Сетевая безопасность

Содержание модуля

1. Основы сетевой безопасности
2. Фаерволы (брандмауэры) и сетевые устройства безопасности
3. IPS/IDS
4. DDOS и Anti-DDOS решения

Основы сетевой безопасности

1

Сетевая безопасность

Сети раскрывают ресурсы широкому кругу лиц, в том числе потенциальным атакующим

Компьютерные сети сложные и, следовательно, уязвимы

Основная задача сетевой безопасности обеспечить три важнейших сервиса для управления рисками

Терминология

Актив (Asset) —
то, что имеет значение для организации

Уязвимость —
слабость в системе или дизайне, которая может быть использована

Угроза —
потенциальная опасность для системы или информации

Терминология

Эксплойт —
механизм, который использует уязвимость для компрометации безопасности или функционирования системы

Риск —
вероятность, что определенная угроза будет реализована посредством уязвимости

Контрмеры —
действия направленные на смягчение и предотвращение последствий потенциального риска

Классификация информационных активов

- Не все активы одинаково ценны
- Цель классификации активов — обеспечить комбинацию целостности, конфиденциальности и доступности соответствующих ценности актива
- Классификация может потребоваться в соответствии с законодательством
- Основные преимущества классификации:
  - Определяет обязательства организации по защите информационных активов
  - Определяет наиболее ценный актив
  - Определяет контрмеры, которые применяются для защиты активов

Уязвимости

Причины уязвимостей

- Недостатки политик
- Ошибки дизайна
- Слабости в протоколах
- Недостатки в программном обеспечении
- Неправильная конфигурация
- Враждебный код
- Человеческий фактор

Контрмеры

Классификация контрмер

- Административные, технические, физические
- Превентивные, реактивные, детективные
- Предотвращение, уменьшение, передача, принятие

Основные этапы атаки

1. Анализ следов (разведка)
2. Перечисление приложений и операционных систем
3. Манипуляция пользователем для получения доступа
4. Повышение привилегий
5. Сбор дополнительных паролей и секретов
6. Установка «черного хода»
7. Использование скомпрометированной системы

Угрозы

Классификация угроз

- Отказ в обслуживании
- Вирусы, черви, трояны
- Фишинг
- Перехват паролей
- Человек в середине
- Ботнет
- Социальная инженерия
- Эксплойты

Дизайн защищенной сети

Основные принципы

- Эшелонированная оборона
- Обособление
- Принцип наименьших привилегий
- Поиск слабых звеньев
- Разделение и ротация обязанностей
- Иерархические доверенные компоненты
- Опосредованный доступ
- Учет и отслеживание

Эшелонированная оборона

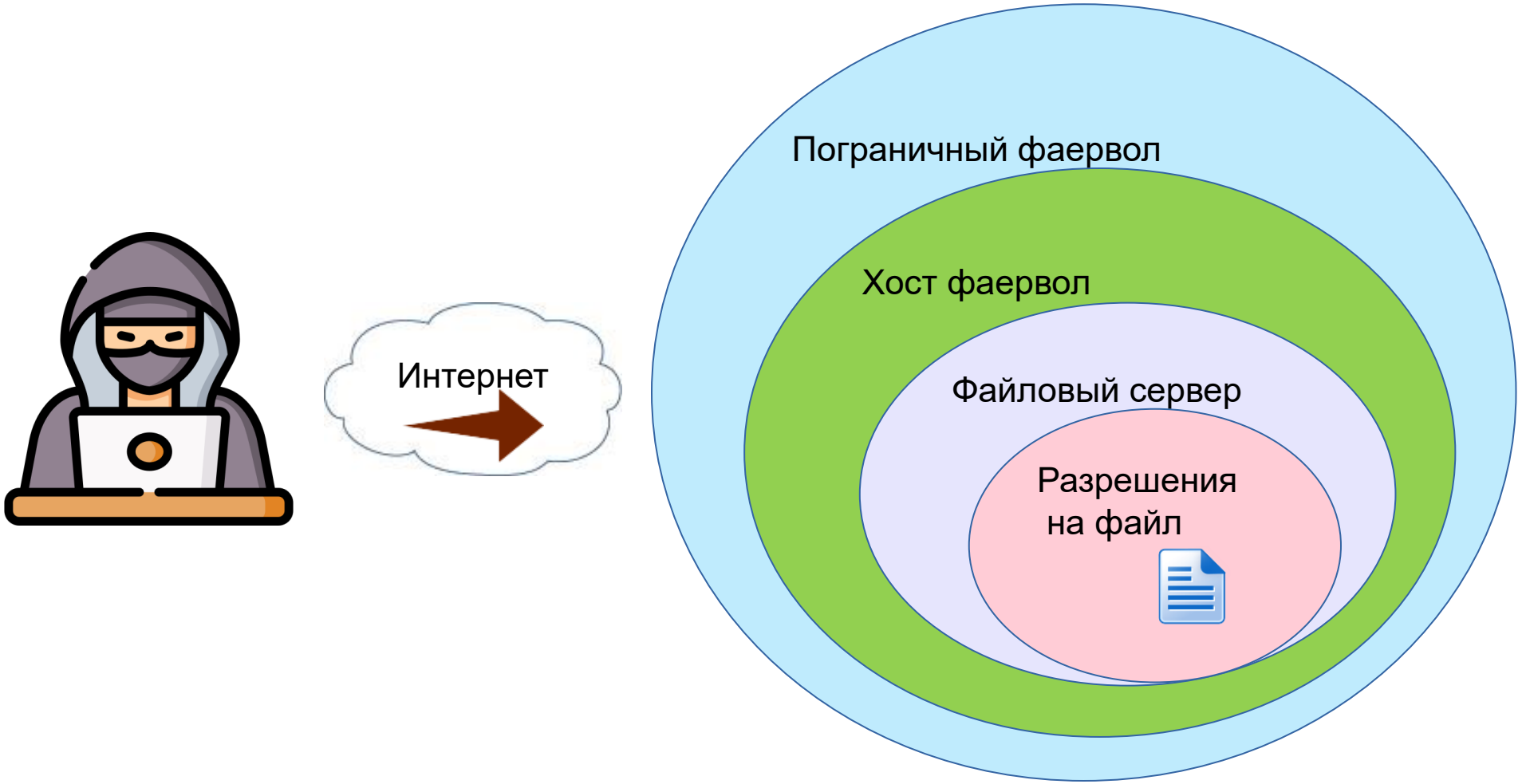
Многоуровневый подход к защите:

- Защита сетевой инфраструктуры
- Защита рабочих станций и автоматизированных рабочих мест
- Защита серверной инфраструктуры
- Централизованное управление, сбор данных и оповещение
- Организационные меры и создание политик безопасности

Рекомендации:

- Механизмы безопасности поддерживают друг друга разнообразно и избыточно
- Механизмы безопасности не зависят друг от друга
- Слабые звенья системы защищаются сильными

Эшелонированная оборона



Терминология

Политика безопасности —
информация для пользователей, персонала и руководства

Зачем?

- Определяет механизмы безопасности
- Является фундаментом обеспечения безопасности

Что делает?

