Анализ кода и информационная безопасность

Лекция 14

МГУ / ВМК / СП

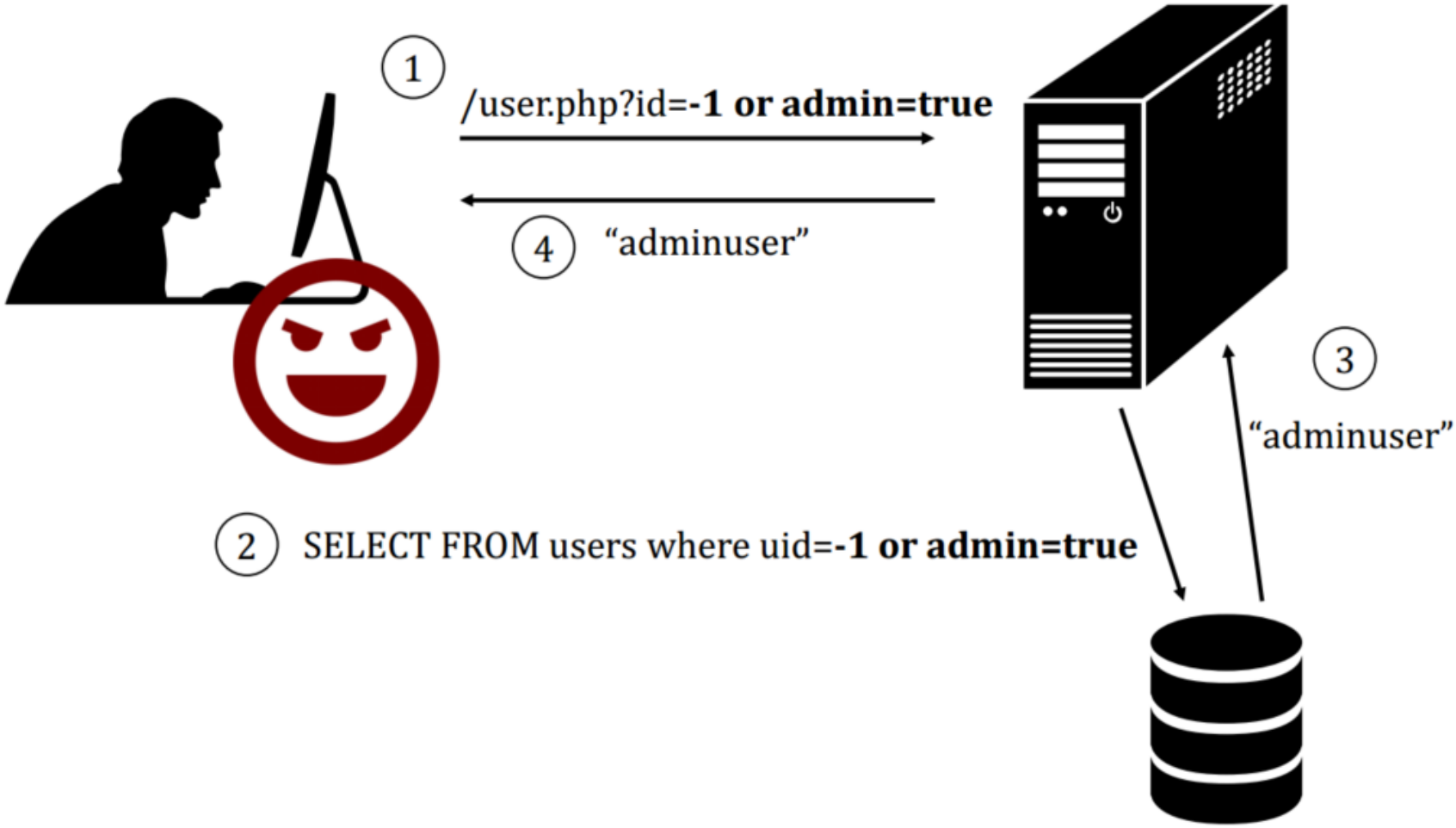
1401

СЕТЕВАЯ БЕЗОПАСНОСТЬ.

Что входит в понятие «сетевая безопасность»?

