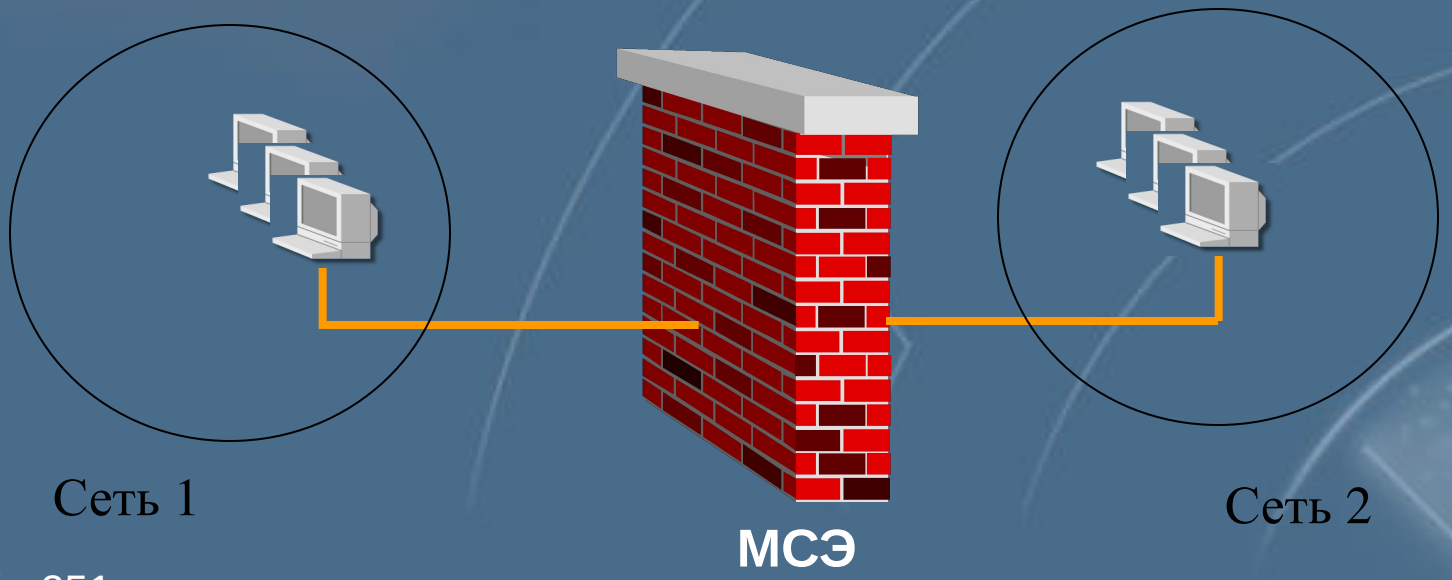
Межсетевые экраны

Раздел 2 – Тема 10

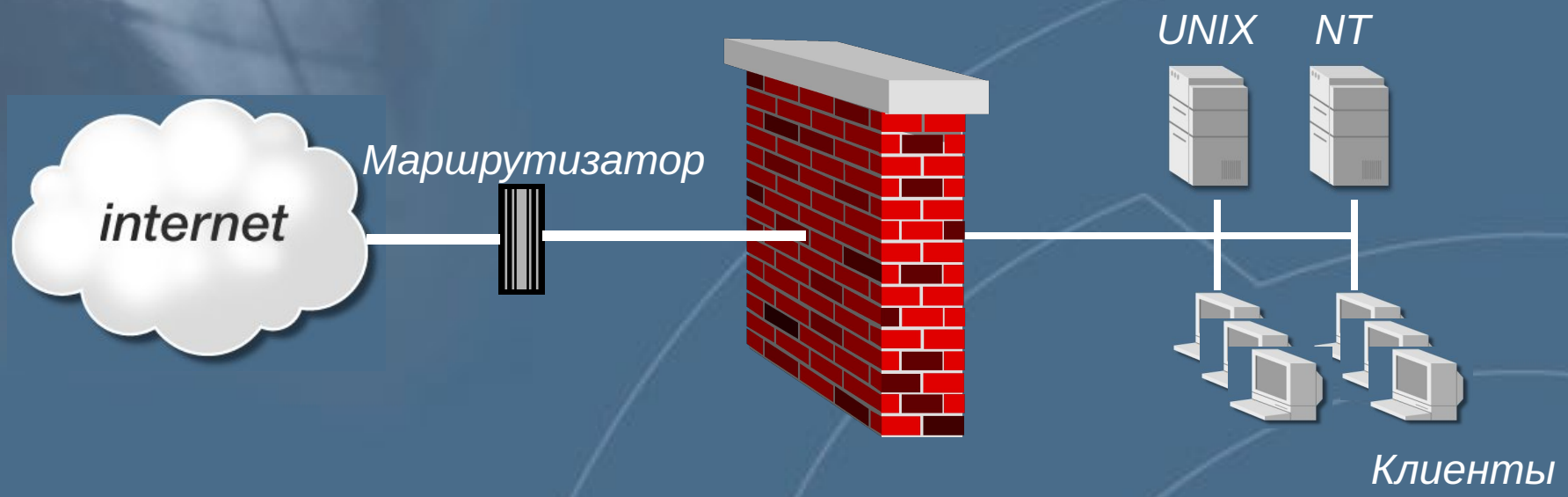
Что такое межсетевой экран?

Межсетевой экран

Это специализированное программное или аппаратное обеспечение, позволяющее разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения сетевых пакетов из одной части в другую



Назначение МСЭ



Основное назначение МСЭ - воплощение политики безопасности, принятой в организации в вопросах обмена информацией с внешним миром

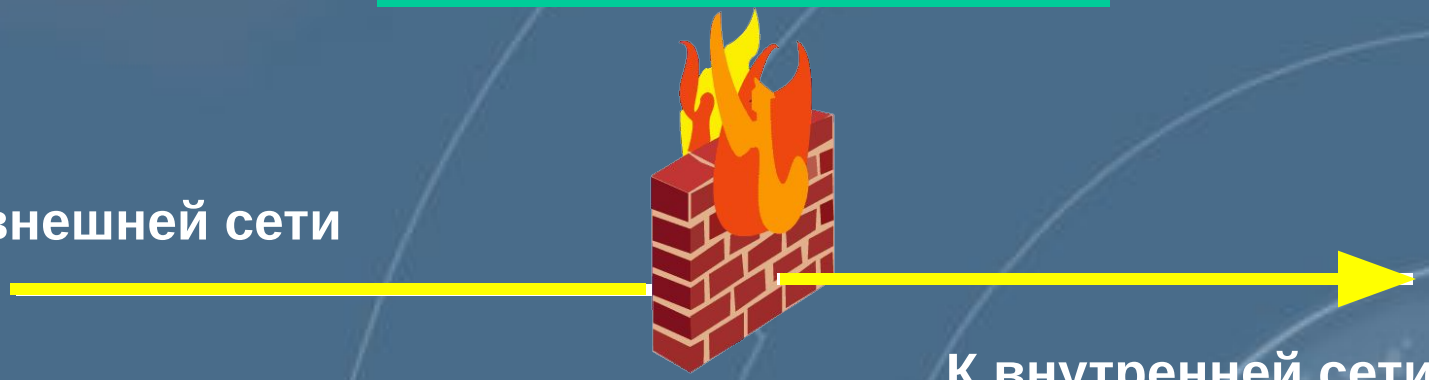
Механизмы защиты, реализуемые МСЭ

- Фильтрация пакетов
- Шифрование (создание VPN)
- Трансляция адресов
- Аутентификация (дополнительная)
- Противодействие некоторым видам атак (наиболее распространенным)
- Управление списками доступа на маршрутизаторах (необязательно)

Фильтрация сетевого трафика

Правила фильтрации

IP-адрес отправителя
IP-адрес получателя
TCP/UDP-порт отправителя
TCP/UDP-порт получателя
Другие критерии



Это основная функция МЭ!