- Защищает людей, имущество и информацию
- Определяет набор правил ожидаемого поведения
- Дает полномочия для специалистов на наблюдение, исследование и проверку
- Определяет ответственность за нарушение

Угрозы безопасности для сетевых устройств

Основные угрозы

- Неавторизованный физический доступ
- Неавторизованный сетевой доступ
- Использование незащищенных протоколов управления
- Неправильное обслуживание

Контрмеры и сетевые устройства

Угроза	Контрмеры
Неавторизованный физический доступ	Физическое ограничение доступа: замки, охрана, контроль доступа в помещение
Неавторизованный сетевой доступ	Пароли, централизованная аутентификация
Использование незащищенных протоколов управления	Использовать SSH, HTTPS, SNMPv3
Неправильное обслуживание	Разработать и строго соблюдать регламент конфигурирования оборудования

Контрмеры угрозам сетевого взаимодействия

Контрмеры	Примеры
Контроль подключения к сети	Portsecurity, 802.1x, WPA
Контроль подключенных устройств	DHCP snooping, Dynamic ARP Inspection, IP Source Guard
Блокировка нежелательного трафика	IP ACL, Zone based firewall, Unicast Reverse Path Forwarding
Защита передаваемого трафика	IPSec, SSL VPN, HTTPS
Инспекция пакетов	Signature-based, Anomaly-based, Policy-based

Демонстрация

- Применение защиты доступа к устройствам
- Защита доступа к сети на 2 уровне (portsecurity)
- Фильтрация трафика на 3 ровне (ACL)

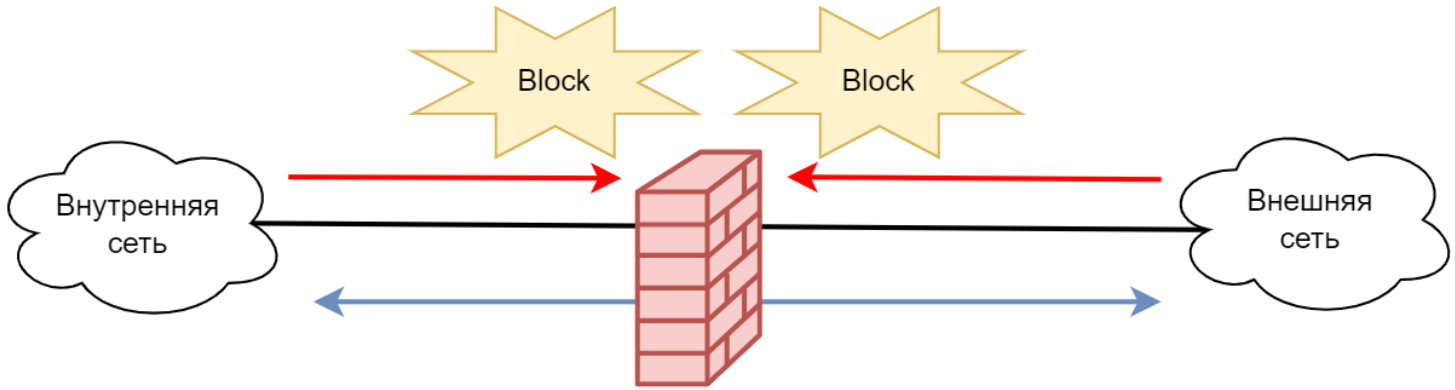
Фаерволы и сетевые устройства безопасности

2

Определение брандмауэра

Брандмауэр (Firewall) —
система, которая обеспечивает соблюдение политики контроля доступа между двумя или более доменами безопасности