- Безопасность Web-приложений (XSS, CSRF, SQL Injection)
- Защита передаваемых данных от перехвата (SSL, …)
- Защита от Man-in-the-Middle (MITM) атак (Kerberos)
- **Защита сети:**
  - **Обеспечение доступности ресурса**
  - **Защита от сетевых атак и вторжений (Firewalls, IDS/IPS)**

Пример SQL Injection



Пример MITM атаки

Защита сети

- **Защита периметра - защита внутренней сети и хостов от угроз извне (Firewall, IDS)**
- Защита внутренней сети – защита хостов от угроз, попавших внутрь периметра (Antivirus)
- Расширение периметра – VPN
- Защита внутренней сети от внутренних угроз:
  - Утечка данных (DLP)
  - Подозрительная активность (SIEM)

1402

ЗАЩИТА ПЕРИМЕТРА.

Параметры системы защиты периметра

- **Выразительность:** Типы политик, которые могут задаваться
- **Эффективность:** Какая доля атак блокируется и какова доля ложных срабатываний
- **Ресурсоёмкость:** Потребность системы в ресурсах
- **Производительность:** пропускная способность системы
- **Простота** настройки и использования
- **Защищённость:** вносит ли система новые уязвимости
- **Прозрачность:** влияние системы на трафик и настройки сетевых приложений

Задачи межсетевого экрана

- Отделение защищаемой сети от внешнего мира
- Контроль доступа между подсетями с разным уровнем безопасности
- Защита от атак извне: сканирование портов, syn-flood, массовые пакеты
- Защита от нарушений работы сети: внешние SNMP пакеты
- Защита отдельных уязвимых приложений: FTP, SMTP, и т.д.

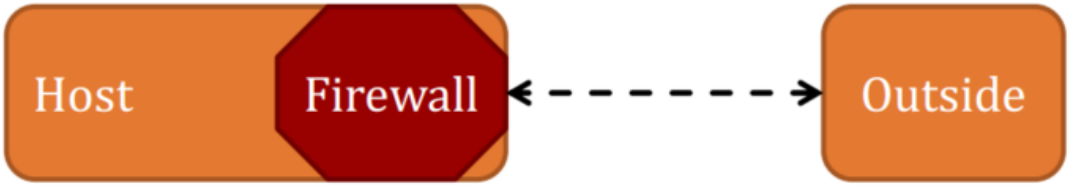
Параметры межсетевого экрана

- Особенности размещения:
  - Размещение на сетевом шлюзе
  - Установка на отдельные хосты
- Особенности обработки данных:
  - Фильтрация пакетов
  - Учёт состояния потока
  - Проксирование для отдельных приложений

Сравнение видов защит

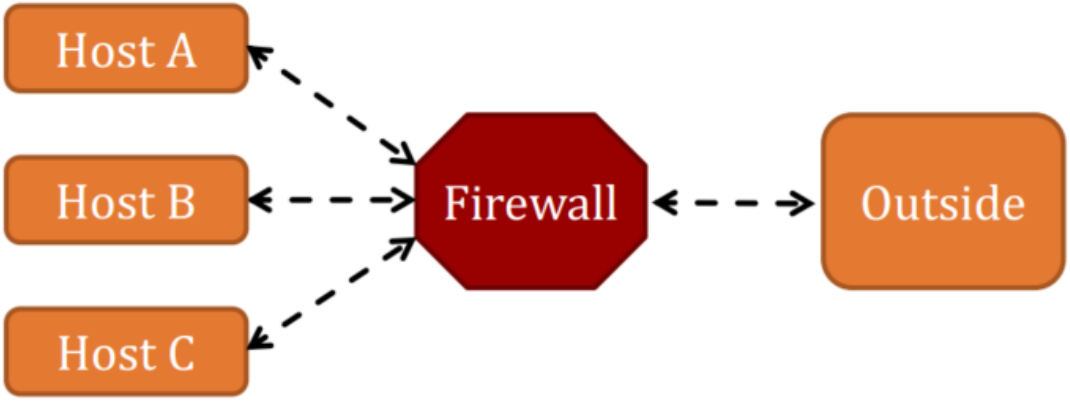
Особенности:

Host-based Firewall



- Учёт локальной конфигурации
- Мобильность

Network-Based Firewall



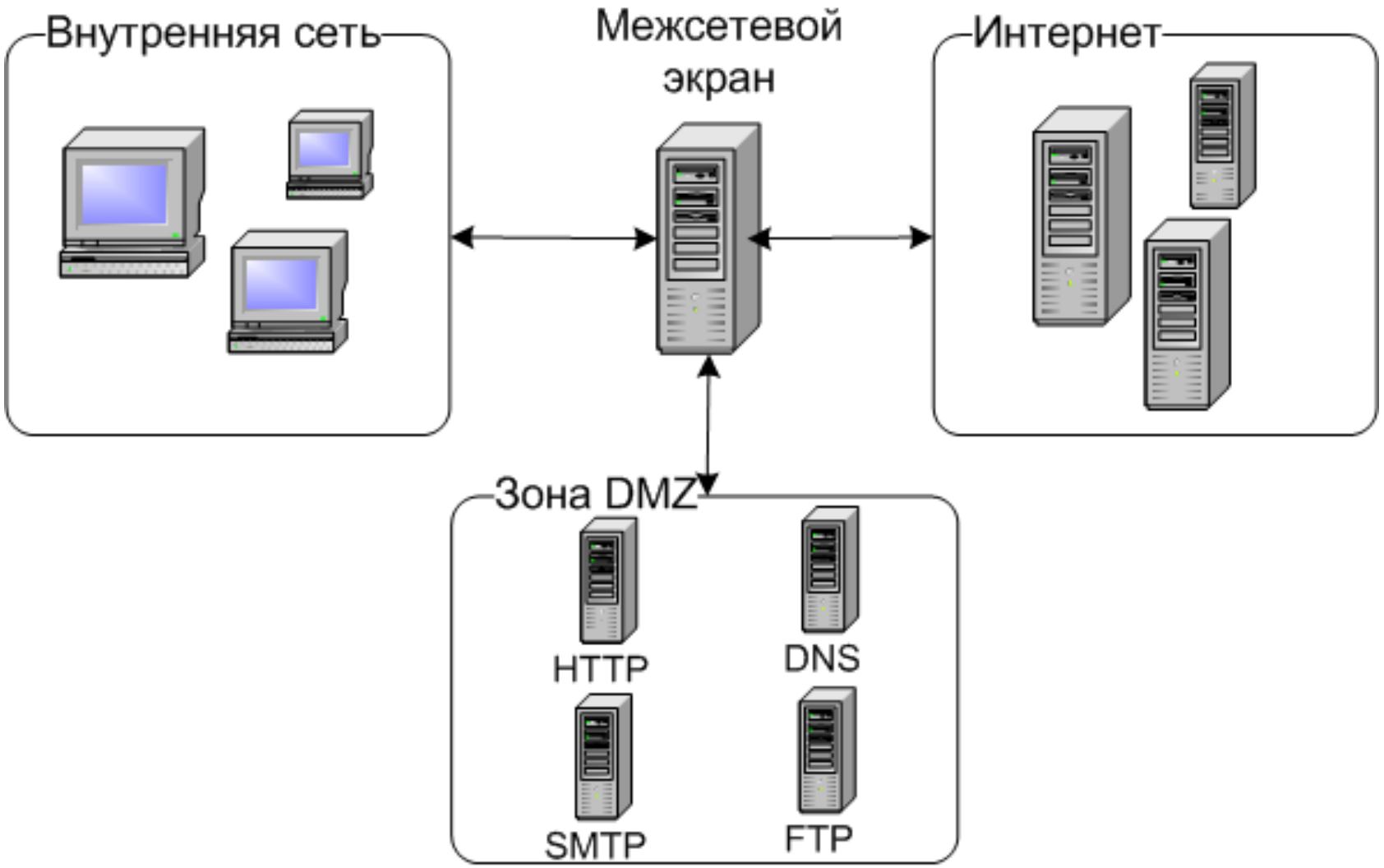
- Защита всей сети
- Учёт всего трафика при принятии решений (поиск аномалий)

