Межсетевые экраны

Сети и системы телекоммуникаций

Межсетевые экраны

Принцип проектирования сетей TCP/IP

- Каждый компьютер может соединиться с любым другим компьютером в сети

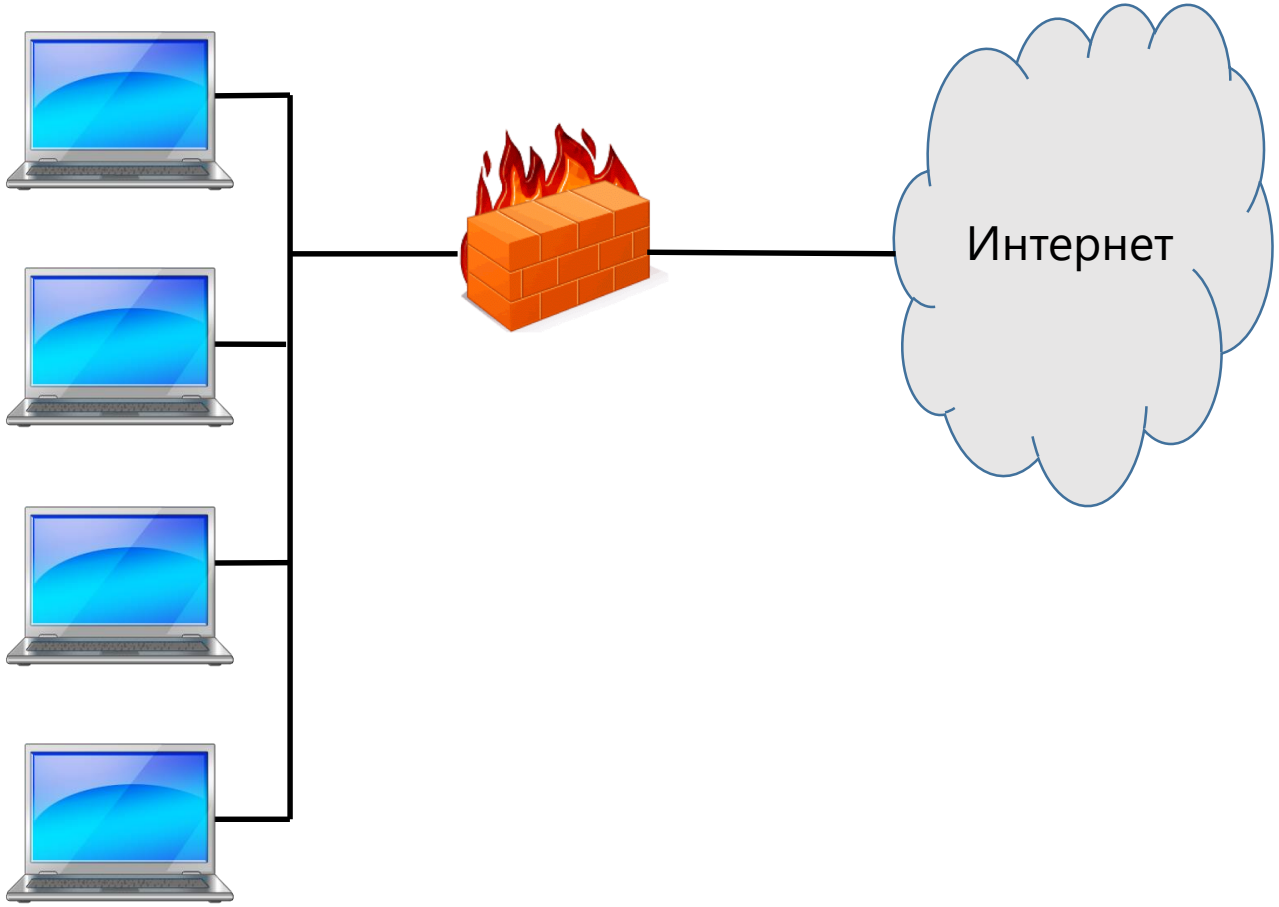
Безопасность

- Сейчас в Интернет много злоумышленников

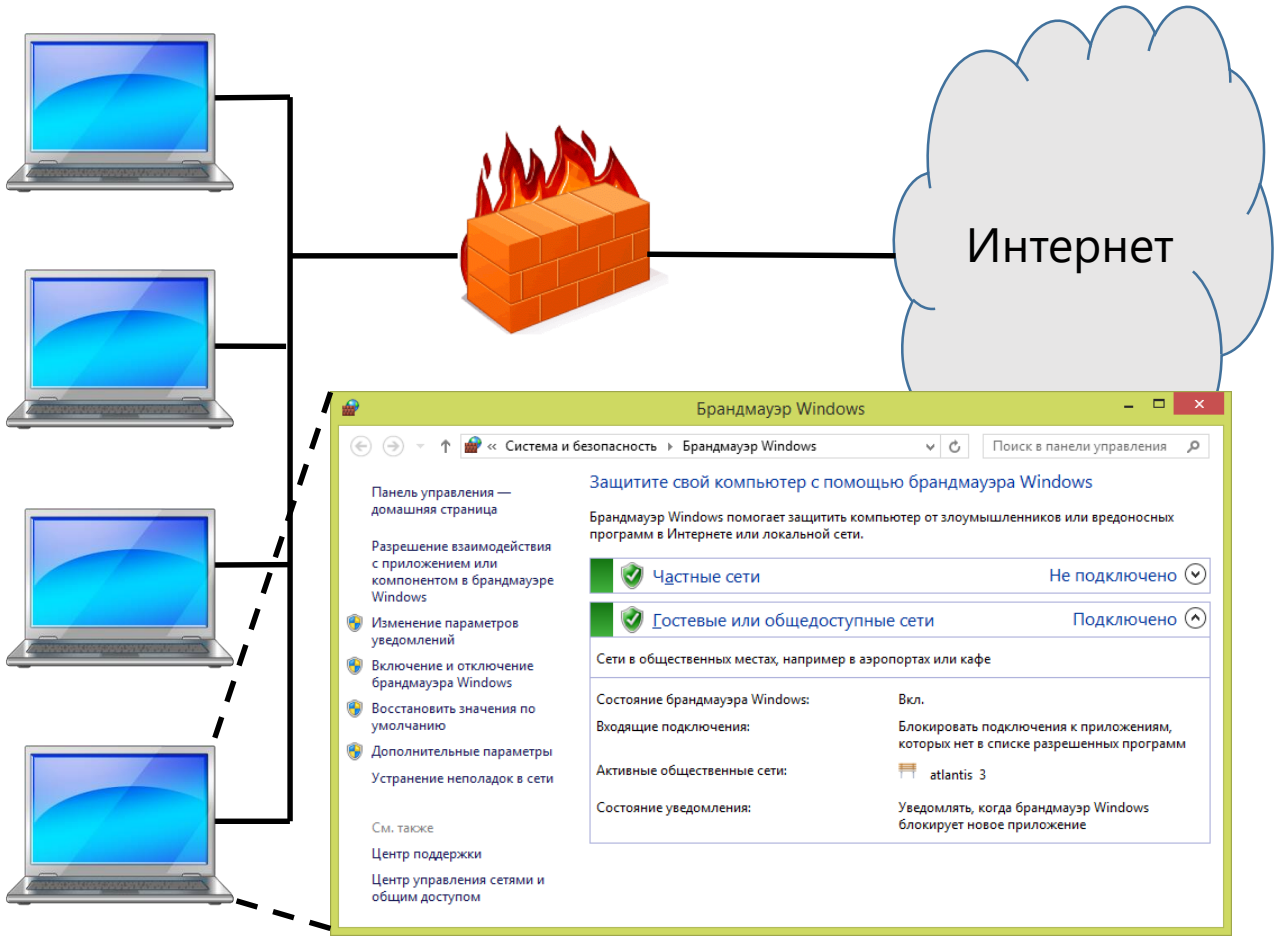
Межсетевой экран