Фильтрация сетевого трафика

Уровень приложений

Уровень представления

Уровень соединения

Уровень транспортный

Уровень сетевой

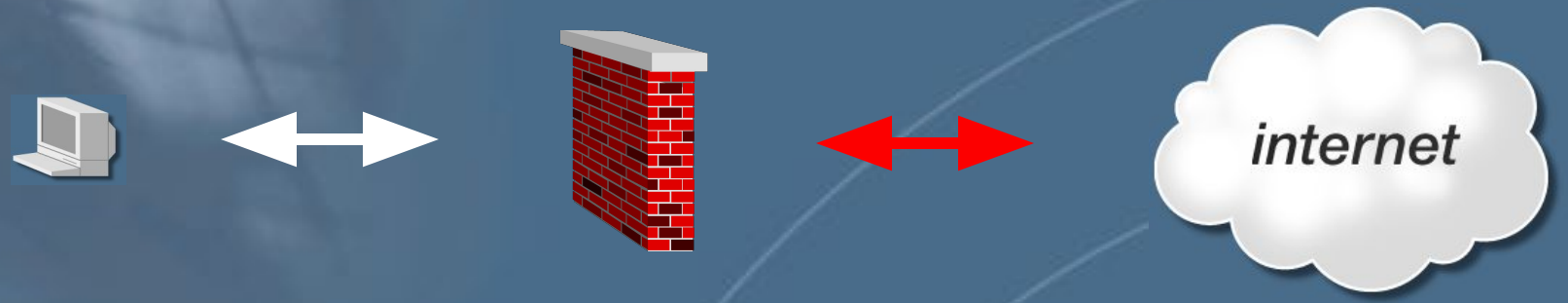
Уровень канальный

Уровень физический

Сегмент 1

Сегмент 2

Шифрование



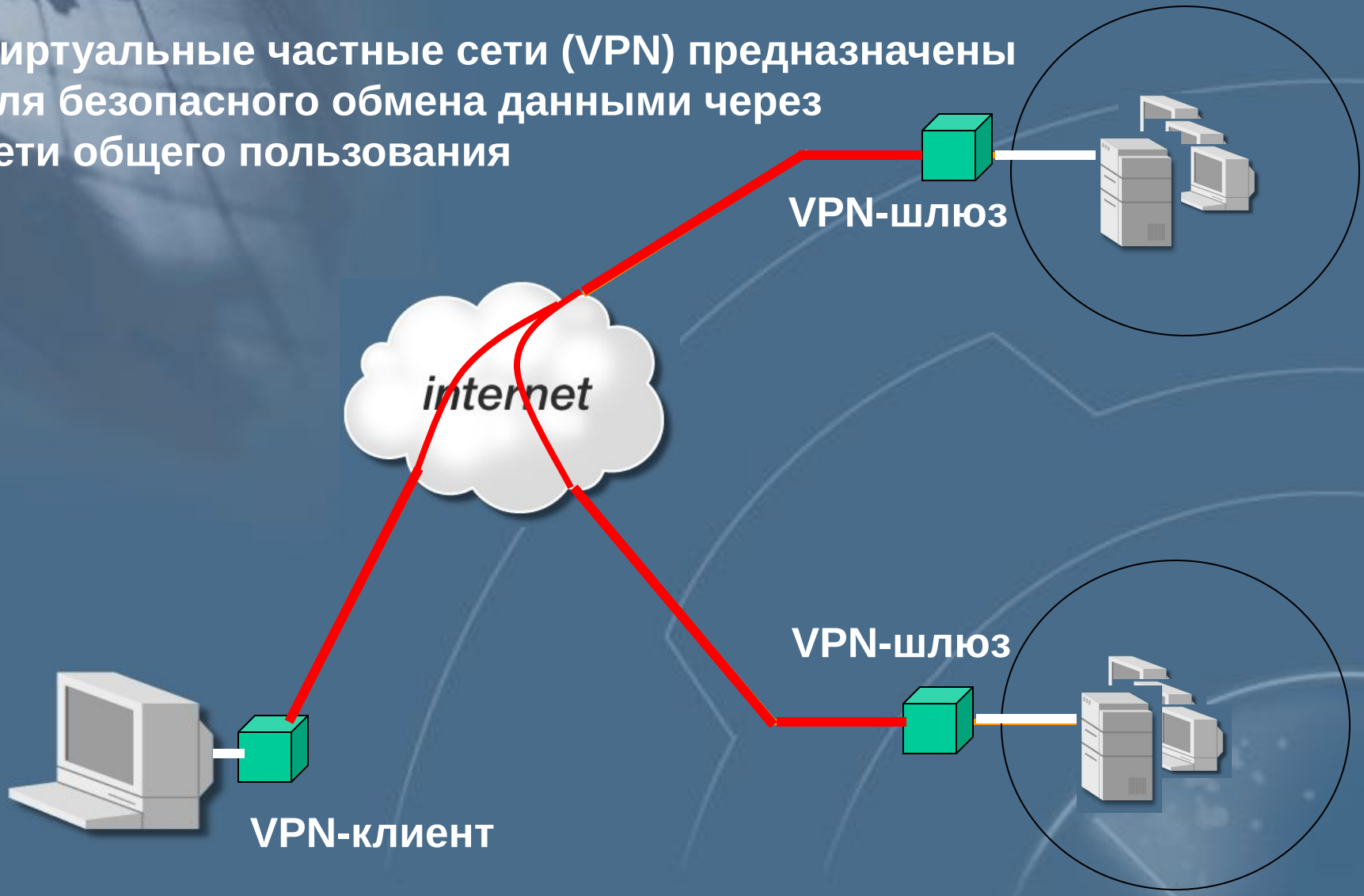
Незашифрованный трафик

Зашифрованный трафик

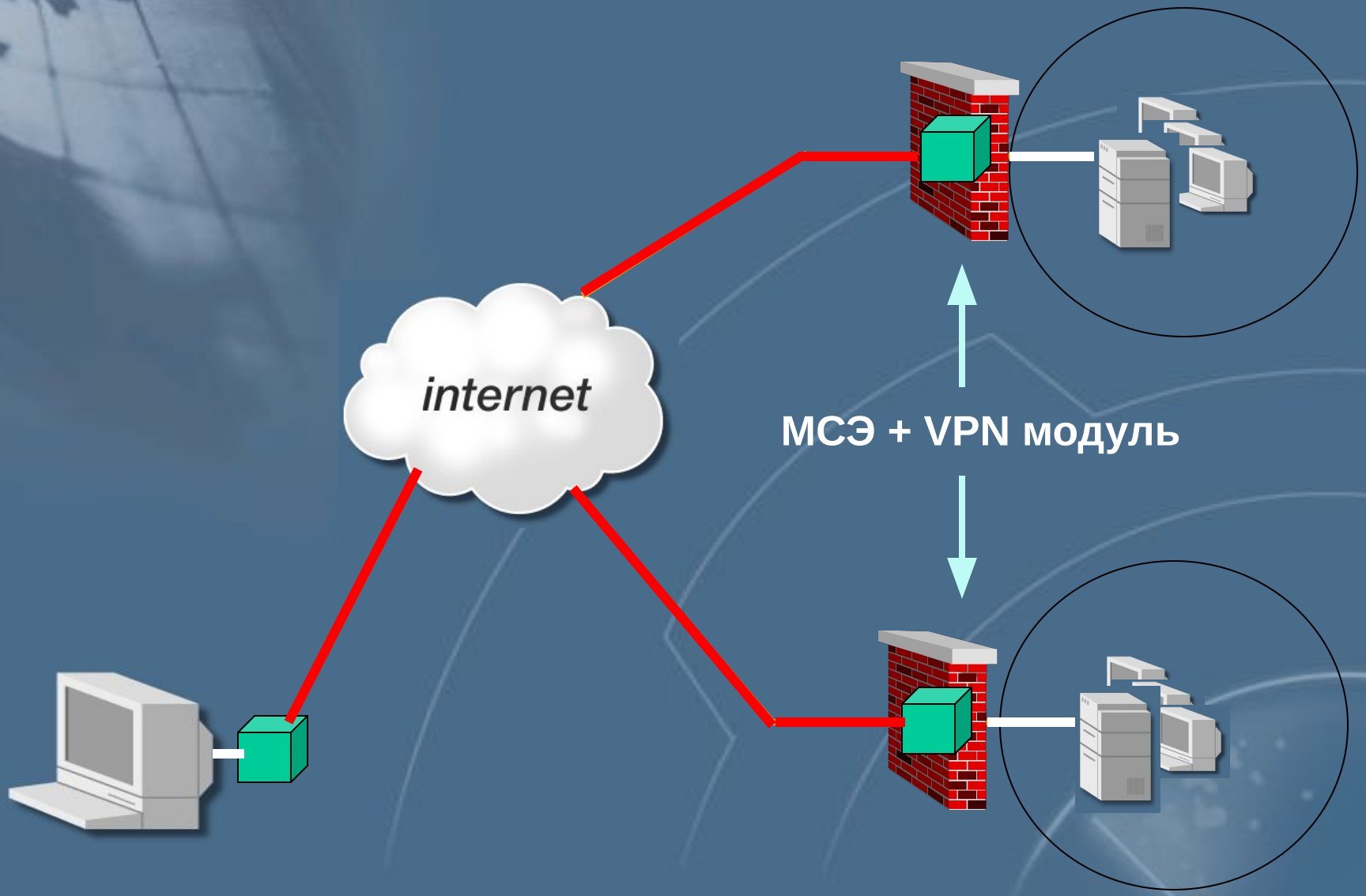
Функции шифрования позволяют защитить данные, передаваемые по общим каналам связи

Виртуальные частные сети

Виртуальные частные сети (VPN) предназначены для безопасного обмена данными через сети общего пользования

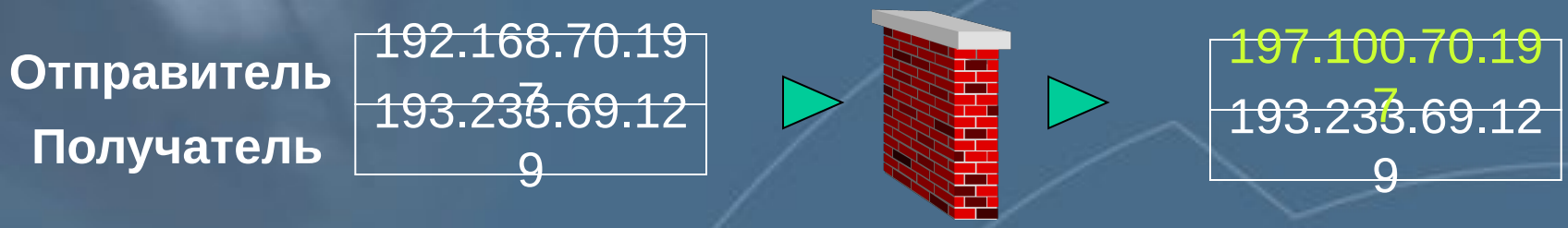


Организация виртуальных частных сетей с использованием МСЭ



Трансляция адресов

Это замена в IP-пакете IP-адреса отправителя или получателя другим IP-адресом при прохождении пакета через устройство, осуществляющее трансляцию



Обоснование

- **Маскировка внутренних IP-адресов от внешнего мира**
- **Решение проблемы некорректности либо нехватки IP-адресов внутренней сети**

Виды трансляции адресов

Статическая
(двунаправленная)

Это задание однозначного соответствия между внутренним адресом ресурса и его адресом во внешней сети

Динамическая
(трансляция адресов-портов)

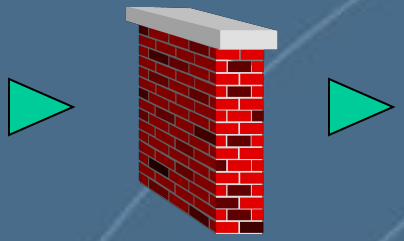
Это отображение адресного пространства внутренней сети на один адрес из внешней сети

Статическая трансляция адресов

Внутренние адреса
200.0.0.100 - 200.0.0.200

Внешние адреса
199.203.73.15 - 199.203.73.115

source	200.0.0.108
dest	193.233.69.129



source	199.203.73.23
dest	193.233.69.129

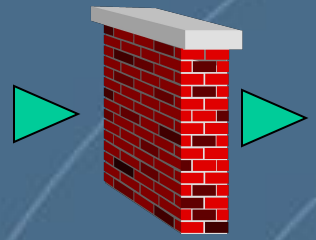
- **Позволяет иметь доступ к внутренним узлам извне**
- **Применяется в случае сложившегося распределения внутренних адресов**

Динамическая трансляция адресов

Внутренние адреса
200.0.0.100 - 200.0.0.200

Внешний адрес
199.203.145.35

	адрес	порт
source	200.0.0.104	1305
dest	193.233.145.35	x



	адрес	порт
source	199.203.145.35	2531
dest	193.233.69.129	x

- **Не позволяет инициировать доступ к внутренним узлам извне**
- **Решает проблему нехватки адресов**

Недостатки трансляции адресов

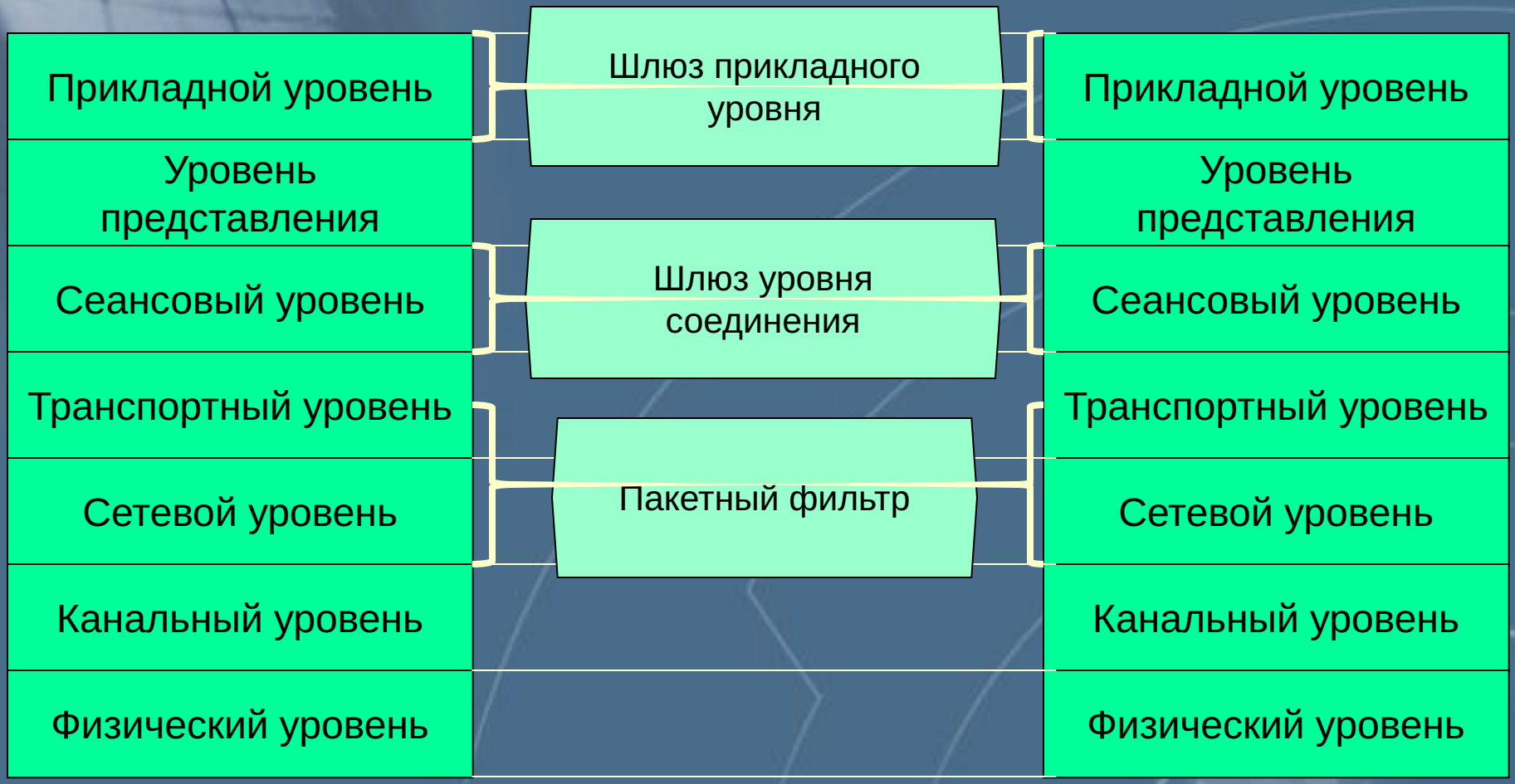
Увеличение вероятности неверной адресации