Отделение внутренней сети от внешней

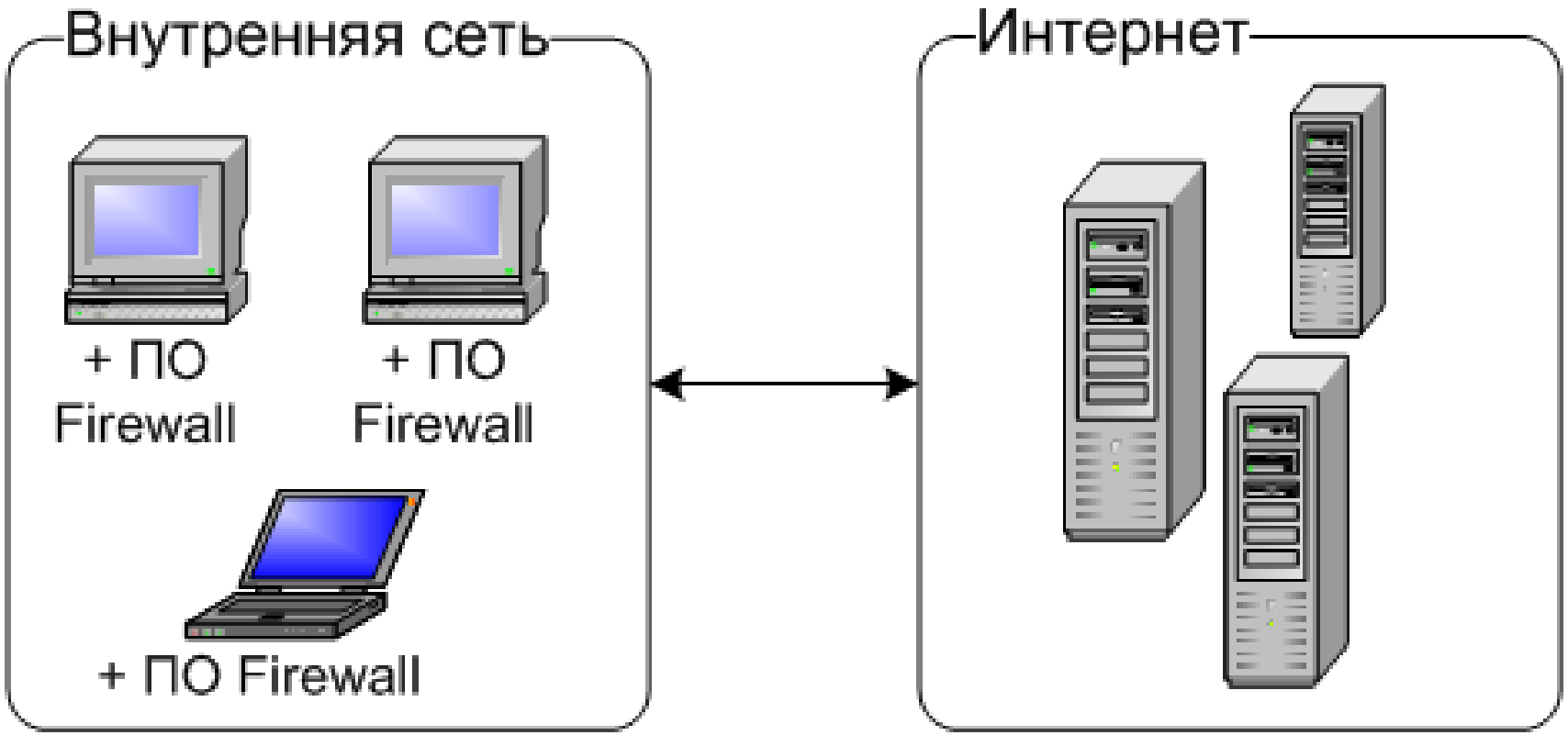
Действия для каждого сообщения:

- Пропустить внутрь или наружу с/без изменений
- Блокировать путём отбрасывания или посылки сообщения об отказе
- Добавление в очередь ожидания

Выделение зоны DMZ



Установка на отдельные хосты



Фильтрация пакетов

Уровни стека TCP/IP

Уровень фильтрации – транспортный.
Используются поля:

- IP-адреса
- транспортный протокол (TCP/UDP)
- порты транспортного уровня
- флаги транспортного уровня (в случае TCP)

Действия: запретить/разрешить пакет + действие по-умолчанию

Пример правила фильтрации: разрешить входящие DNS пакеты только к DNS-серверу (IP A.A.A.A)

1. Разрешить UDP пакеты на 53 порт с IP-адресом A.A.A.A
2. Запретить UDP пакеты на 53 порт с другими IP-адресами

