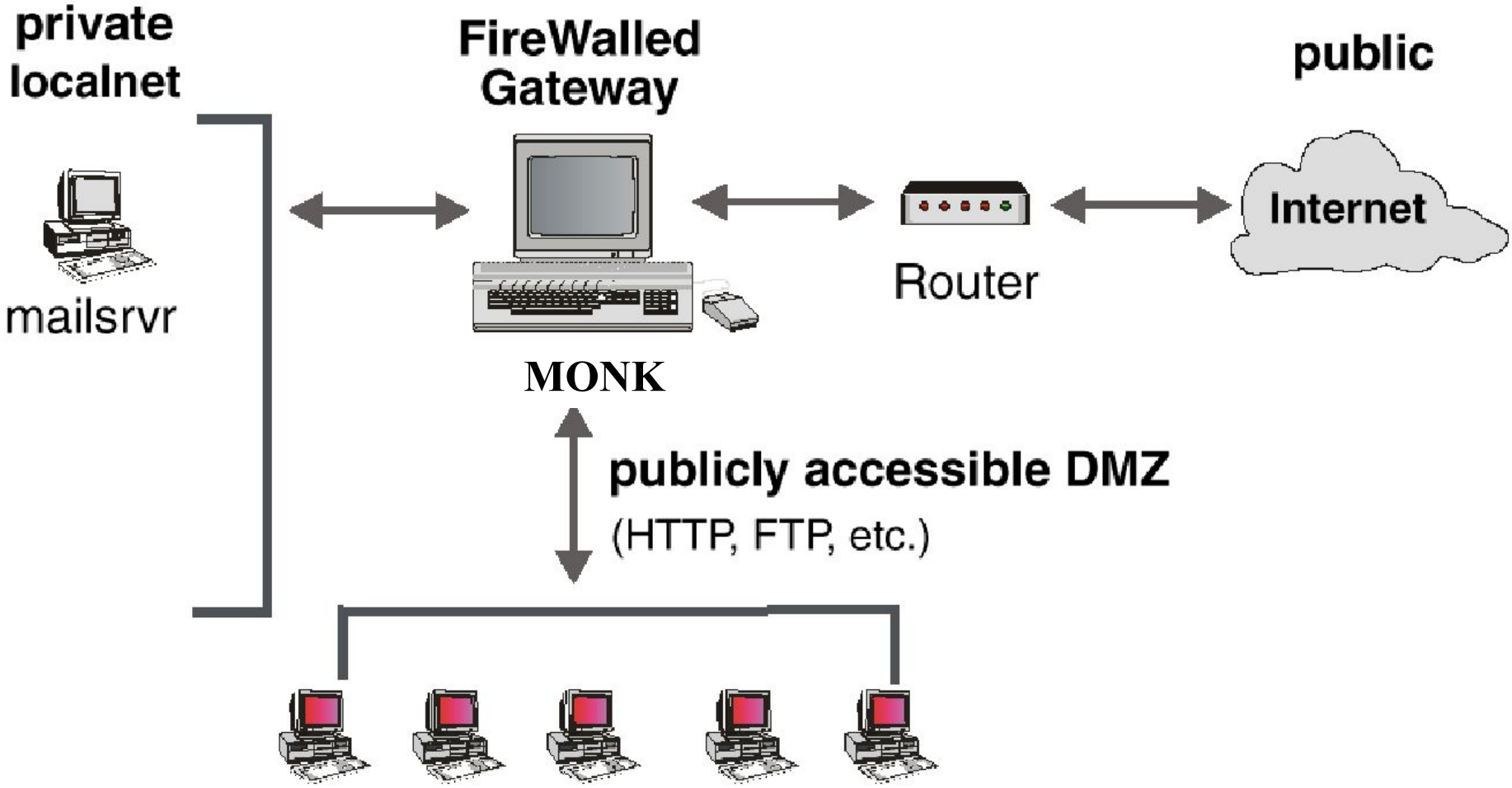
D) VPN-шлюз имеет параллельное соединение с защищаемой сетью