Невозможность или трудности запуска некоторых приложений

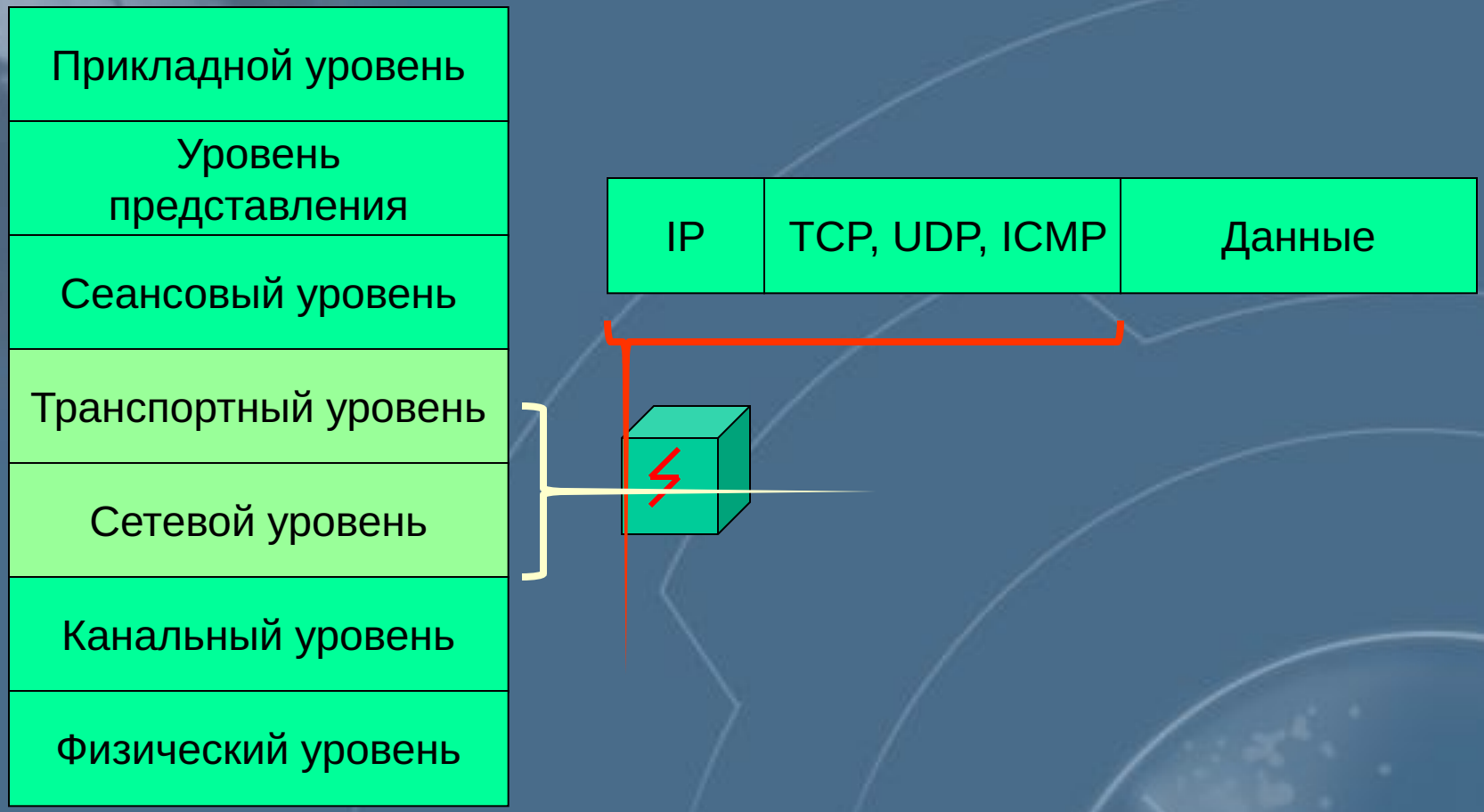
Проблемы с SNMP, DNS и т. д.

Замедление работы

Типы межсетевых экранов



Пакетный фильтр



Преимущества и недостатки пакетных фильтров

Преимущества

- Низкая стоимость
- Небольшая задержка прохождения пакетов

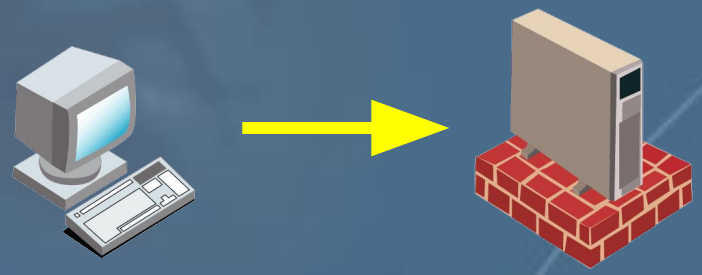
Недостатки

- Открытость внутренней сети
- Трудность описания правил фильтрации

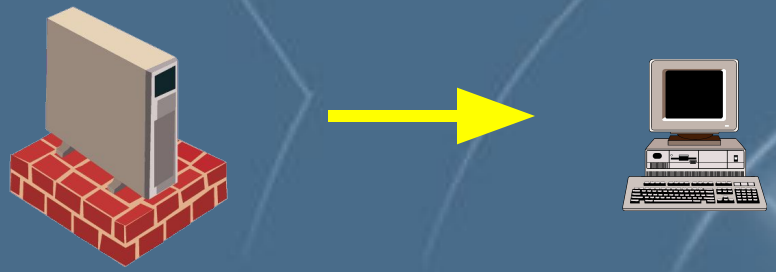
Технология «Proxy»

Proxy - это приложение - посредник, выполняющееся на МСЭ и выполняющее следующие функции:

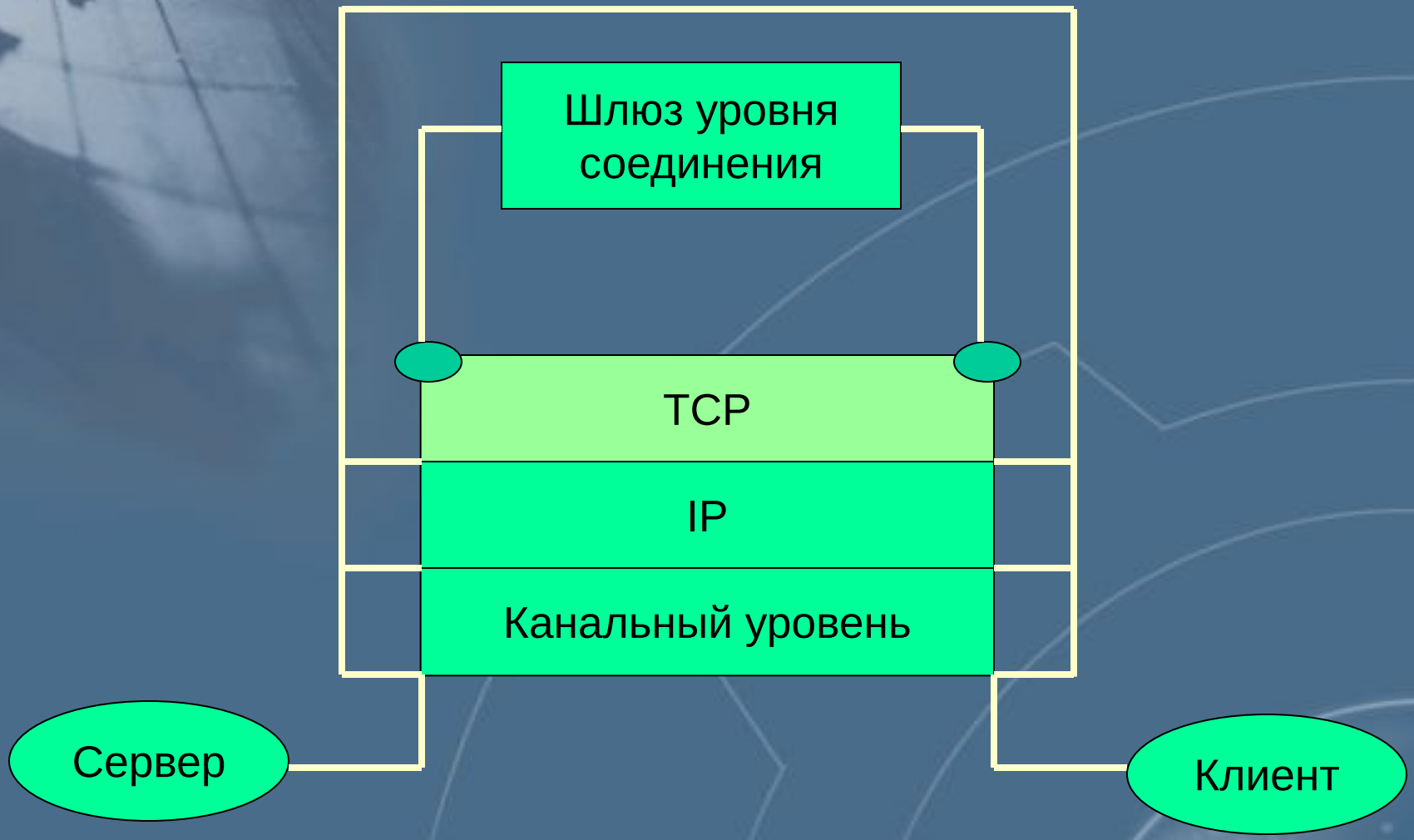
Приём и анализ запросов от клиентов



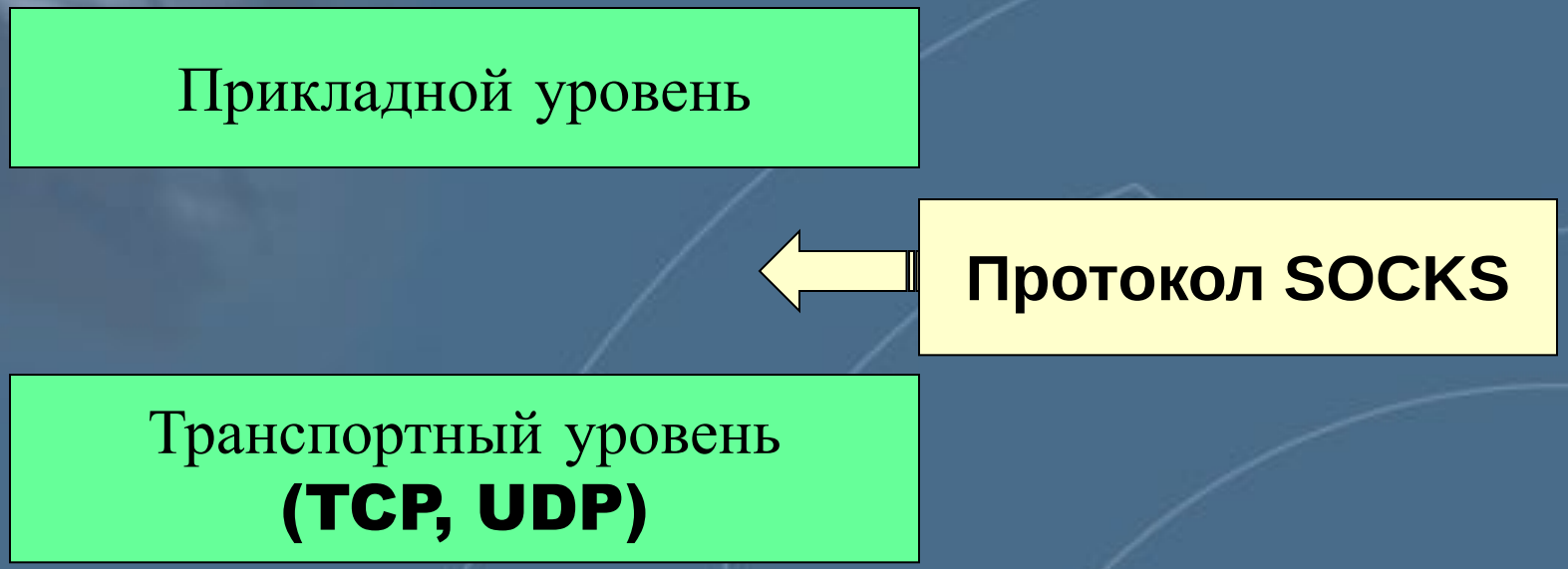
Перенаправление запросов реальному серверу