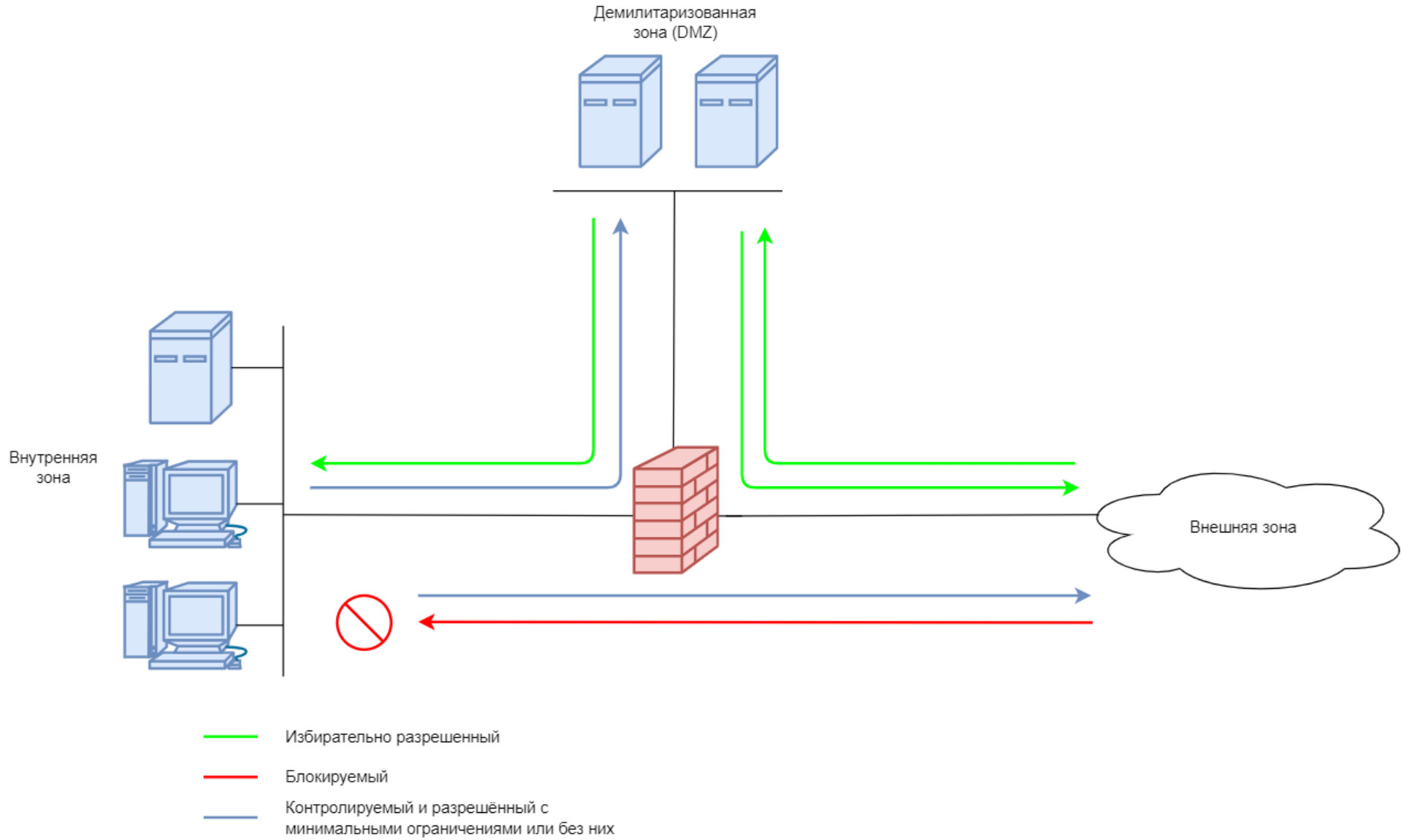
Принцип работы брандмауэра



Запрещенный трафик

Разрешенный трафик

Разделение на зоны



Задачи фаервола

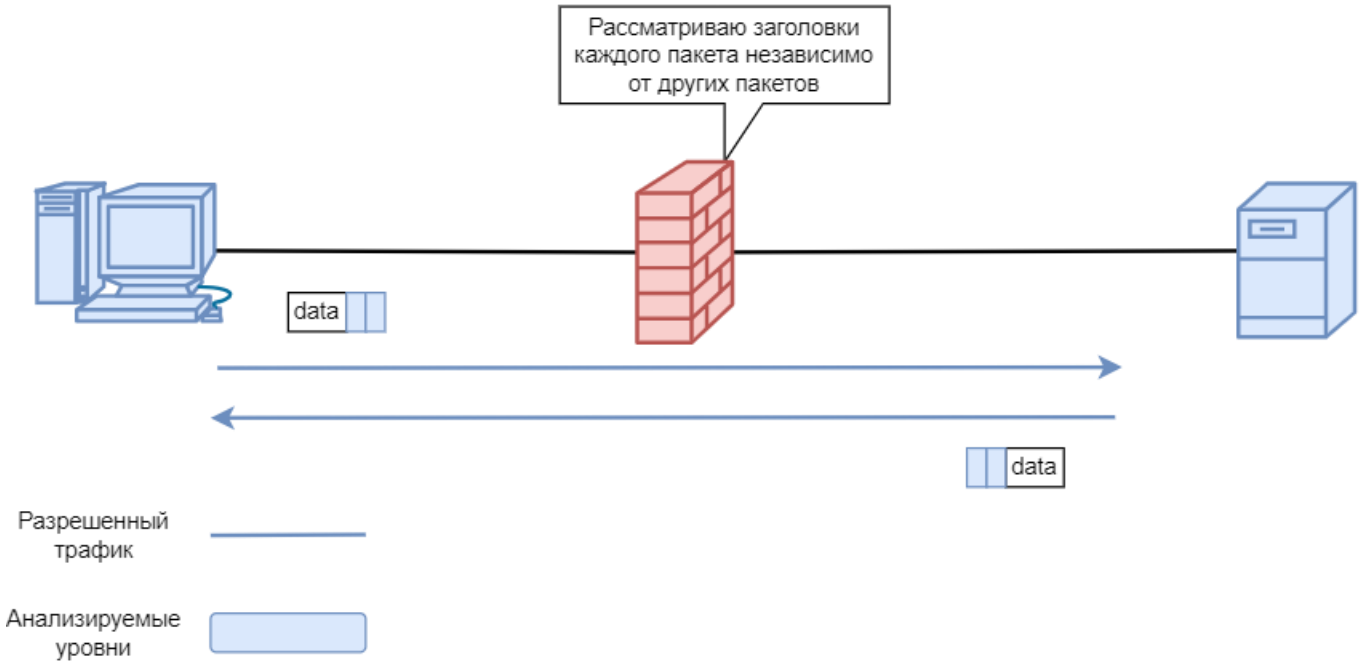
Основные

- Фильтрация пакетов без отслеживания соединений
- Фильтрация пакетов с отслеживанием соединений
- Фильтрация пакетов с отслеживанием соединений, инспекцией и контролем приложений

Дополнительные

- Предотвращение вторжений
- Анализ сетевого поведения
- Шлюз для приложений
- Виртуальные частные сети (VPN)

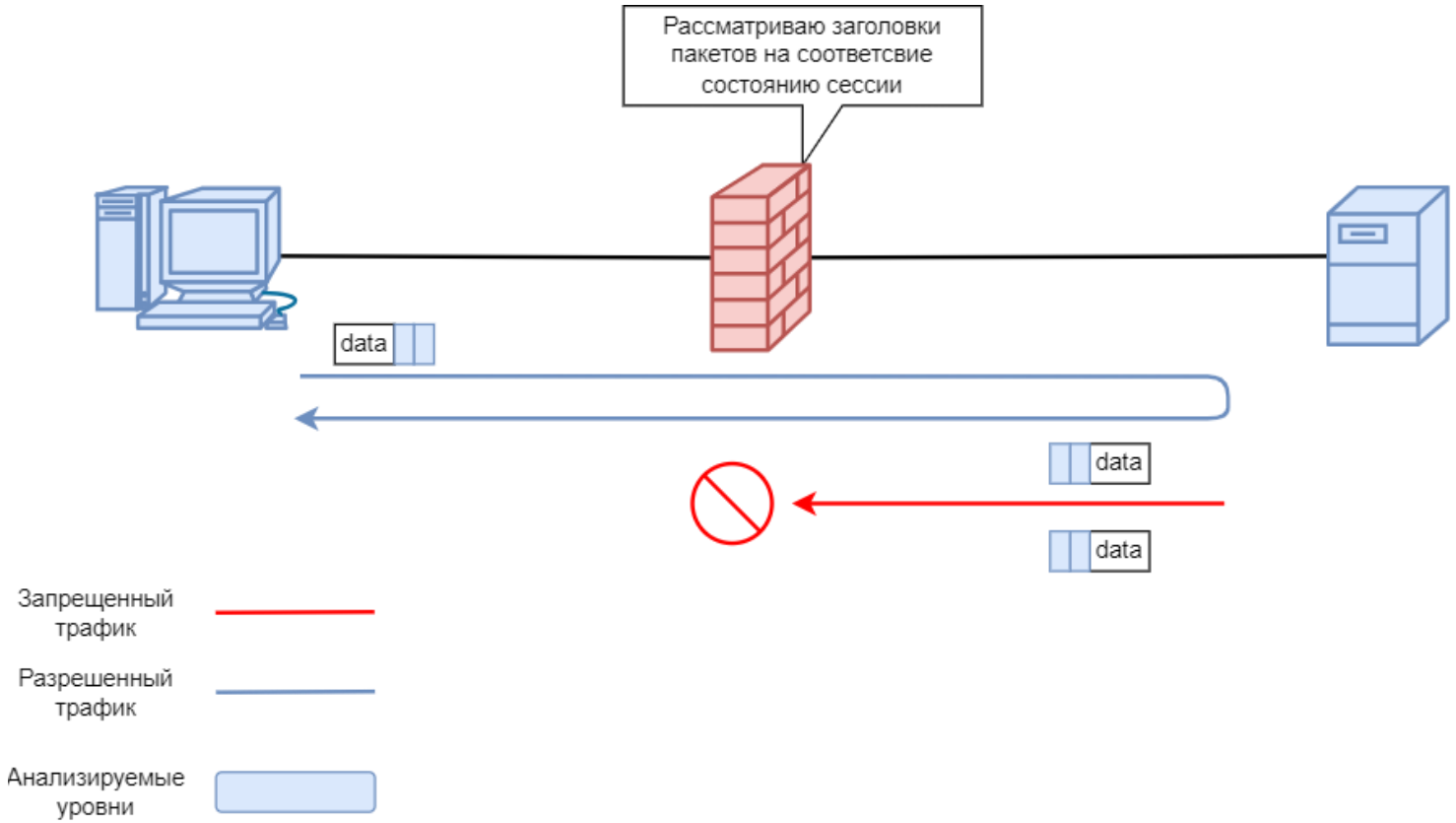
Фильтрация пакетов без отслеживания соединений



Уровень модели OSI

- 7 - Уровень приложений
- 6 - Уровень представления
- 5 - Сеансовый уровень
- 4 - Транспортный уровень
- 3 - Сетевой уровень
- 2 - Канальный уровень
- 1 - Физический уровень