- Недостаточная степень защиты - зашифрованный трафик не проходит через firewall
- Высокая надежность соединения с публичной сетью (резервирование каналов)

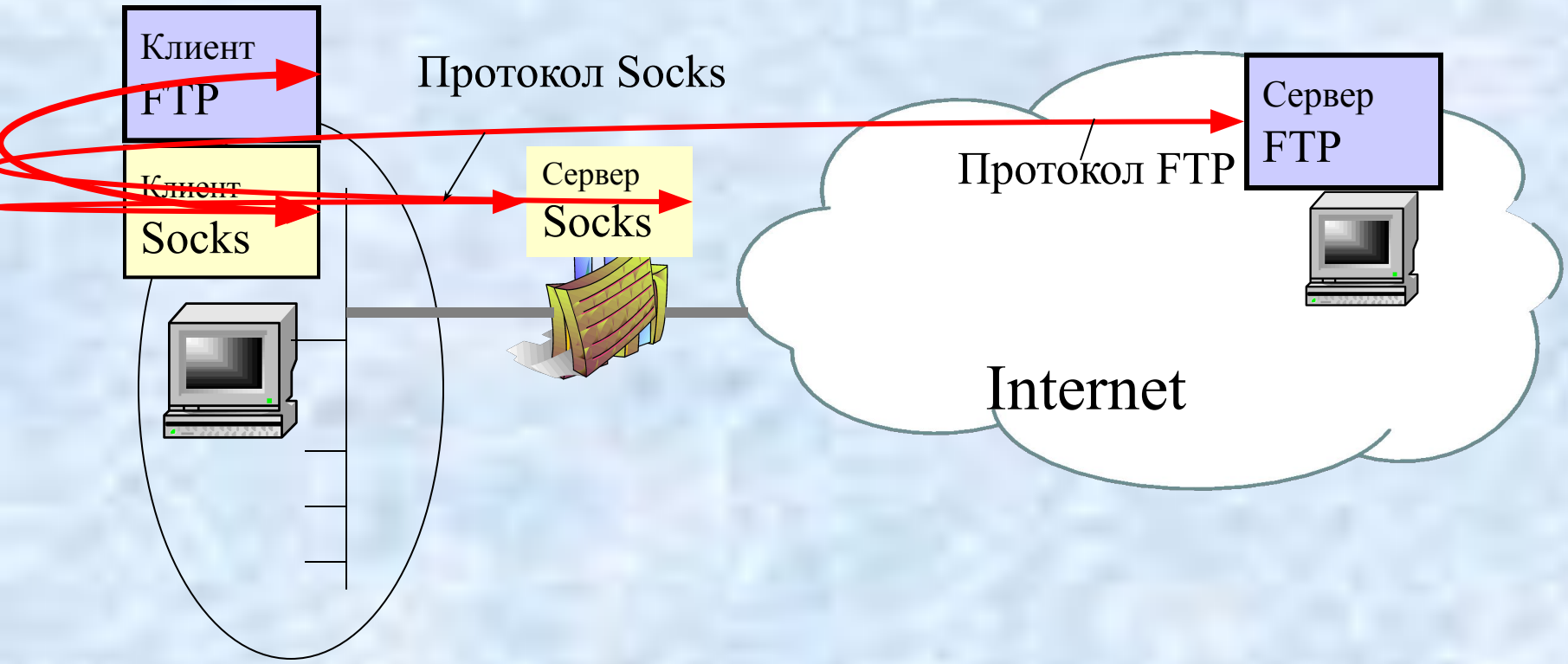


Относительная вычислительная мощность, требуемая для выполнения основных операций маршрутизатора, брандмауэра и устройства VPN

Пример применения FireWall-1



Сервер-посредник (proxy-server)



Сервер-посредник (proxy-server)