Шлюз уровня соединения

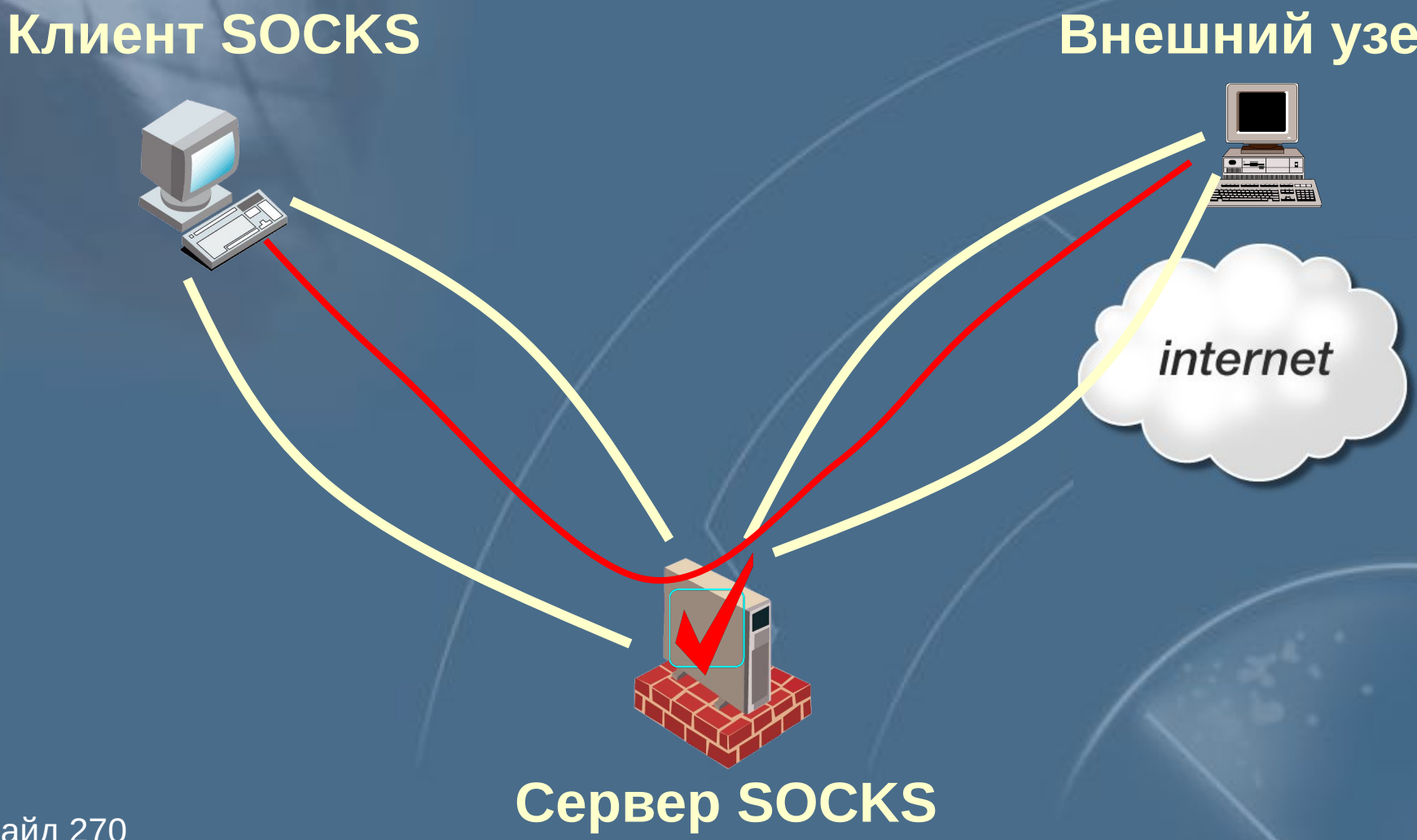


Протокол SOCKS

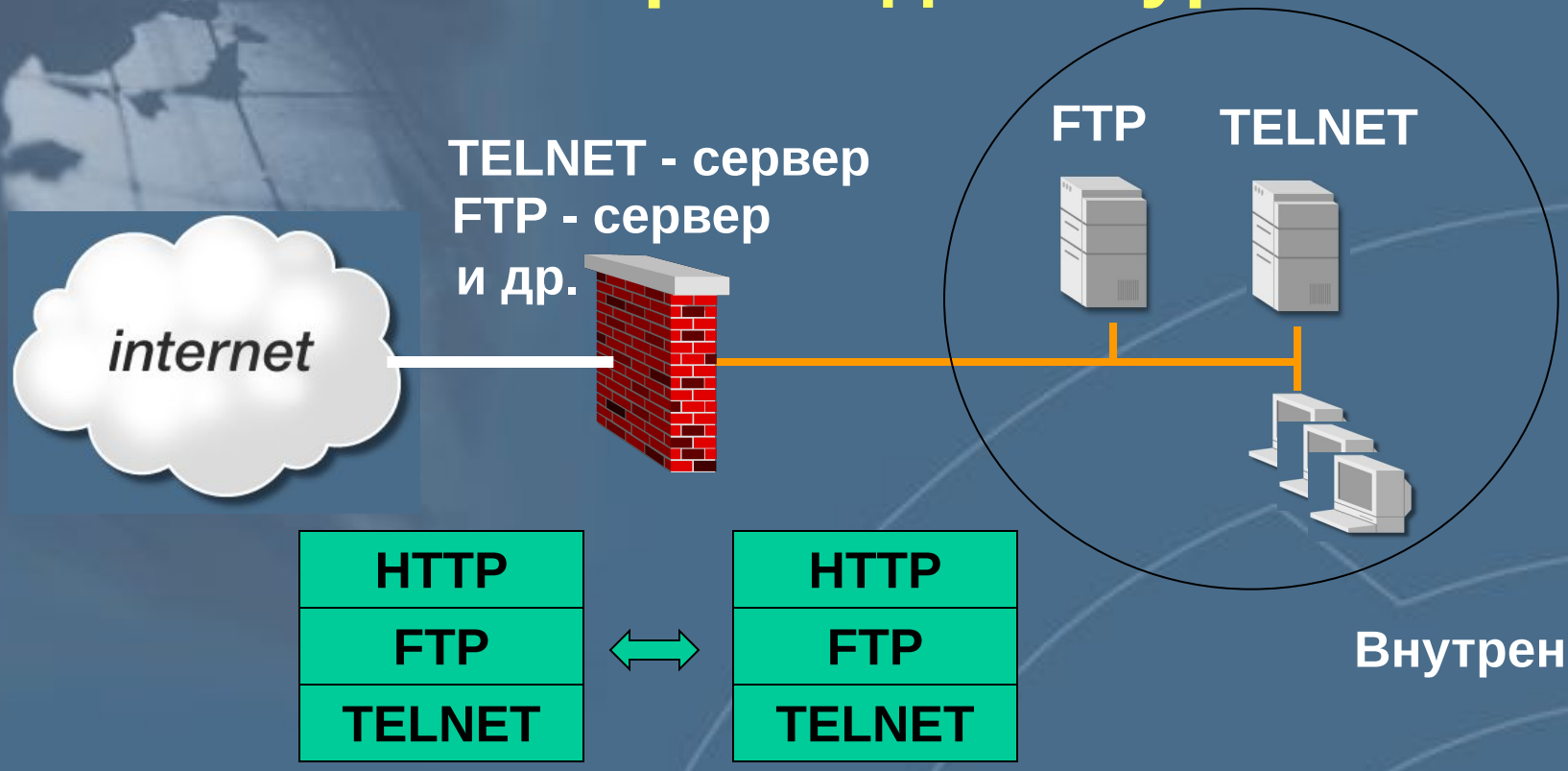


Шлюз уровня соединения -пример

Шлюз уровня соединения -пример



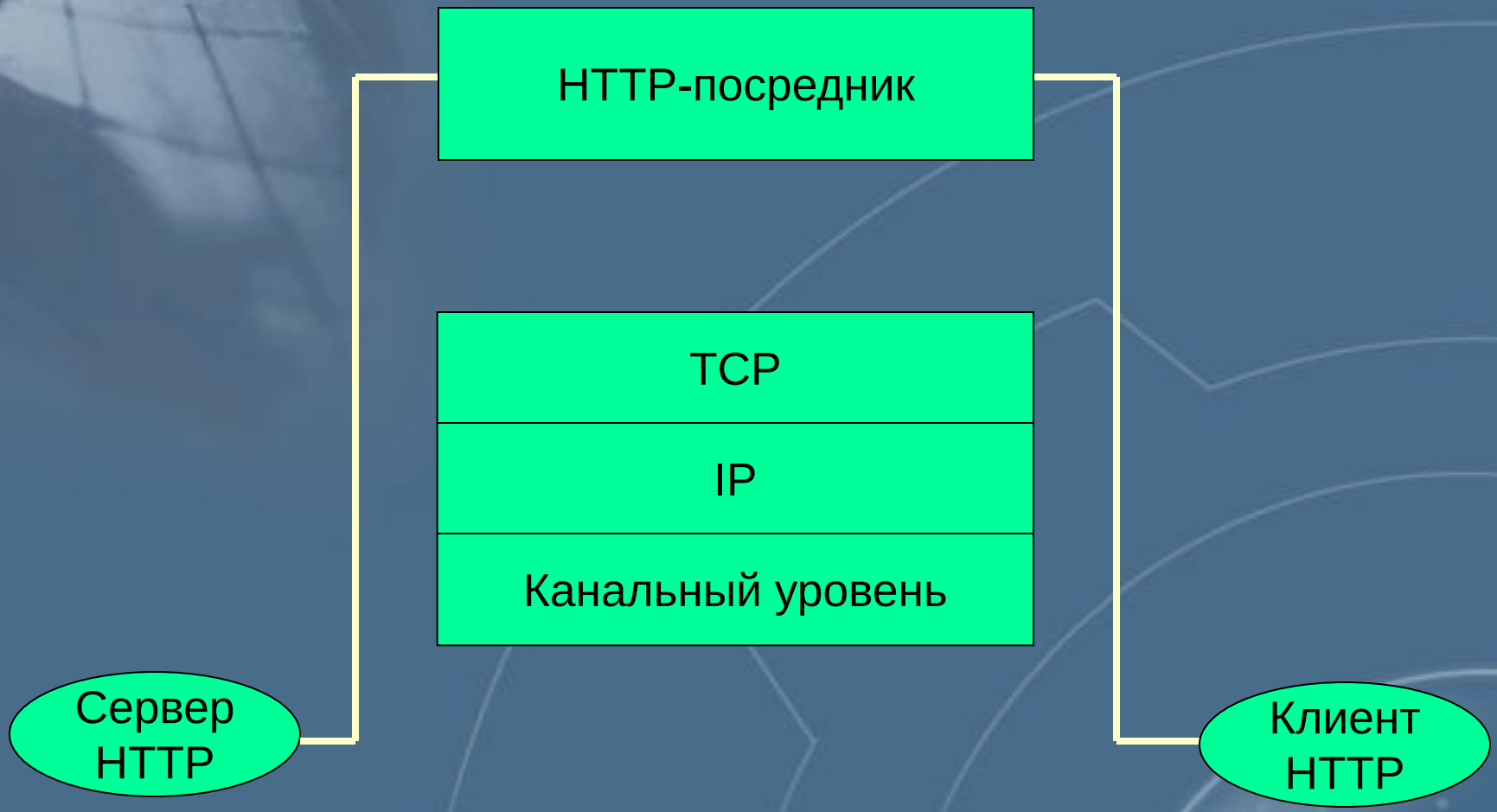
Шлюзы прикладного уровня



Пользователь устанавливает соединение с сервисом, запущенным на межсетевом экране

Правила доступа формируются на основе названия сервиса, имени пользователя, времени работы и т. д.

Шлюзы прикладного уровня



Преимущества и недостатки технологии «PROXY»

Преимущества

- Закрытость внутренней сети
- Надёжная аутентификация
- Простые правила фильтрации

Недостатки

- Двухшаговая процедура для входа во внутреннюю сеть и выхода наружу
- Низкая производительность
- Высокая стоимость

Технология «Stateful Inspection»

IP	TCP	Session	Application

- Прикладной уровень
- Уровень представления
- Сеансовый уровень
- Транспортный уровень
- **Сетевой уровень**

Inspection Module

- Канальный уровень

Пакет перехватывается на сетевом уровне

Специальный модуль анализирует информацию со всех уровней

Информация сохраняется и используется для анализа последующих пакетов

Технология «Stateful Inspection»

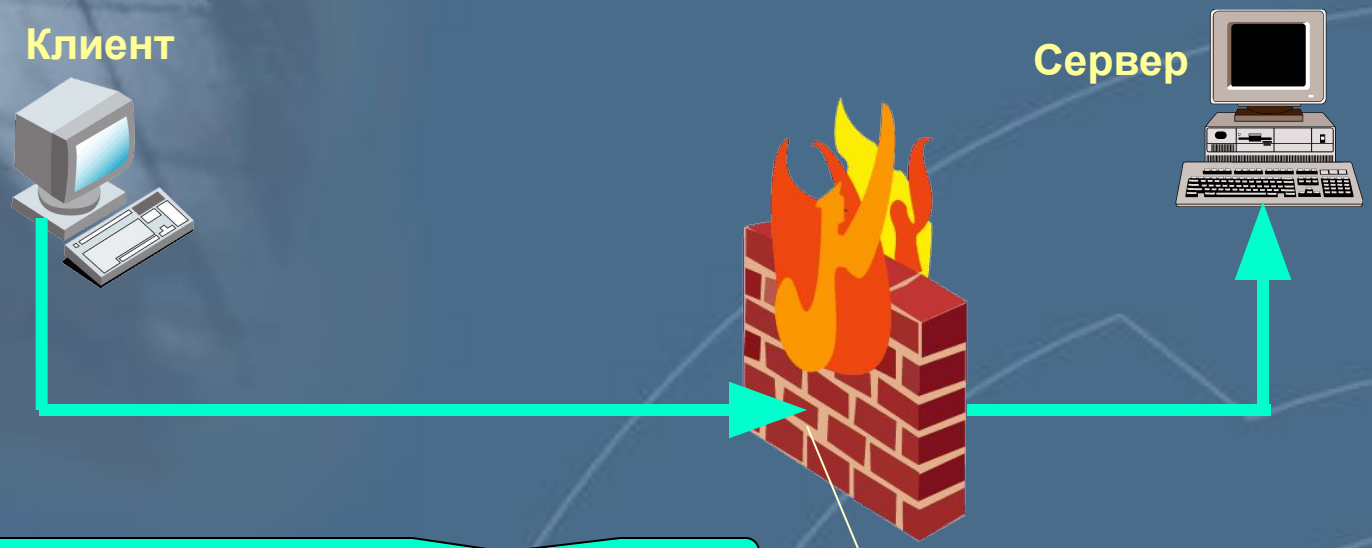
- Хранение информации о состоянии соединения
- Хранение информации о состоянии приложения
- Модификация передаваемой информации