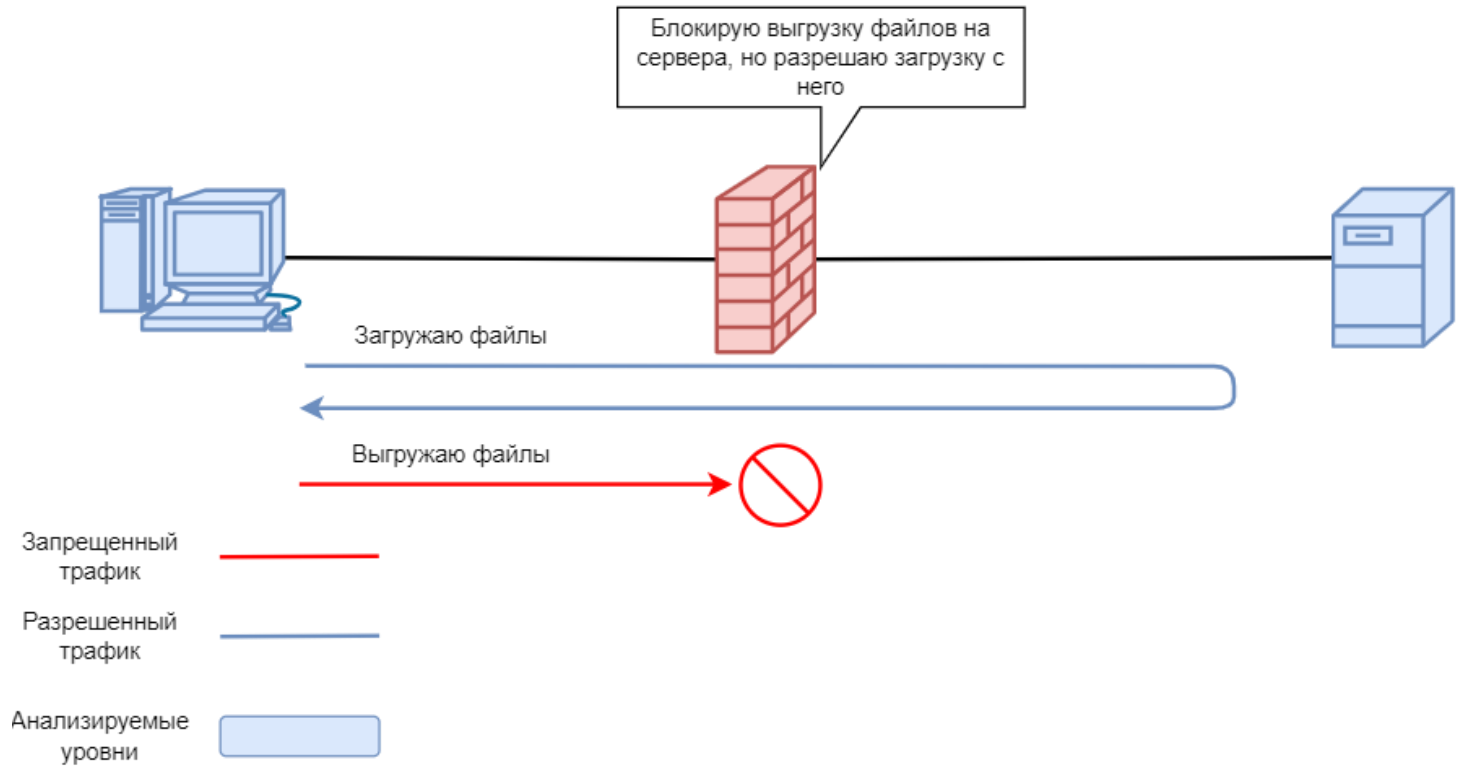
Фильтрация пакетов с отслеживанием соединений



Уровень модели OSI

- 7 - Уровень приложений
- 6 - Уровень представления
- 5 - Сеансовый уровень
- 4 - Транспортный уровень
- 3 - Сетевой уровень
- 2 - Канальный уровень
- 1 - Физический уровень

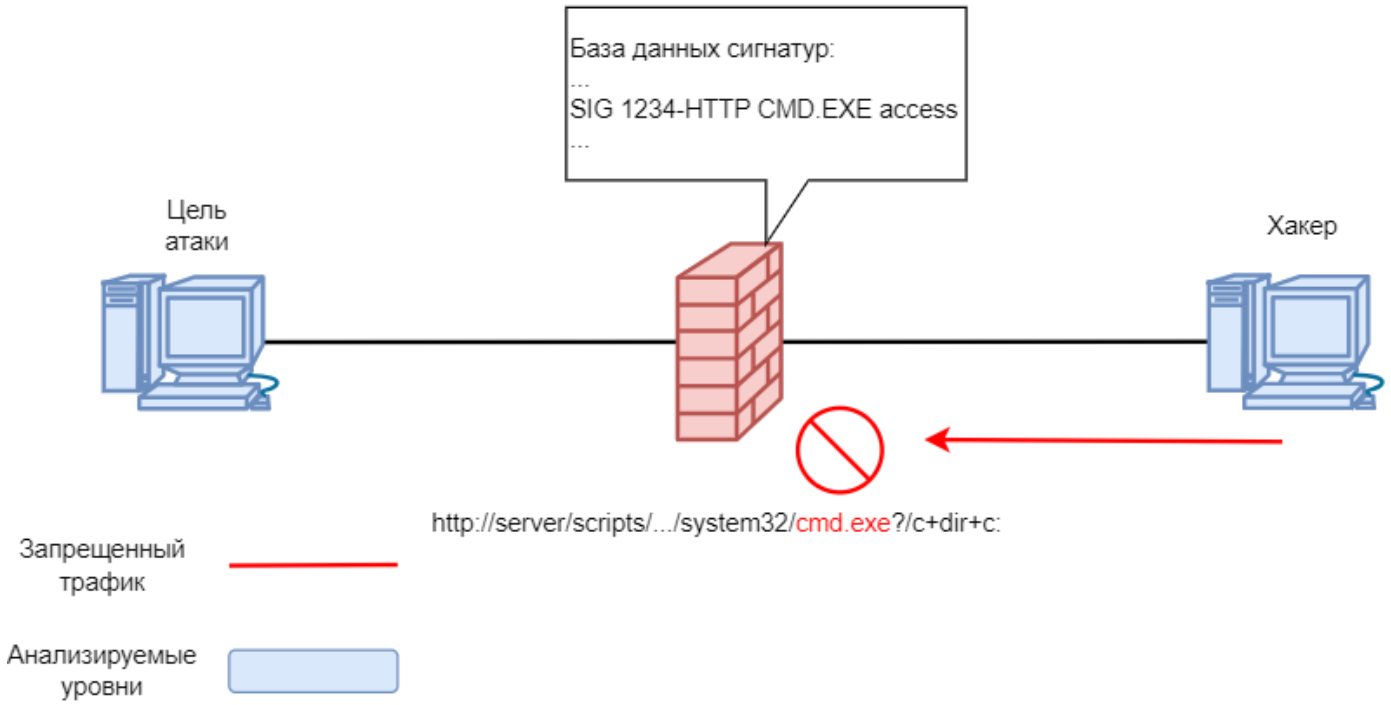
Фильтрация пакетов с отслеживанием соединений, инспекцией и контролем приложений



Уровень модели OSI

- 7 - Уровень приложений
- 6 - Уровень представления
- 5 - Сеансовый уровень
- 4 - Транспортный уровень
- 3 - Сетевой уровень
- 2 - Канальный уровень
- 1 - Физический уровень