Фильтрация пакетов: преимущества и недостатки

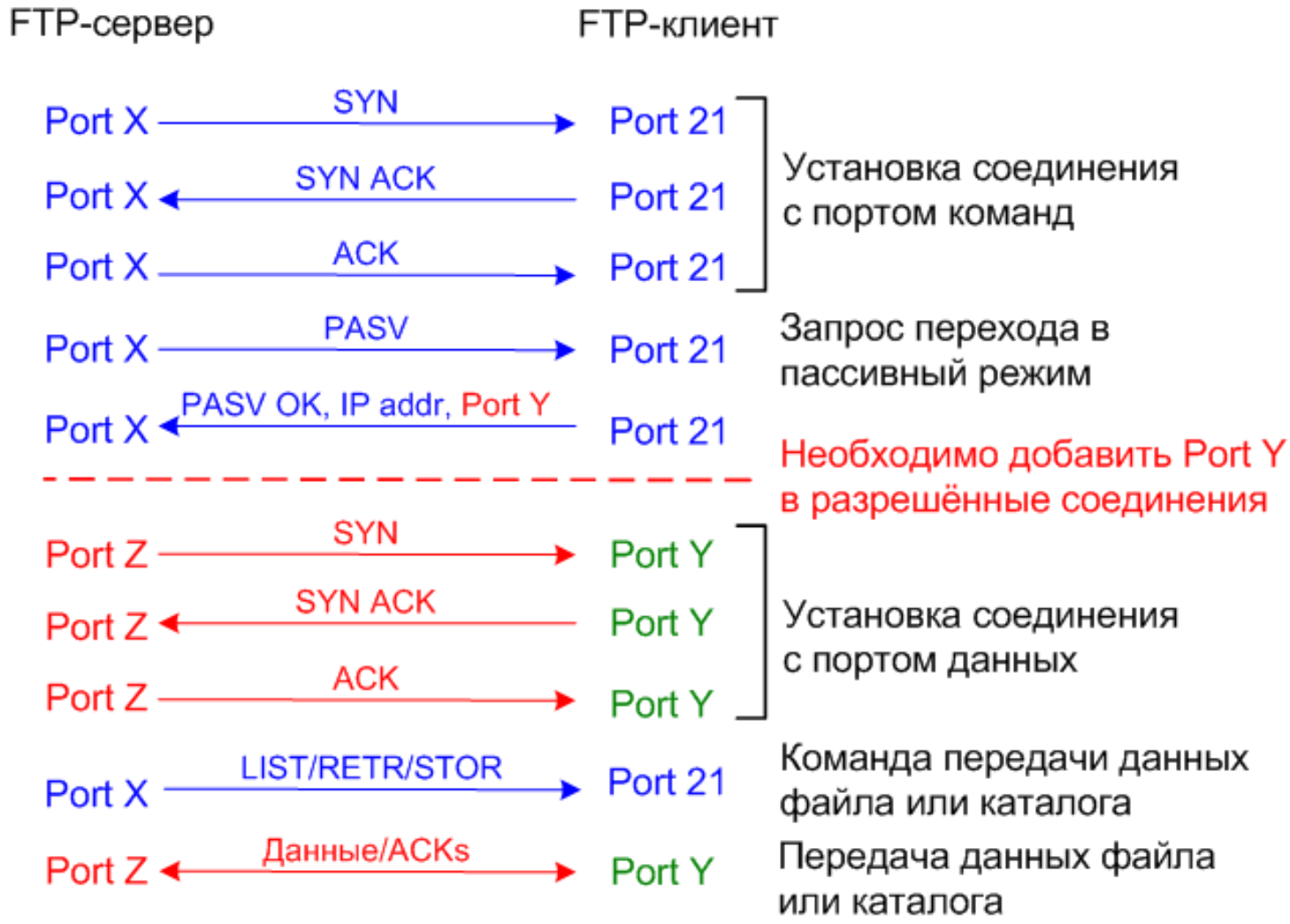
Преимущества:

- Простота правил и скорость работы – просмотр ~64 байт каждого пакета

Недостатки:

- Негибкость – нельзя задать условия на пакеты в рамках потока, например нельзя проверить, что SYN/ACK пакету предшествовал SYN – возможность SYN-flood атаки
- Невозможность работы с динамическими портами (FTP-сервер в пассивном режиме)

Пример. FTP-сервер в пассивном режиме



Учёт состояния

Для каждого открытого соединения сохраняется некоторый набор параметров (состояние).