Это анализ пакета в контексте соединения

Технология «Stateful Inspection»

Обработка нового соединения

Технология «Stateful Inspection»



Последующие пакеты соединения

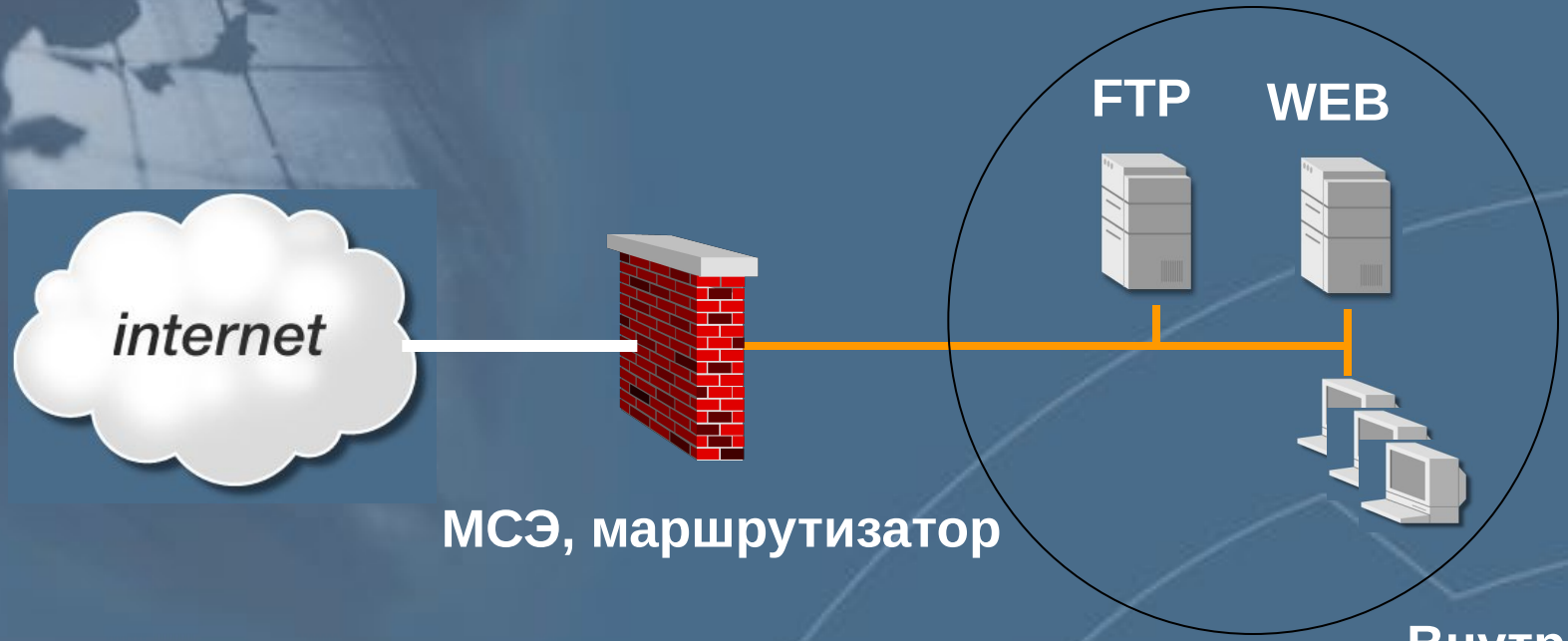
Таблица соединений

....
Соединение
...
...
...

Просмотр таблицы соединений

Обработка следующих пакетов

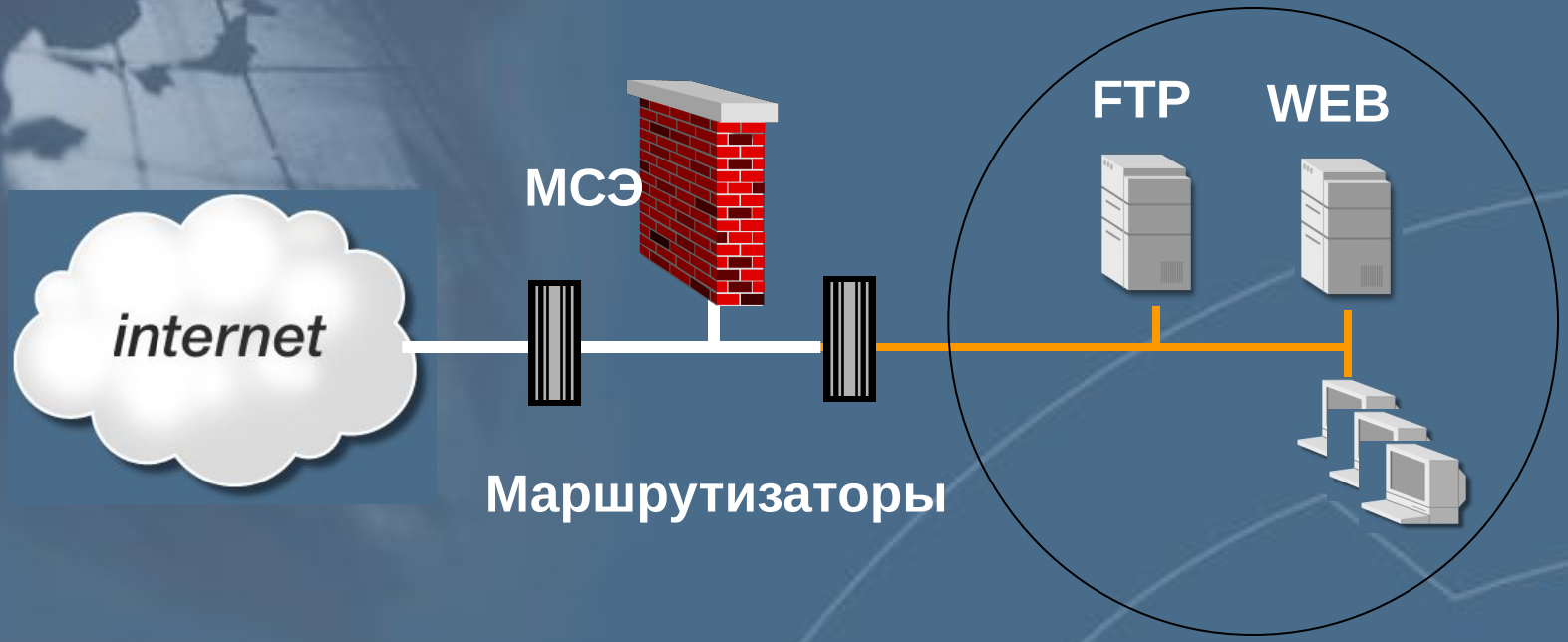
Варианты расположения МСЭ



1

Маршрутизатор является межсетевым экраном

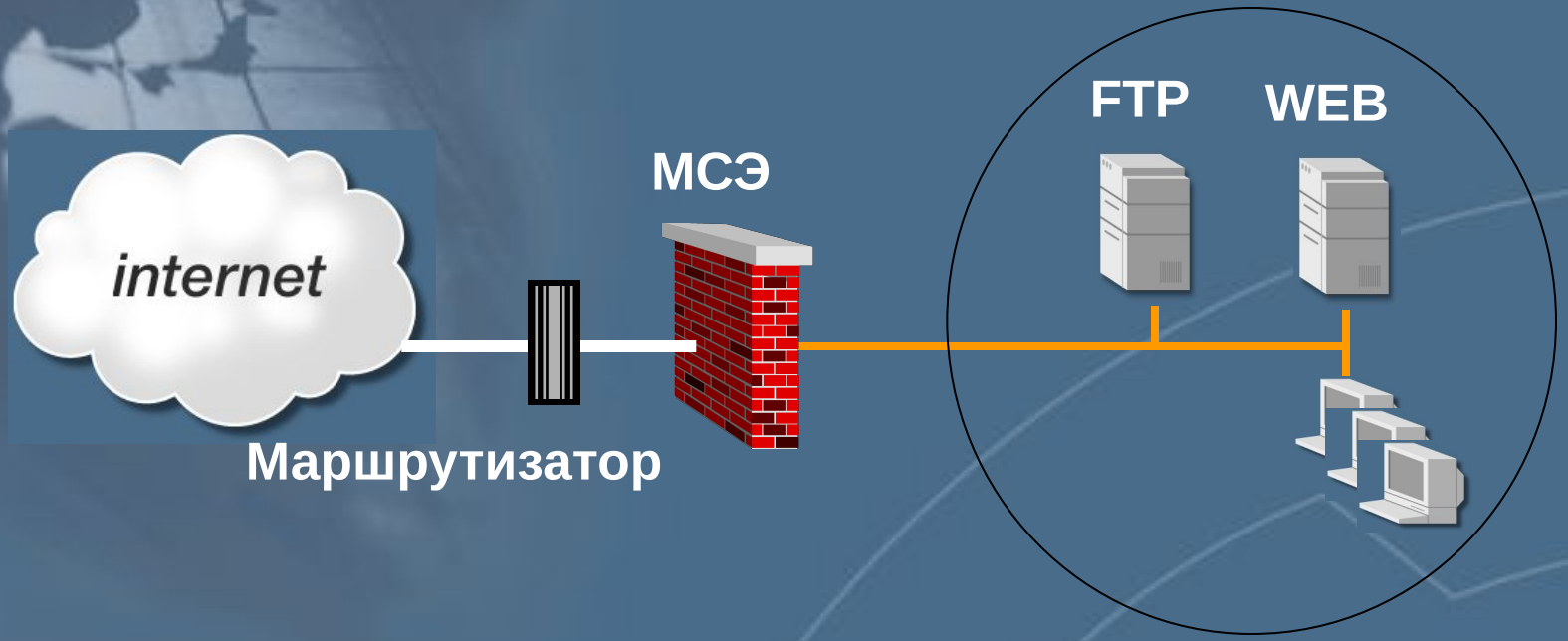
Варианты расположения МСЭ



2

Трафик с внешнего маршрутизатора перенаправляется на МСЭ, а затем на внутренний маршрутизатор