- Отделяет сеть от других сетей
- Другие названия: брандмауэр, firewall

Межсетевые экраны



Межсетевые экраны



Место в моделях OSI и TCP/IP

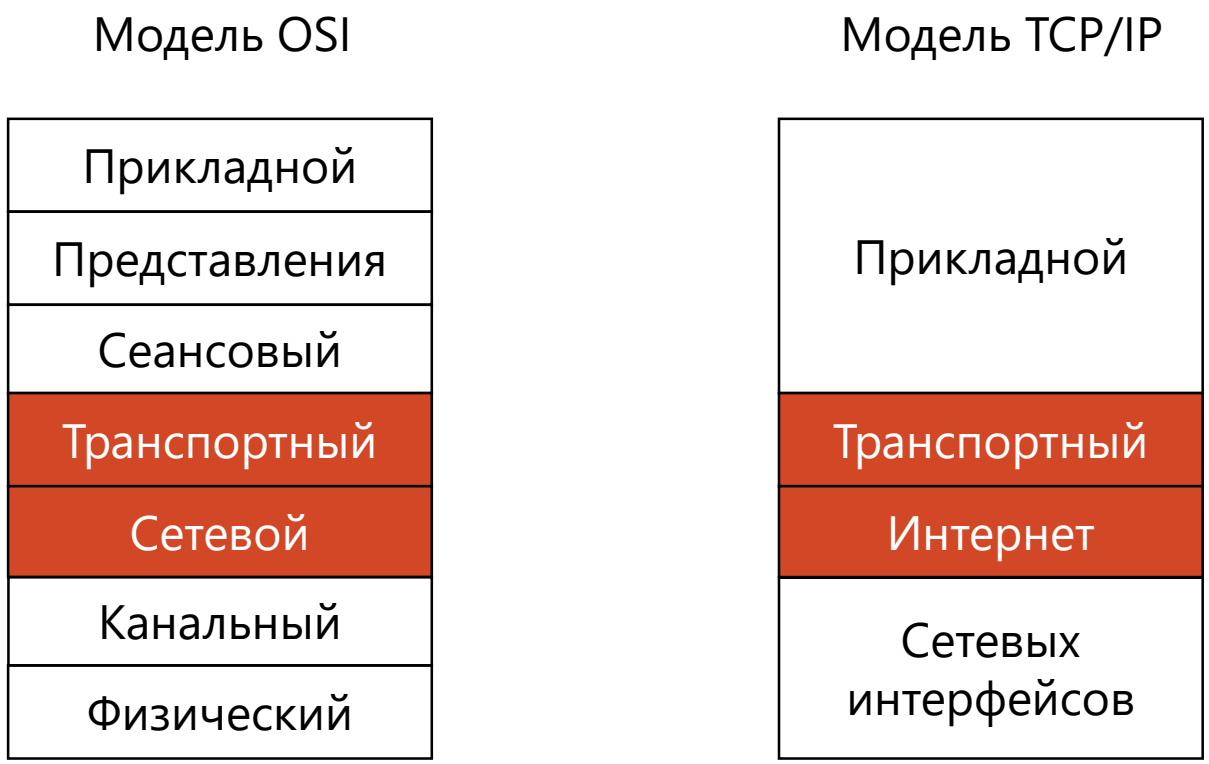


Схема работы межсетевого экрана

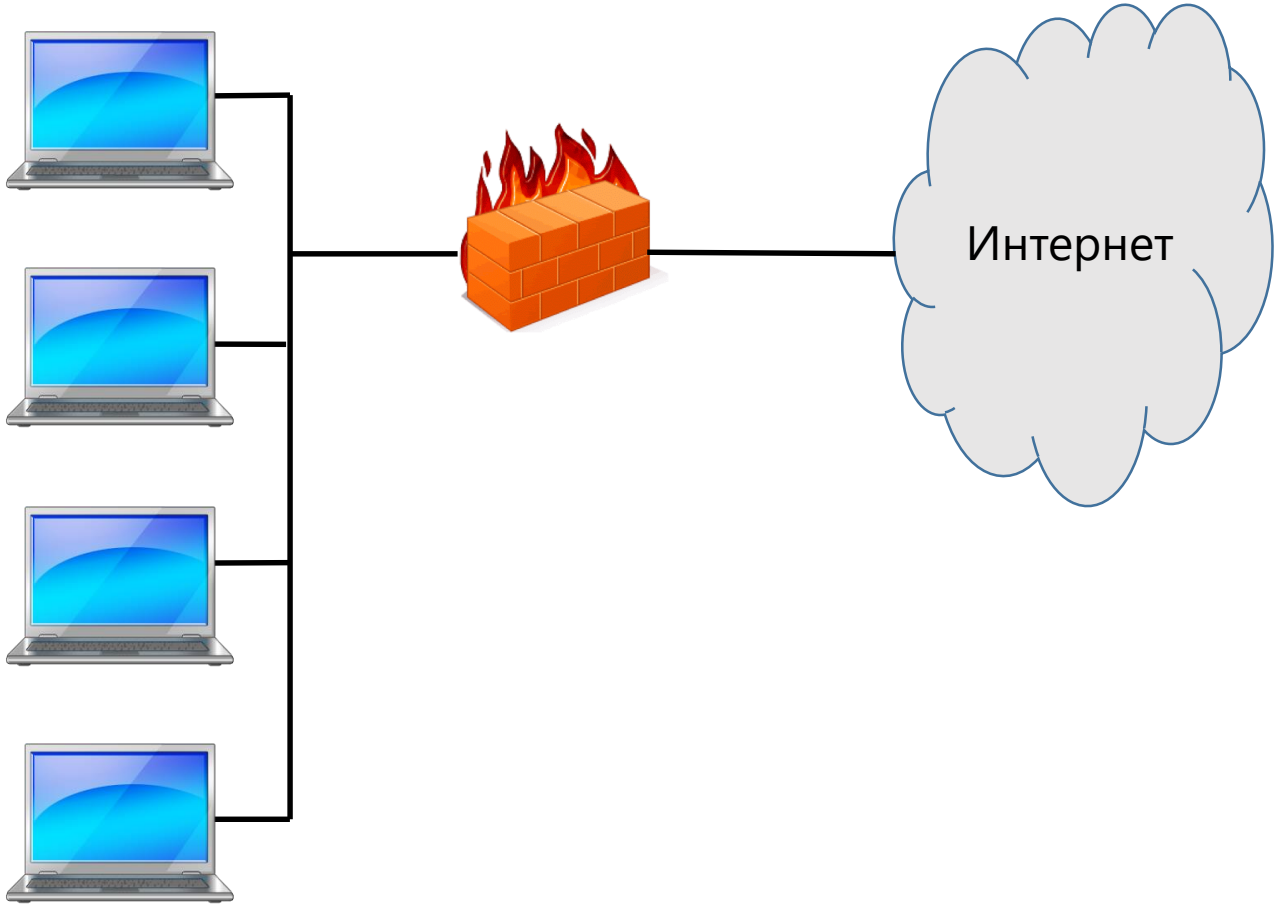


Схема работы межсетевого экрана

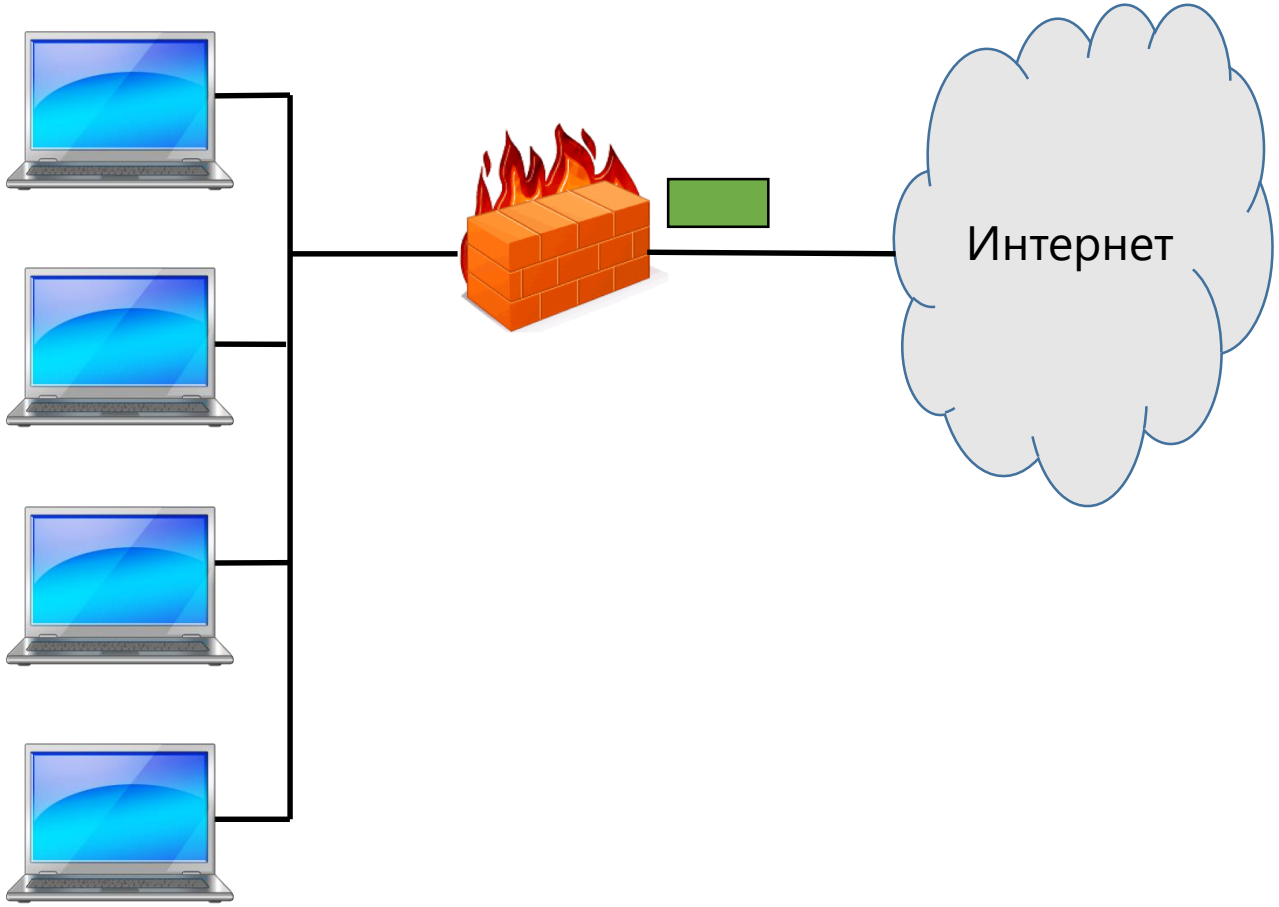