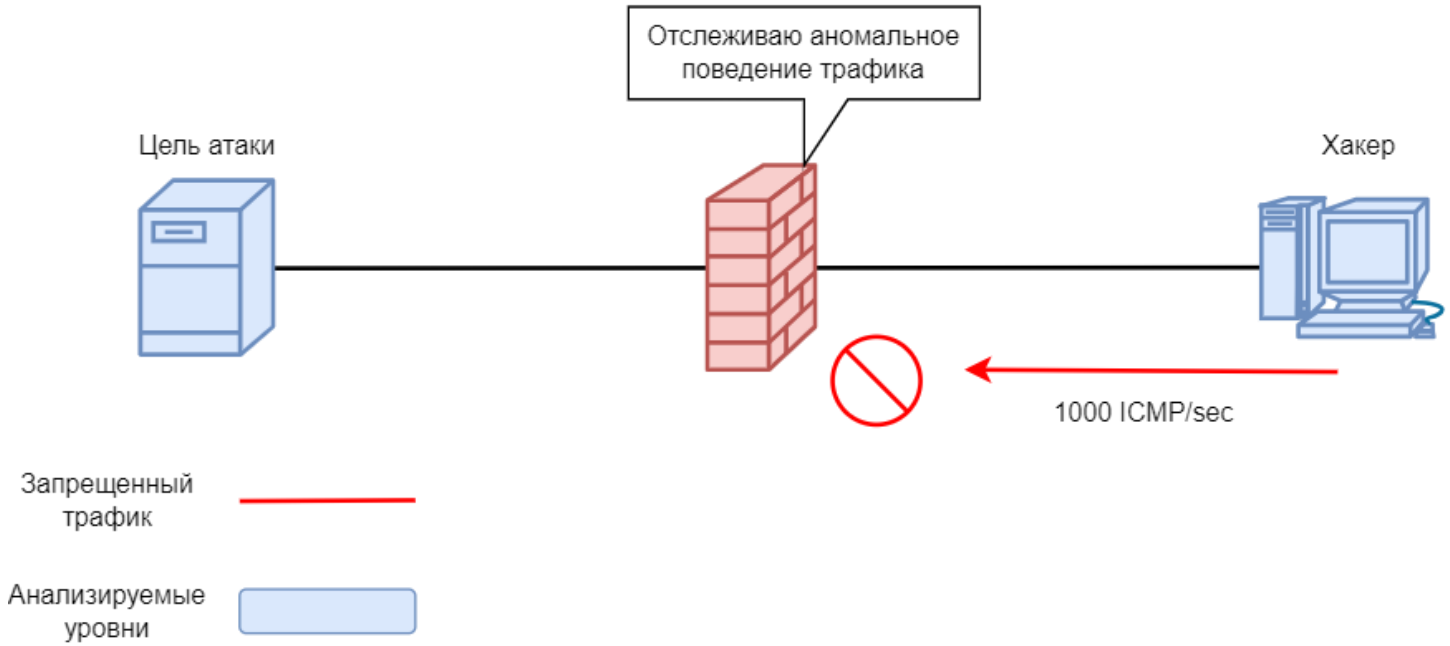
Предотвращение вторжений



Уровень модели OSI

- 7 - Уровень приложений
- 6 - Уровень представления
- 5 - Сеансовый уровень
- 4 - Транспортный уровень
- 3 - Сетевой уровень
- 2 - Канальный уровень
- 1 - Физический уровень

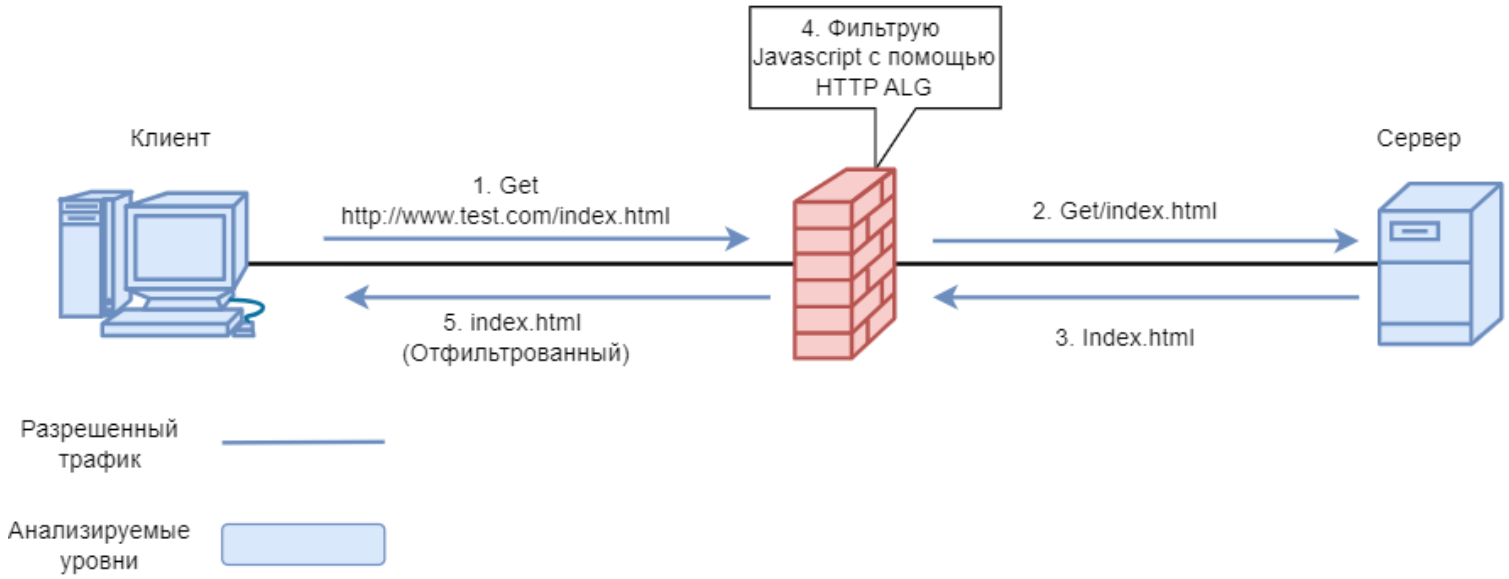
Анализ сетевого поведения



Уровень модели OSI

- 7 - Уровень приложений
- 6 - Уровень представления
- 5 - Сеансовый уровень
- 4 - Транспортный уровень
- 3 - Сетевой уровень
- 2 - Канальный уровень
- 1 - Физический уровень