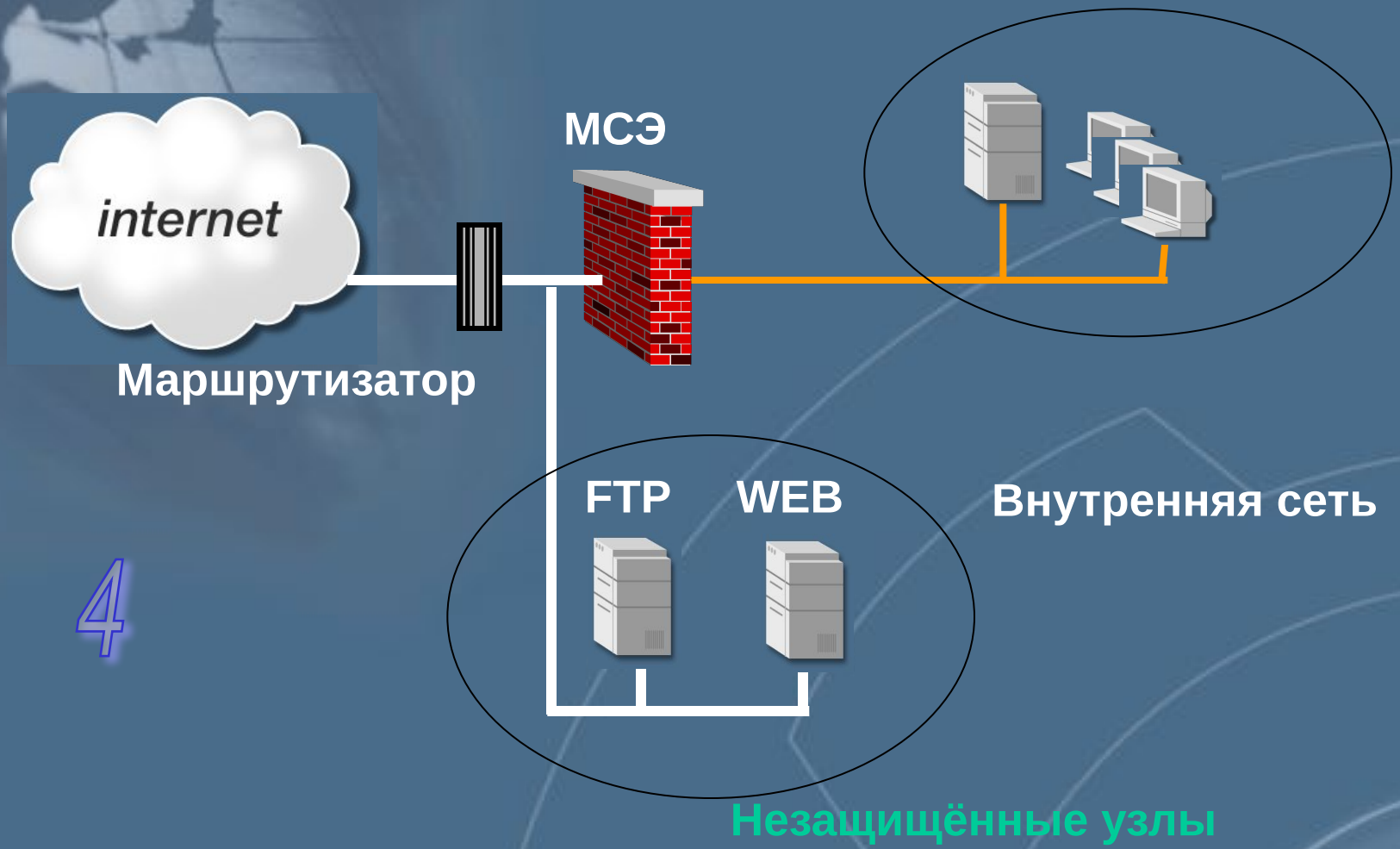
Варианты расположения МСЭ



3

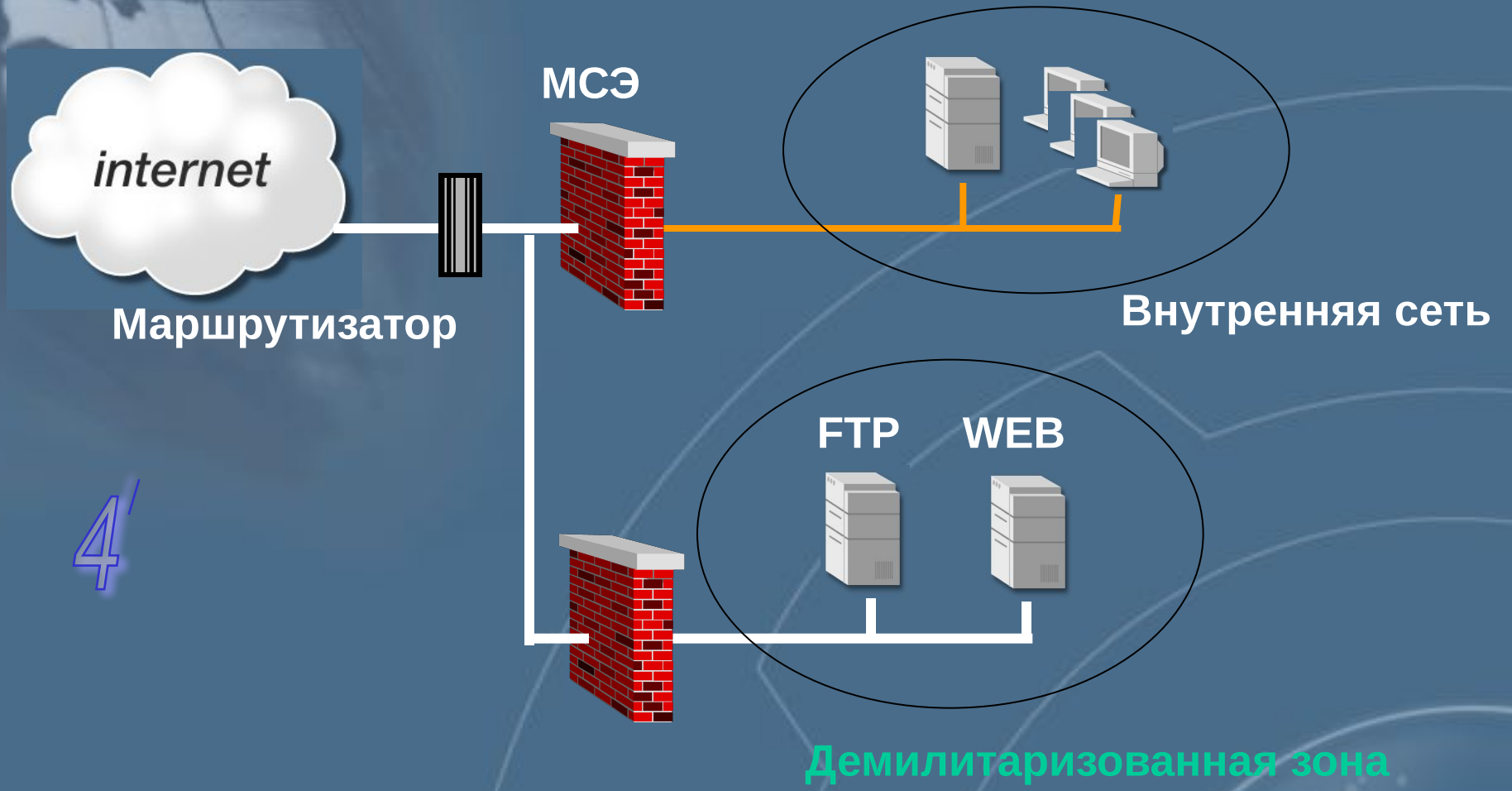
МСЭ является единственной видимой снаружи машиной

Варианты расположения МСЭ



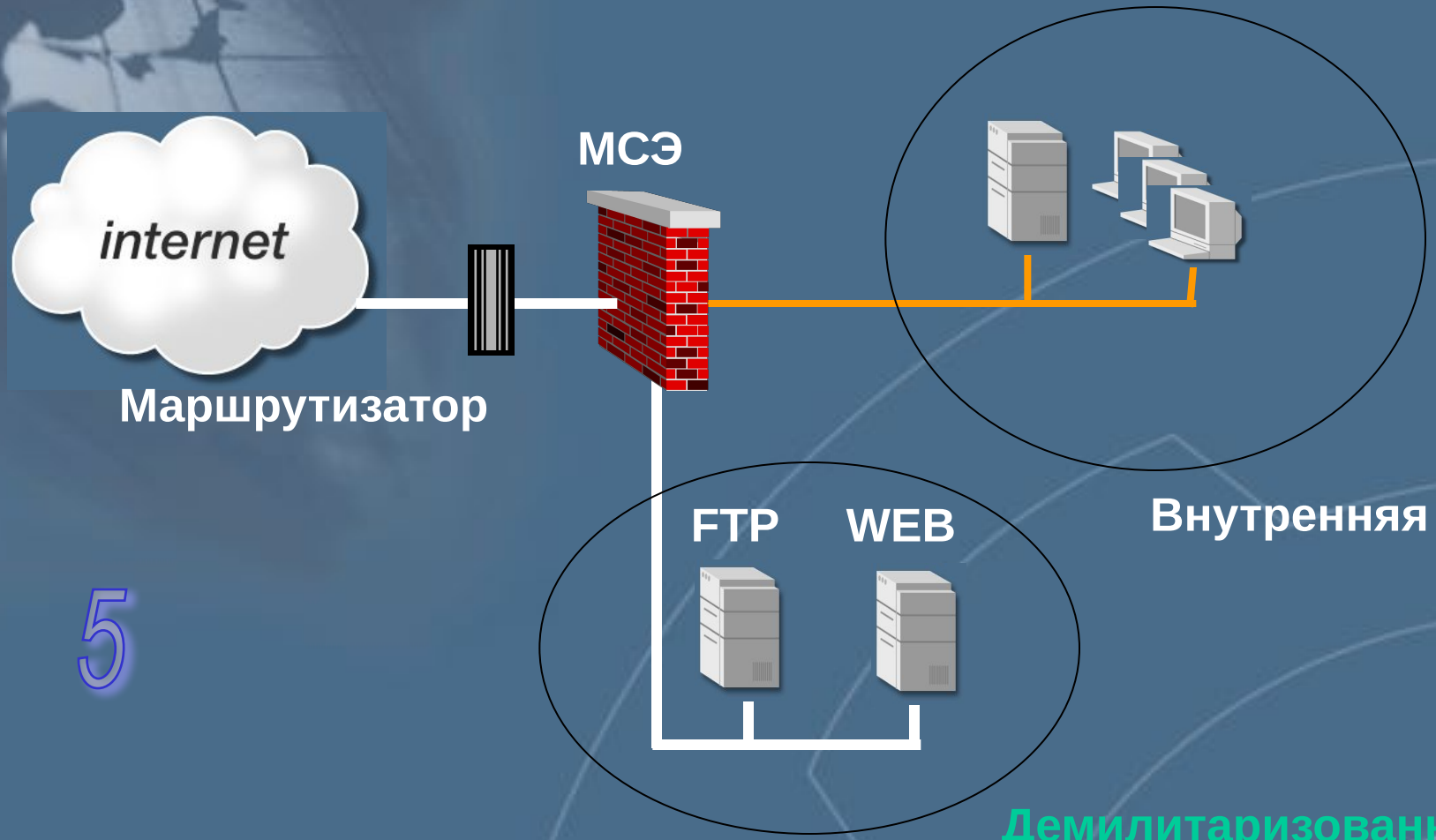
Защищена не вся внутренняя сеть. Узлы, которые должны быть видимы снаружи, не защищены

Варианты расположения МСЭ



Защищена не вся внутренняя сеть. Узлы, которые должны быть видимы снаружи, не защищены

Варианты расположения МСЭ



5

FTP и WEB серверы подключены к отдельному интерфейсу МСЭ, что позволяет создать для них отдельную политику

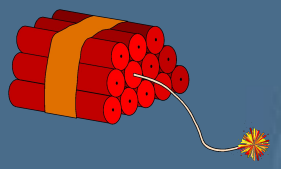
Недостатки МСЭ как средств защиты

Не защищают от пользователей, прошедших авторизацию

Не защищают соединения, установленные в обход МСЭ

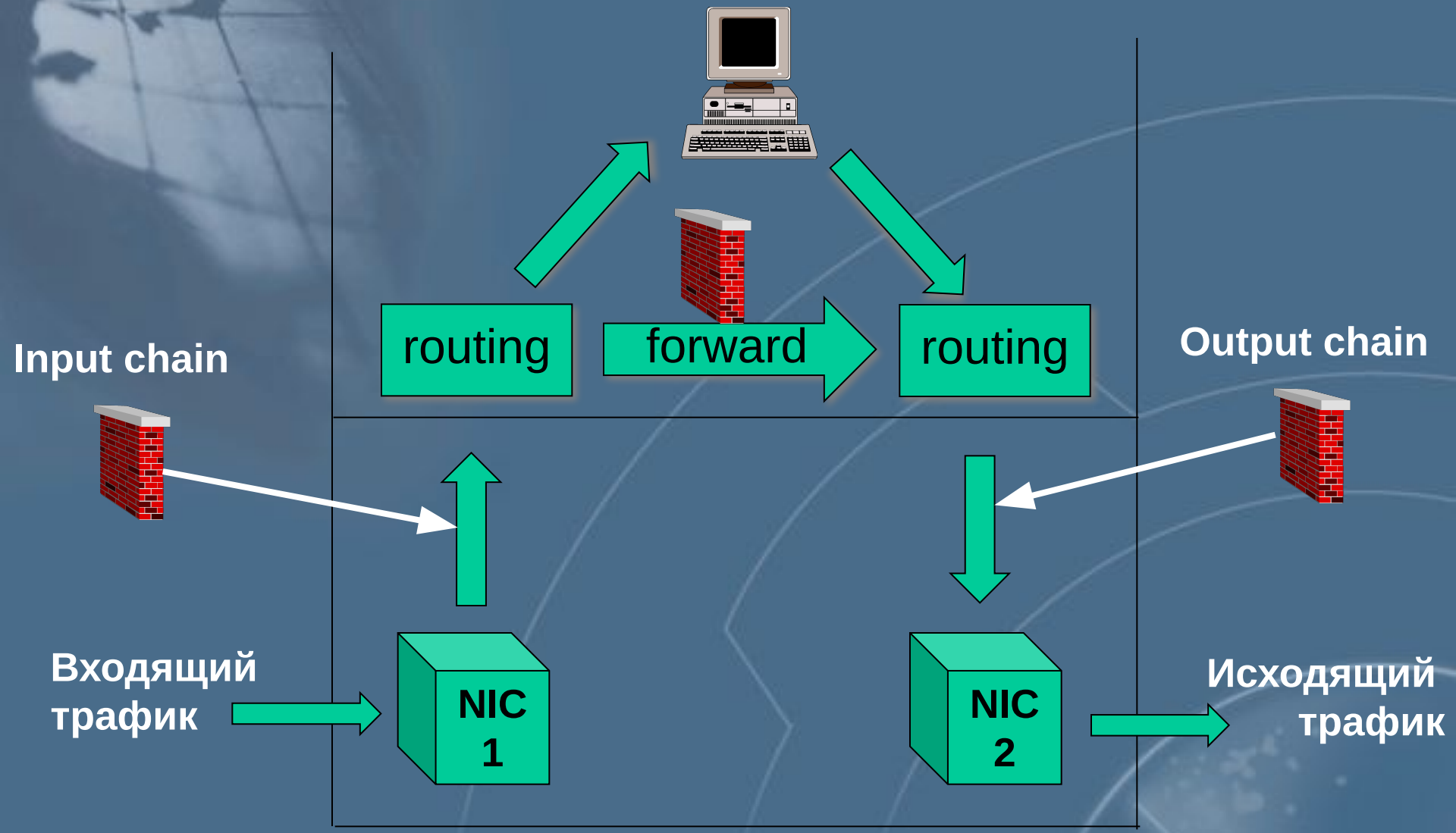
Не защищают от неправильной конфигурации