Схема работы межсетевого экрана

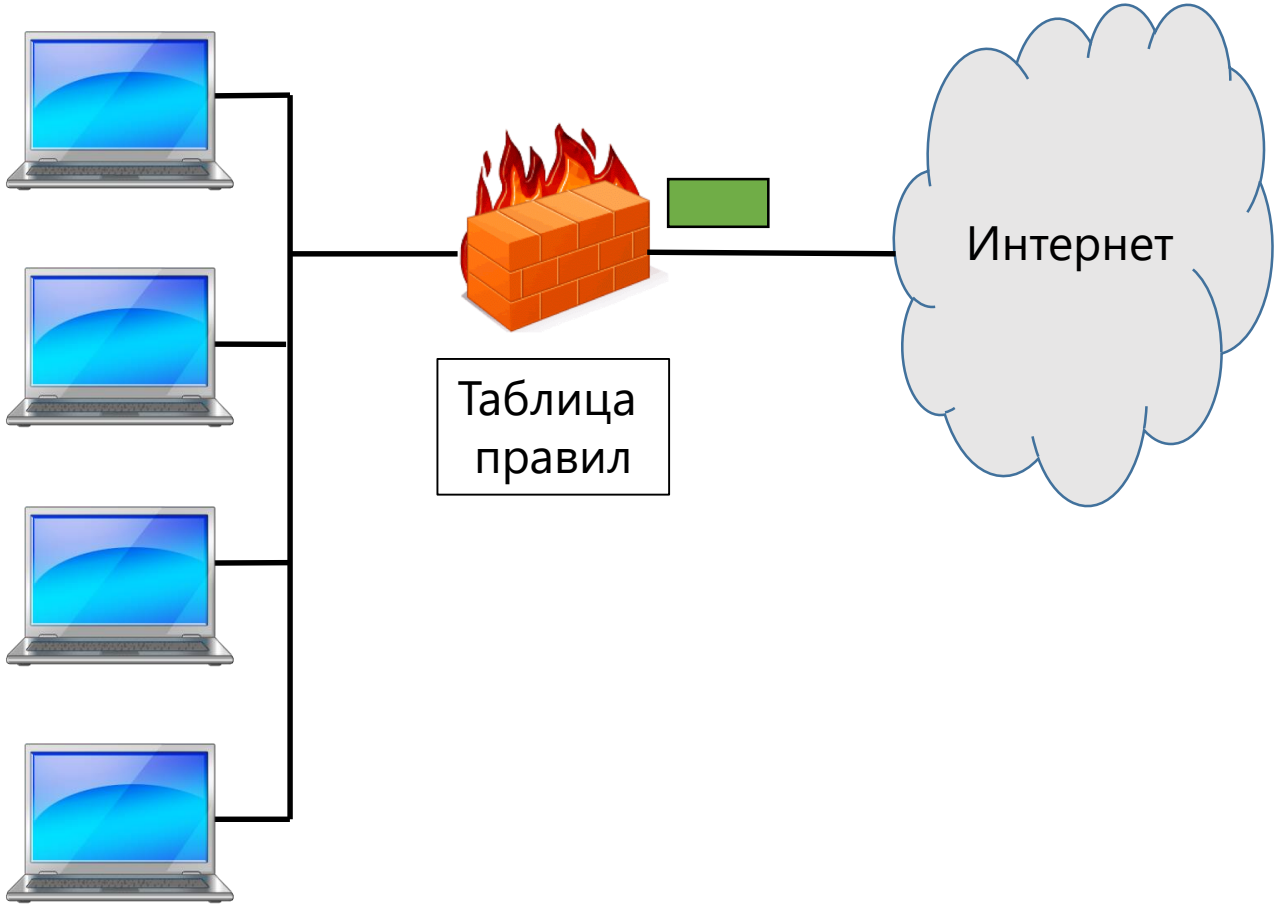


Схема работы межсетевого экрана

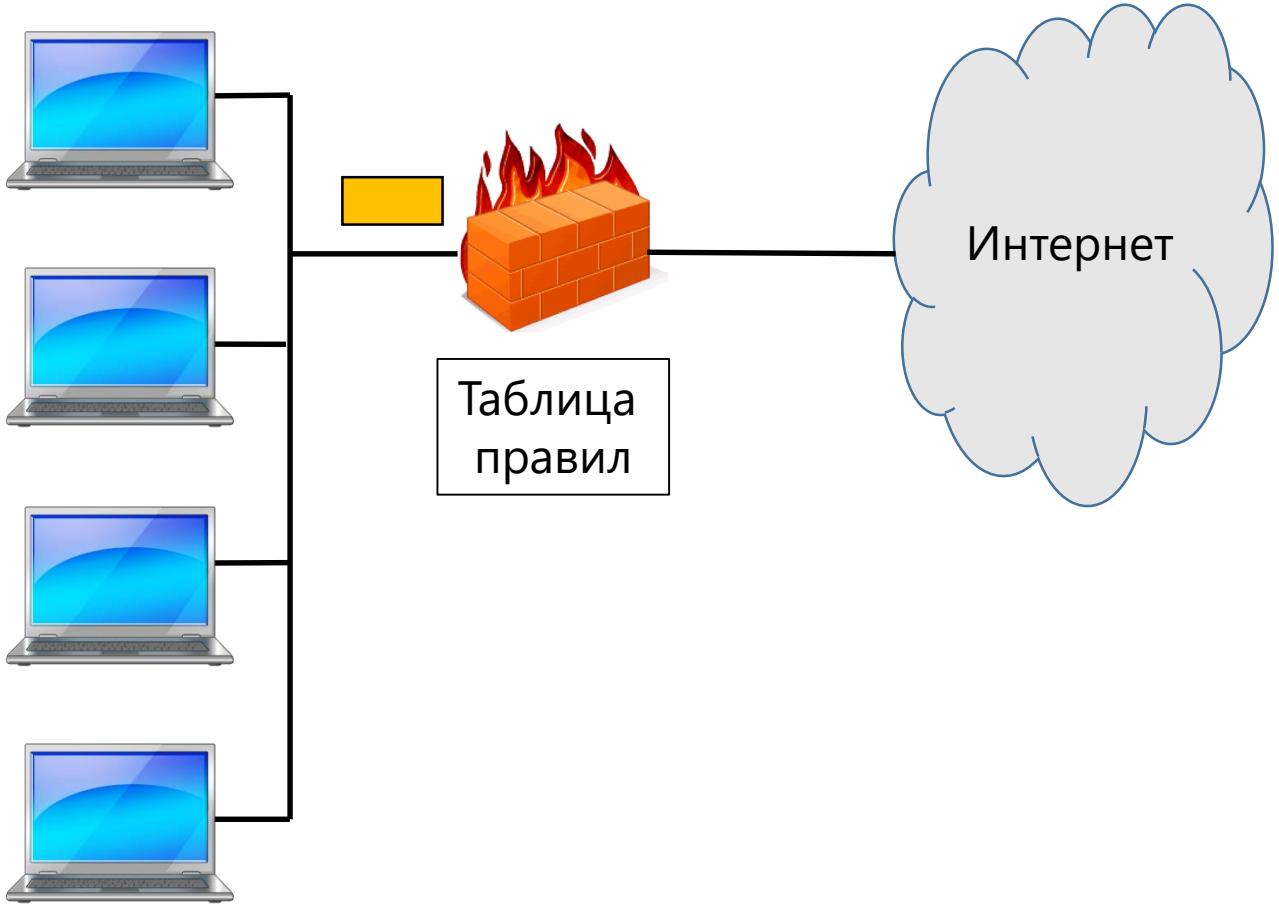


Таблица правил доступа

Отправитель		Получатель		Протокол	Действие
IP	Порт	IP	Порт		
220.10.1.0/24	>1024	Вне 220.10.1.0/24	80	TCP	Разрешить
Вне 220.10.1.0/24	80	220.10.1.0/24	>1024	TCP	Разрешить