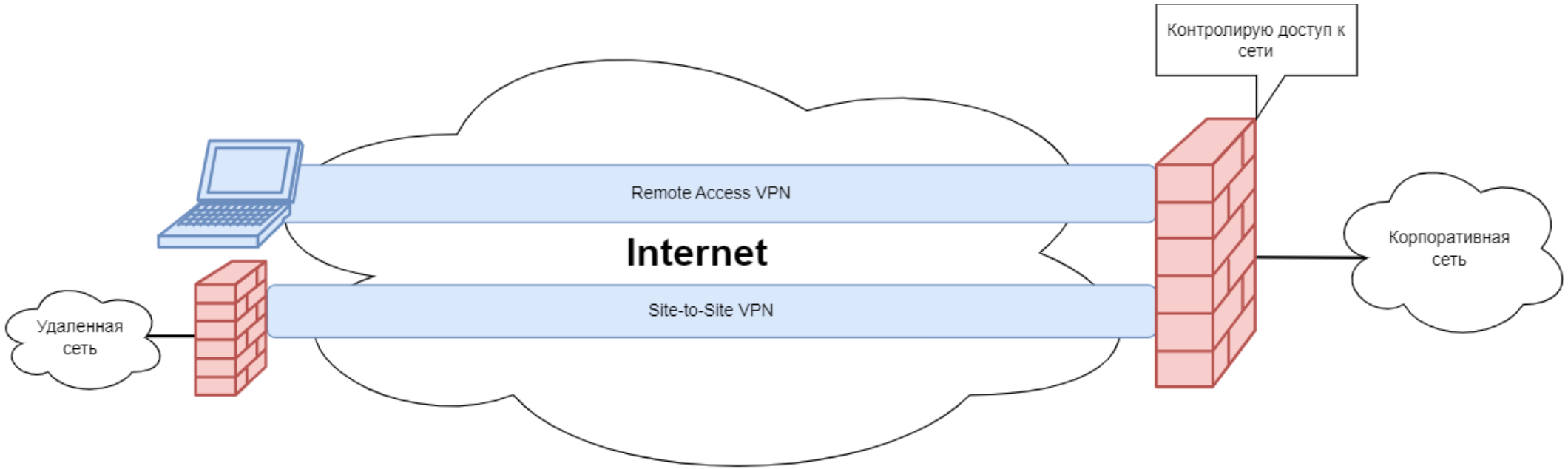
Шлюз для приложений



Уровень модели OSI

- 7 - Уровень приложений
- 6 - Уровень представления
- 5 - Сеансовый уровень
- 4 - Транспортный уровень
- 3 - Сетевой уровень
- 2 - Канальный уровень
- 1 - Физический уровень

VPN

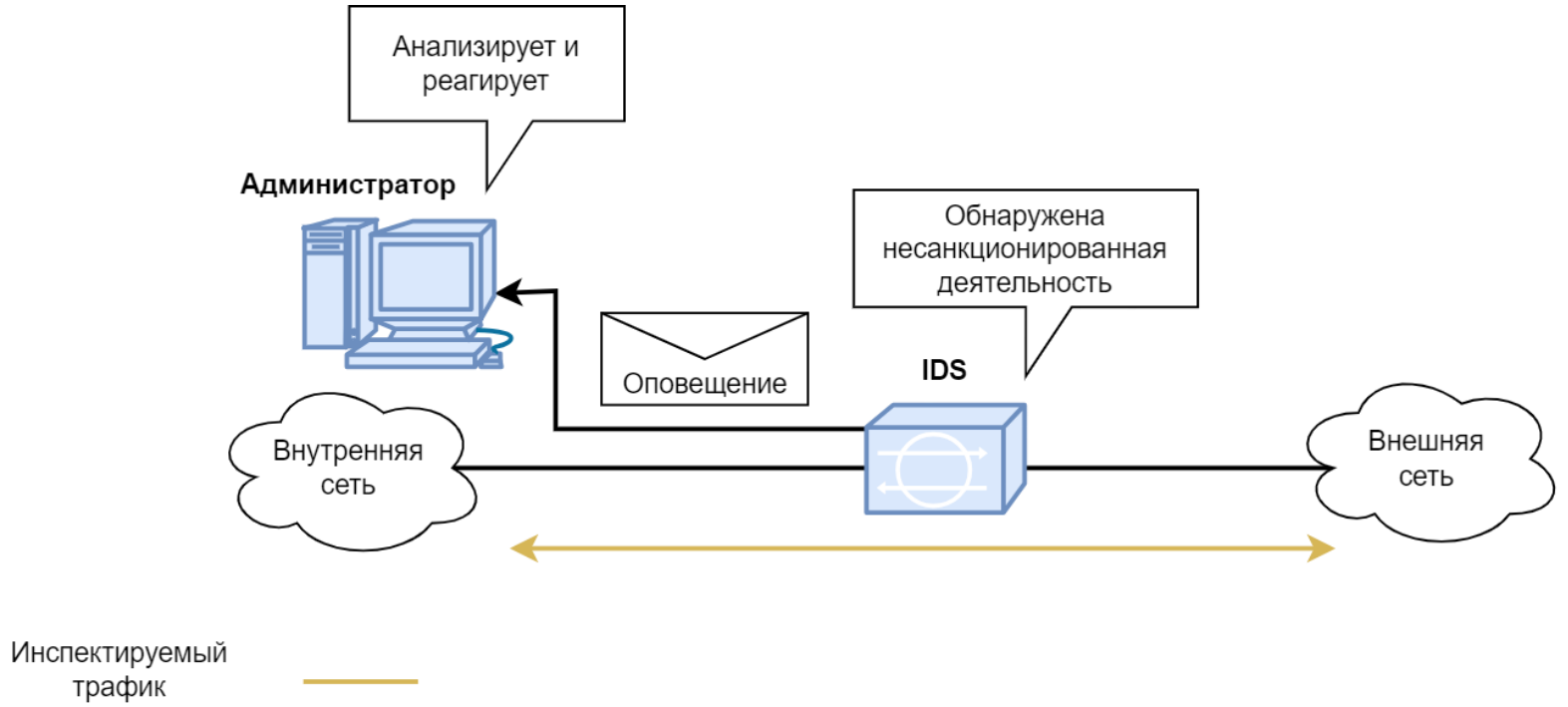

Контролирую доступ к сети
Remote Access VPN
Internet
Site-to-Site VPN
Удаленная сеть
Корпоративная сеть

Intrusion Prevention System (IPS)/ Intrusion Detection System (IDS)