Не гарантируют 100% защиты от вторжений

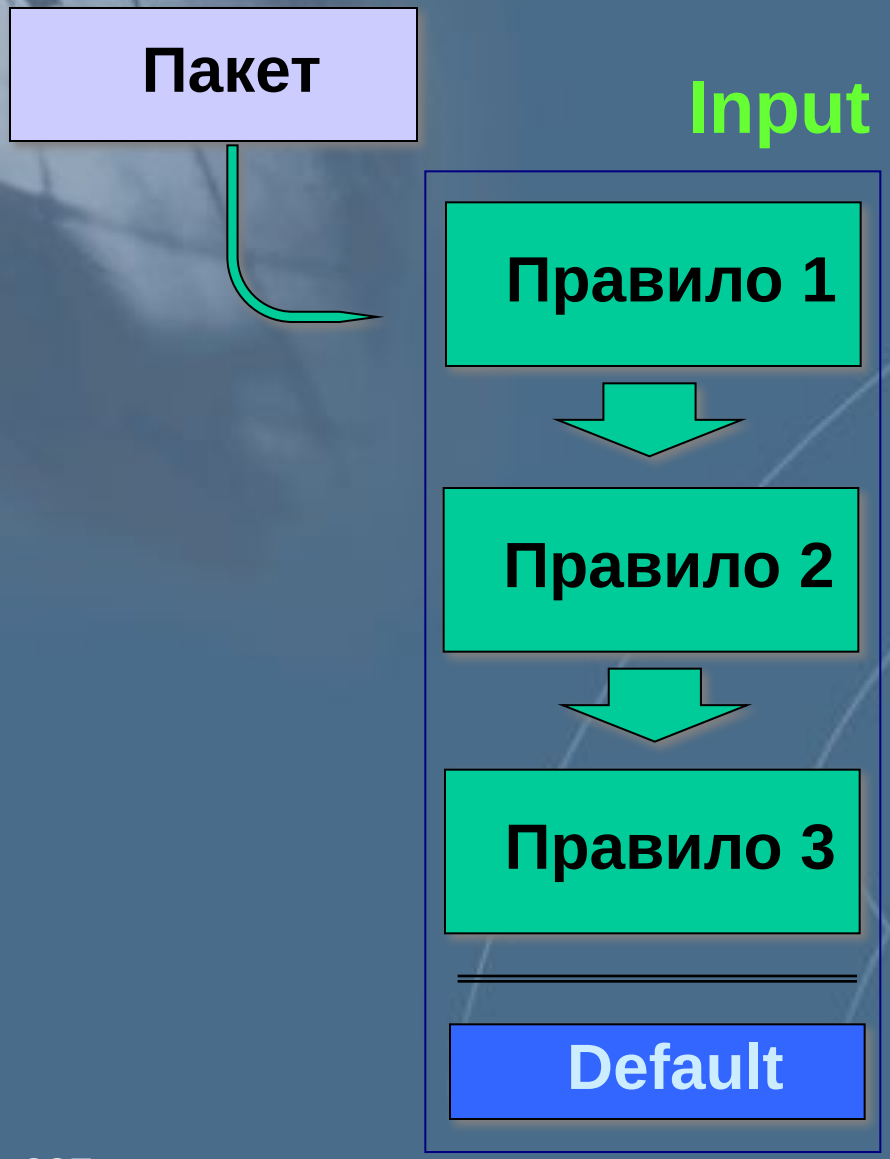


Пакетный фильтр на базе ОС Linux

Архитектура пакетного фильтра ipchains



Работа отдельной цепочки фильтрации

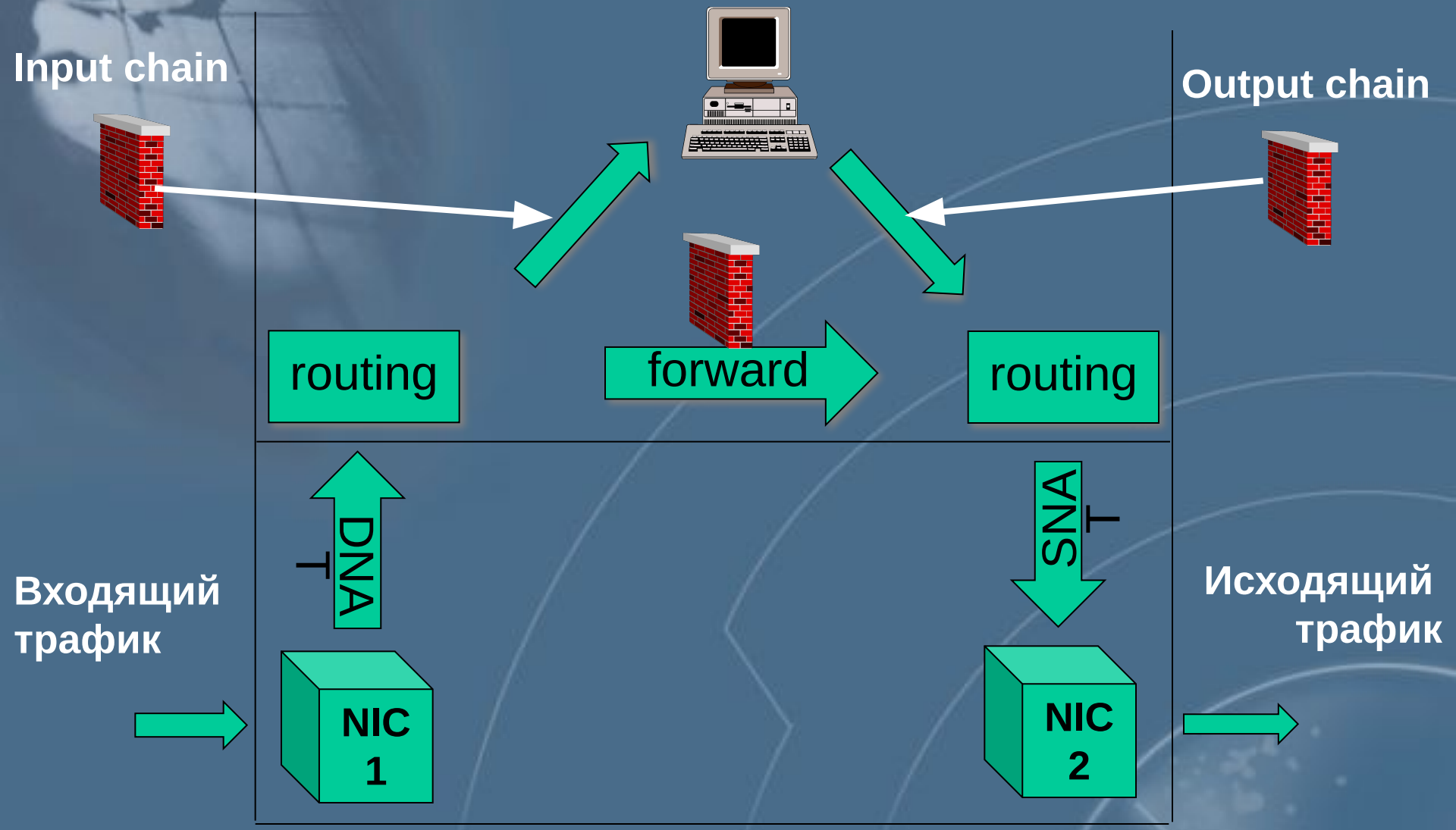


<условие>
<действие>

Если пакет подходит под условие, то к нему применяется действие.

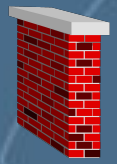
ACCEPT либо DROP

Архитектура пакетного фильтра iptables



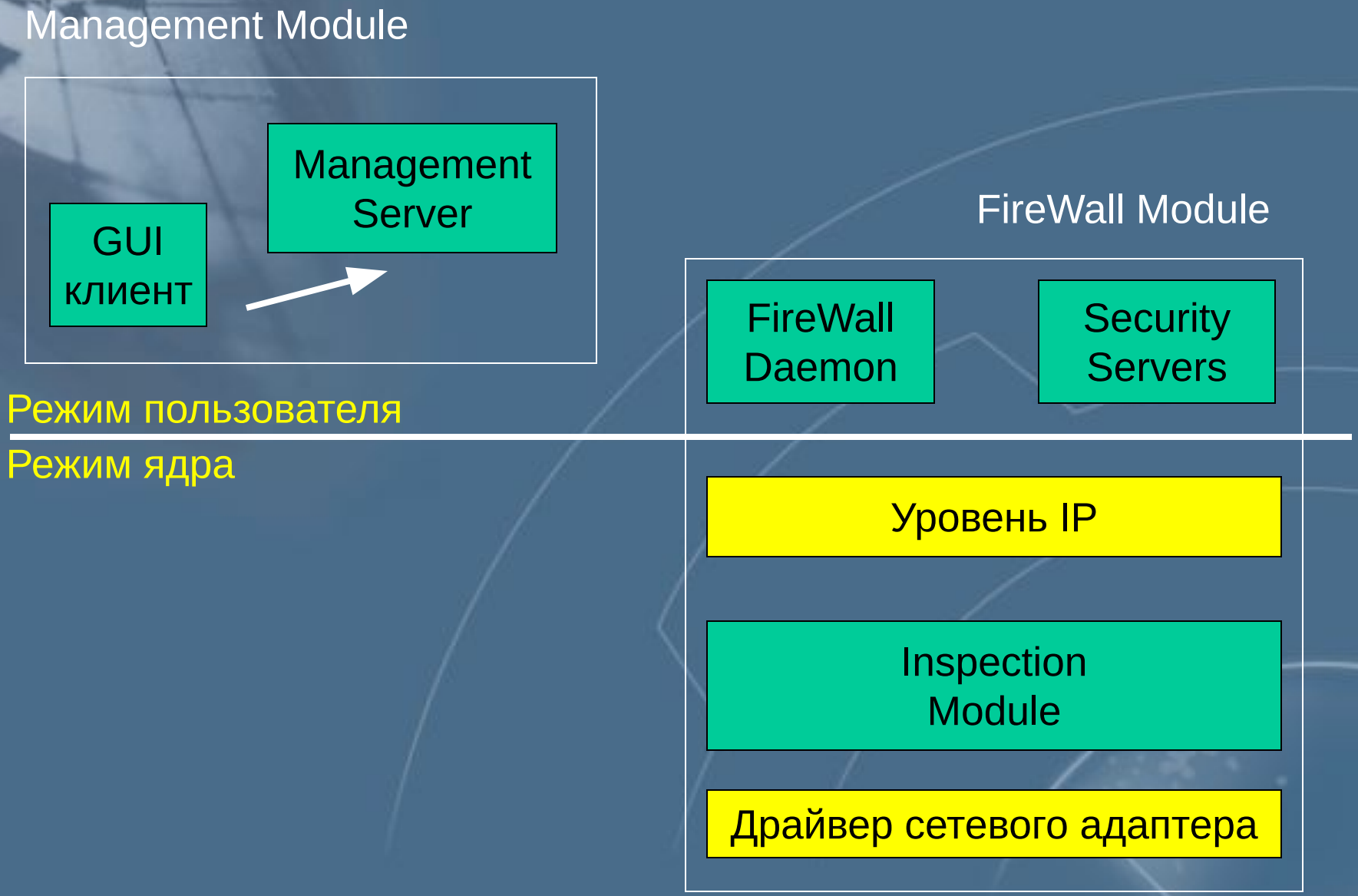
Практическая работа 5
Пакетный фильтр на базе Linux