Любой	Любой	Любой	Любой	Любой	Запретить

Таблица правил доступа

Отправитель		Получатель		Протокол	Флаг	Действие
IP	Порт	IP	Порт			
220.10.1.0/24	>1024	Вне 220.10.1.0/24	80	TCP	Любой	Разрешить
Вне 220.10.1.0/24	80	220.10.1.0/24	>1024	TCP	Ack	Разрешить
Любой	Любой	Любой	Любой	Любой	Любой	Запретить

Проверка соединения

Отправитель		Получатель		Протокол	Флаг	Соеди-нение	Действие
IP	Порт	IP	Порт				
220.10.1.0/24	>1024	Вне 220.10.1.0/24	80	TCP	Любой	-	Разрешить
Вне 220.10.1.0/24	80	220.10.1.0/24	>1024	TCP	Ack	Проверять	Разрешить
Любой	Любой	Любой	Любой	Любой	Любой	-	Запретить

Таблица соединений

Отправитель		Получатель	
IP	Порт	IP	Порт
220.10.1.86	53638	77.88.55.66	80

Другие методы ограничения доступа

Канальный уровень

- Фильтрация на портах коммутатора по MAC-адресам

Прикладной уровень

- Прокси-сервер (proxy server)
- Фильтр содержимого (content filter)

Система обнаружения вторжений (intrusion detection system, IDS)

Система предотвращения вторжений (intrusion prevention system, IPS)

Итоги

Межсетевые экраны
- Отделение сетей друг от друга

Фильтрация пакетов
- Сетевой и транспортный уровень
- IP-адреса, порты, типы протоколов, флаги

Преимущества
- Безопасность

Недостатки
- Неправильная конфигурация может привести к неработоспособности сети
- Возможно снижение производительности сети