3

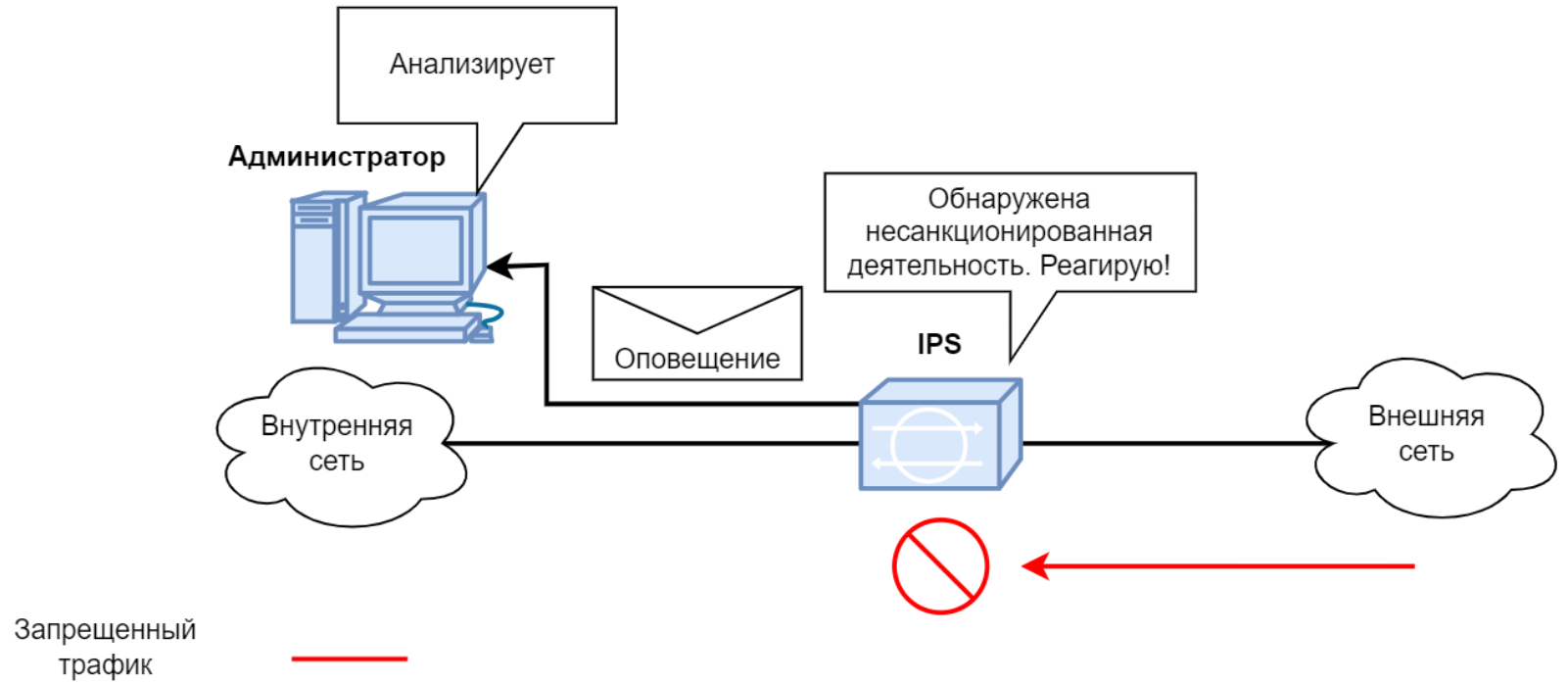
Определение IDS

Система обнаружения вторжений (Intrusion Detection System (IDS)) — система контроля безопасности, которая обнаруживает неправомерное использование сетевых ресурсов и несанкционированный доступ к ним



Определение IPS

Система предотвращения вторжений (Intrusion Prevention System (IPS)) — система контроля безопасности, которая обнаруживает и предотвращает неправомерное использование сетевых ресурсов и несанкционированный доступ к ним



Реакции системы безопасности

Типы реакций

Истинно-позитивный **(true positive)**	Ложно-позитивный **(false positive)**	Истинно-негативный **(true negative)**	Ложно-негативный **(false negative)**
система безопасности сработала в результате вредоносной активности	система безопасности сработала ложно в результате безобидных действий	система безопасности не сработала, поскольку вредоносных действий не было	система безопасности не сработала несмотря на наличие вредоносных действий

Режимы работы IPS

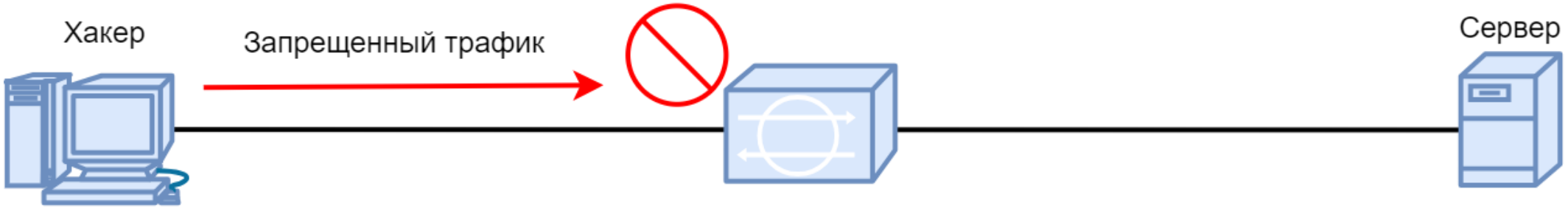
Подходы к предотвращению сетевых вторжений

- Signature-Based IPS (на основе сигнатур)
- Anomaly-Based IPS (на основе отклонений)
- Policy-Based IPS (на основе политик)
- Endpoint Security Controls (контроль безопасности узлов)

Signature-Based IPS

Требуется база данных об известном вредоносном трафике

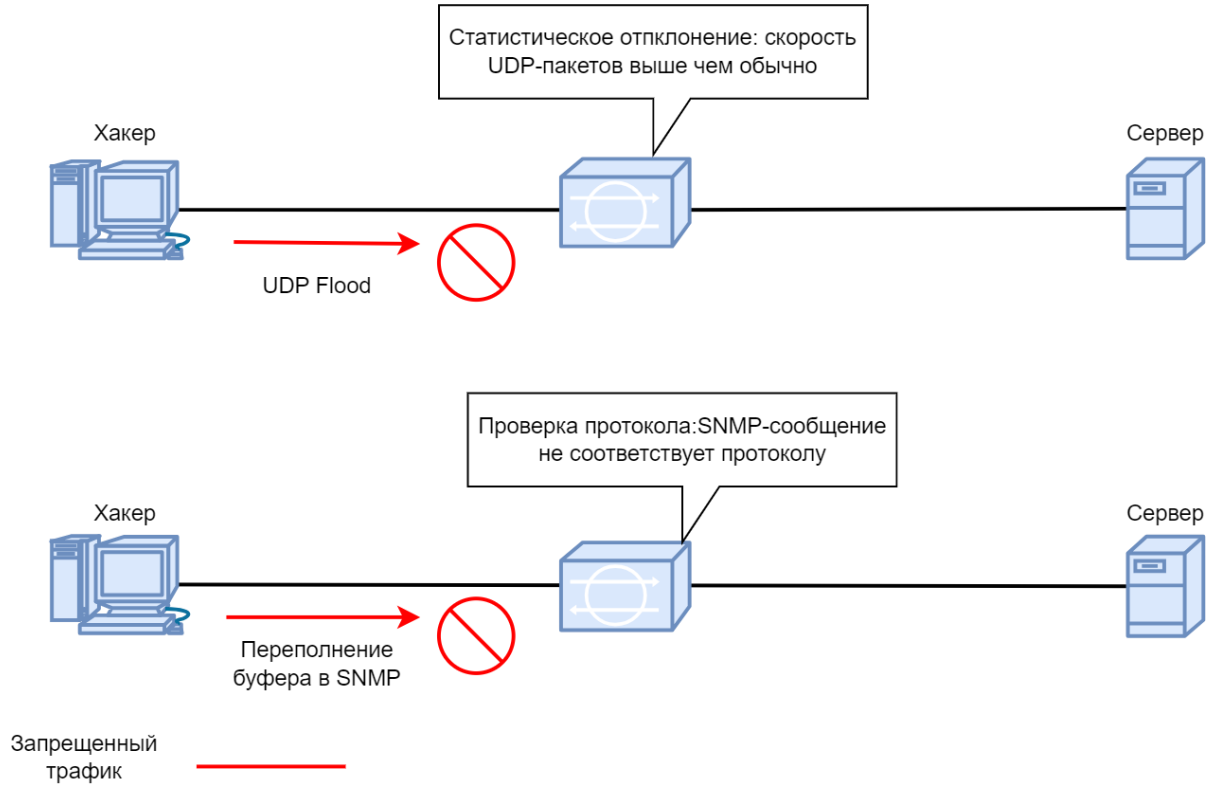
База данных должна постоянно обновляться