Настройка фильтрации ICMP и UDP



Межсетевой экран CheckPoint FireWall-1

Архитектура FireWall-1

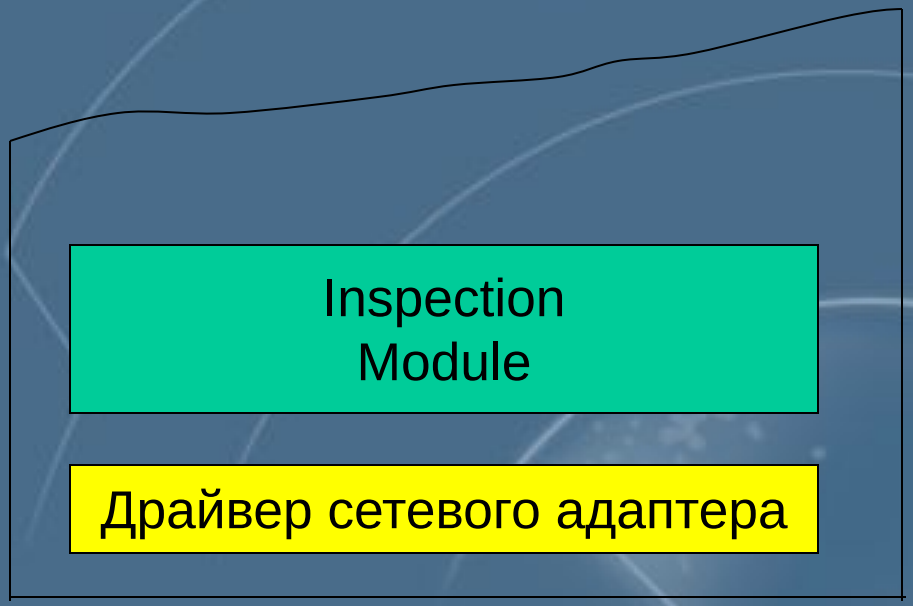


Inspection Module

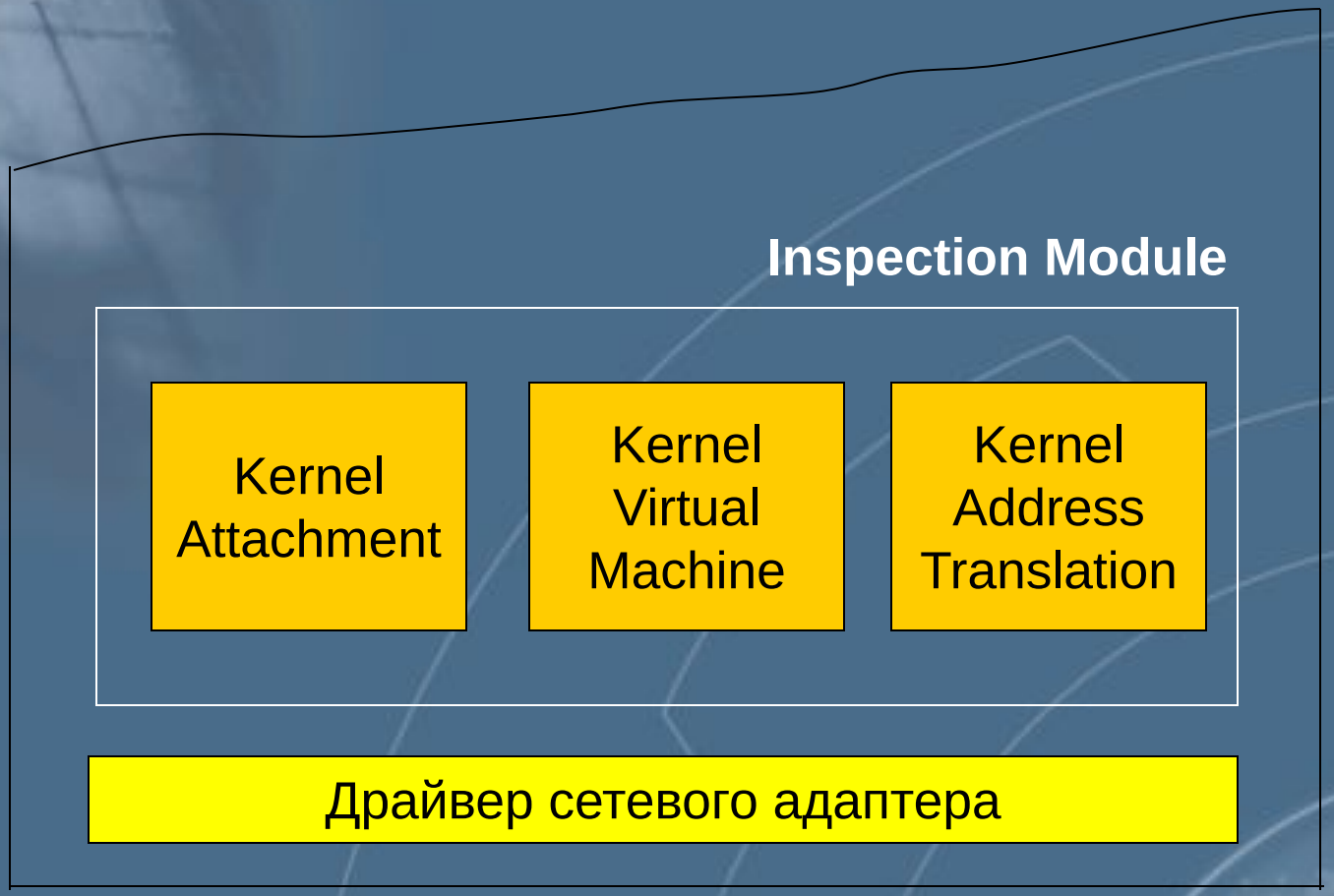
Реализован в виде драйвера

Выполняет функции

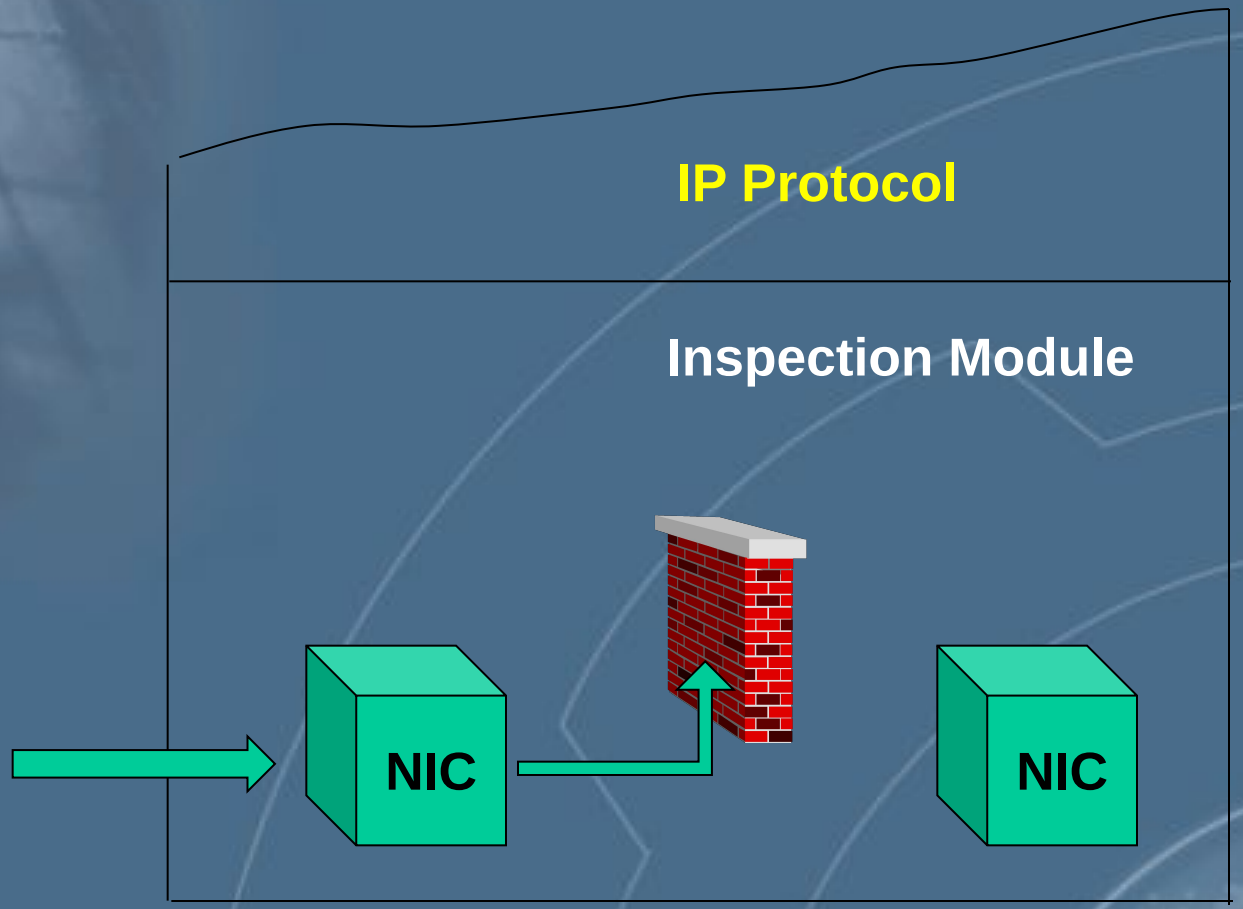
- **Клиентская аутентификация**
- **Аутентификация сессии**
- **Трансляция адресов**
- **Контроль доступа**
- **Аудит**



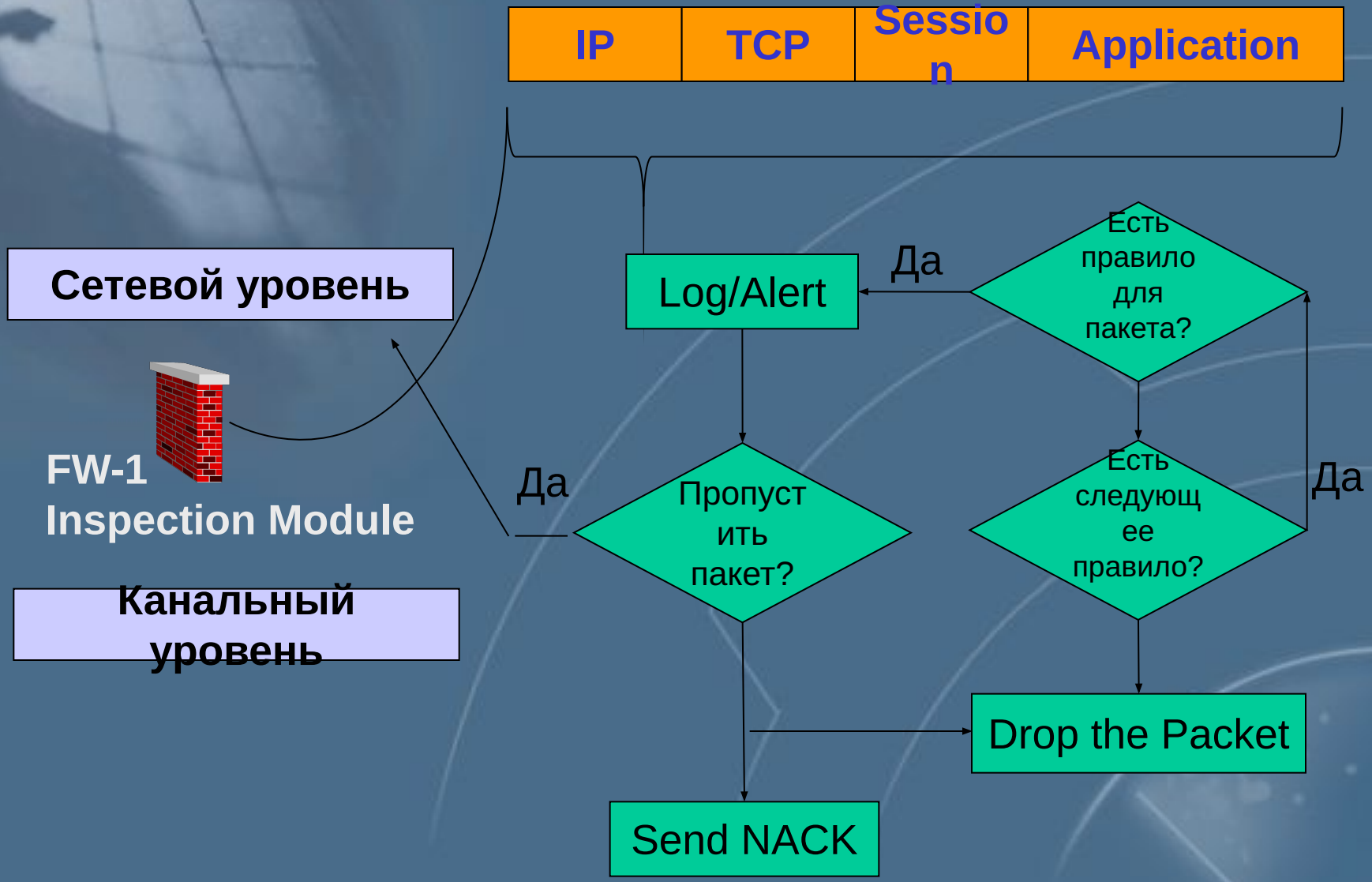
Компоненты Inspection Module



Работа Inspection Module



Работа Inspection Module



Конфигурация FireWall-1

GUI клиент

GUI клиент

FireWall Module

Management Module

Management Server

GUI клиент

Практическая работа 6
МЭ CheckPoint Firewall-1

Управление объектами
Задание правил фильтрации