Anomaly-Based IPS

Существует два типа: обнаружение статистических аномалий и проверка протокола

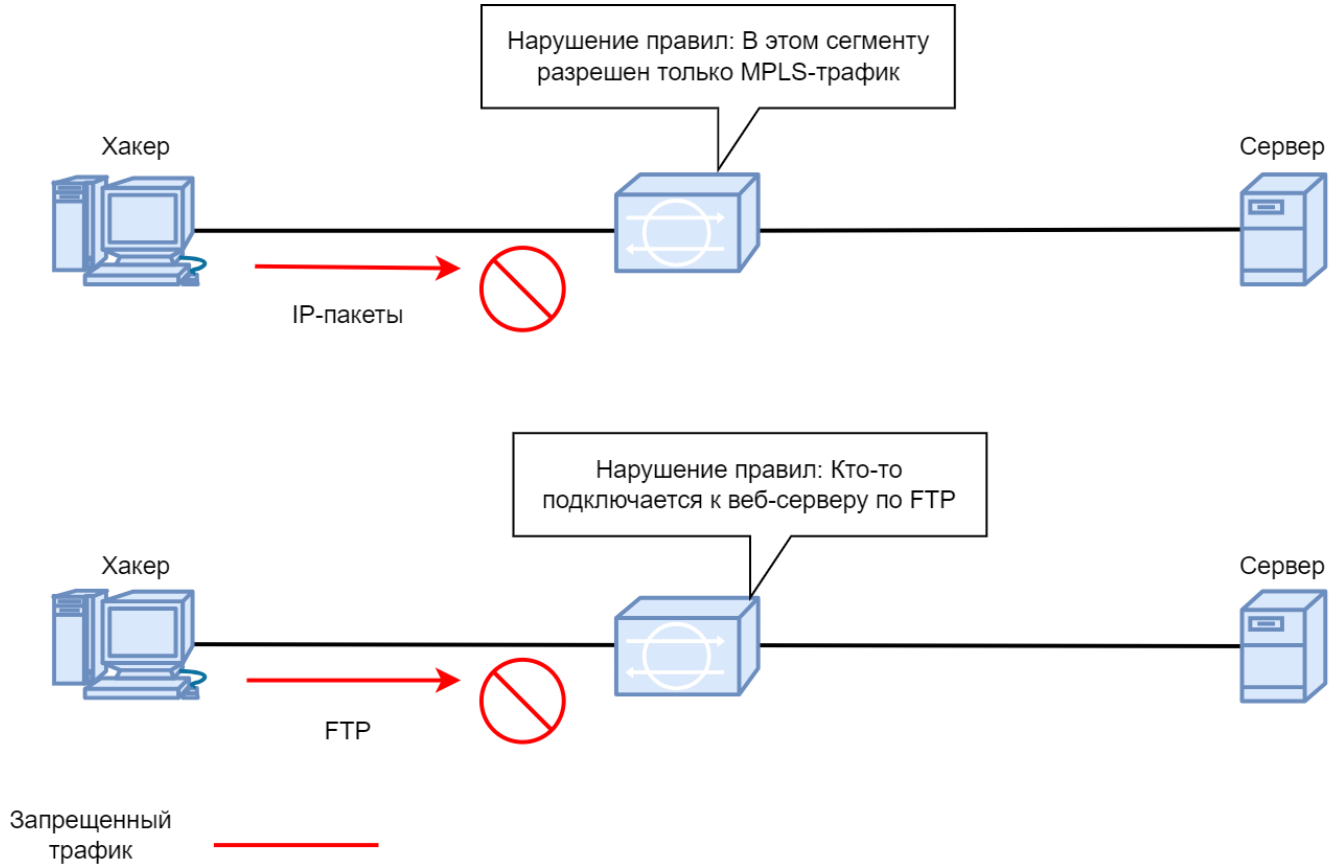
Для обнаружения статистических аномалий требуется определение «нормы»



Policy-Based IPS

Требуется база данных политик

Часто это реализуется классическими системами брандмауэров

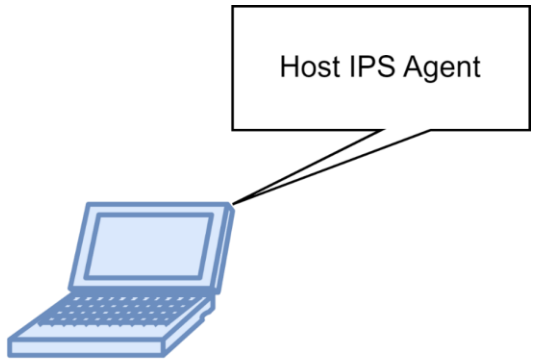


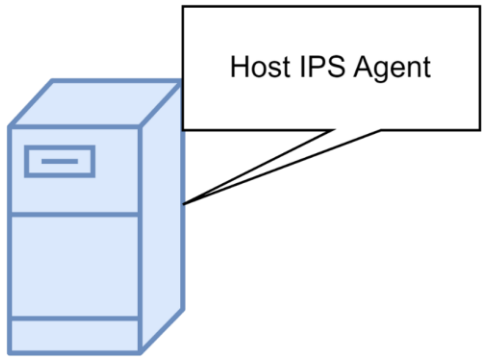
Endpoint Security Controls

Собственные элементы управления ОС и приложениями

На хостах устанавливается ПО агента:

- Расширяет встроенные средства контроля безопасности ОС
- Обеспечивает обнаружение уязвимостей и защиту отдельных хостов
- Не требует специального оборудования





Методы обеспечения безопасности

Ориентированные на сеть

- Защищенные сетевые устройства
- Строгие правила брандмауэра
- Использование IPS в сети

Ориентированные на конечные устройства

- Защищенная и обновленная ОС
- IPS-агент на базе хоста
- Защищенные приложения

DDOS и Anti-DDOS решения

4

DOS и DDOS

DoS - атака (Denial of Service) —
отказ в обслуживании, атака на вычислительную систему с целью довести её до отказа, ситуации, когда система станет недоступна для пользователей

DDoS - атака (Distributed Denial of Service) —
перегрузка системы происходит при одновременной атаке с большого количества устройств на конкретный виртуальный сервер или домен

Классификация

- Атаки уровня инфраструктуры
- Атаки уровня приложения

Последствия DDoS-атак

- Частичная или полная недоступность сетевой инфраструктуры
- Финансовые расходы
- Репутационные потери

Атаки уровня инфраструктуры

Виды инфраструктурных атак

- Перегрузка вычислительных ресурсов
- Занятие дискового пространства
- Обход системы квот
- Злоупотребление доступом к ресурсам
- Атака второго рода

Атаки уровня приложения

DDoS-атаки

Признаки

- Некорректная работа серверного ПО и операционных систем
- Пиковая нагрузка по запросам на сервер
- Рост числа запросов на порты
- Одинаковая модель поведения
- Однотипные запросы к портам и сервисам

Защита от DDoS

Способы защиты

- Контроль версий ПО и сетевых служб
- Следить за доступом к сетевым службам
- Сканировать систему на наличие уязвимостей
- Использовать брандмауэр
- Использовать аппаратные средства защиты
- Актуальная отказоустойчивая архитектура
- Аппаратная избыточность

Что мы изучили?

1. Основы сетевой безопасности
2. Фаерволы (брандмауэры) и сетевые устройства безопасности
3. IPS/IDS
4. DDOS и Anti-DDOS решения

Спасибо за внимание!