Преимущества:

- Большая гибкость – отслеживание «рукопожатий», отсутствия пакетов после завершения соединения и т.д.

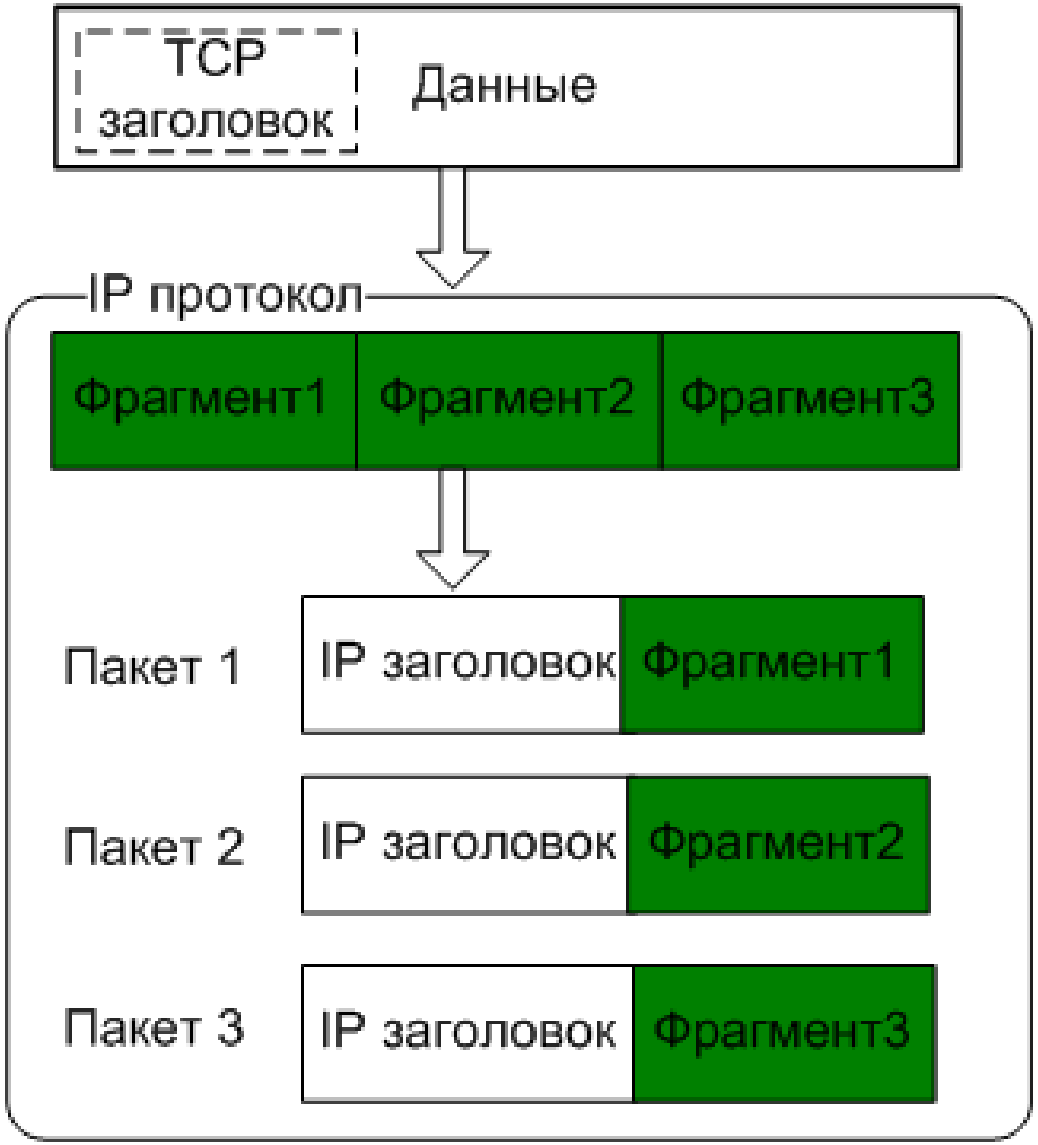
Недостатки:

- Необходимо управлять размером таблицы состояний (защиты от переполнения)
- Возможность атак с применением “уклонения”

IP-фрагментация

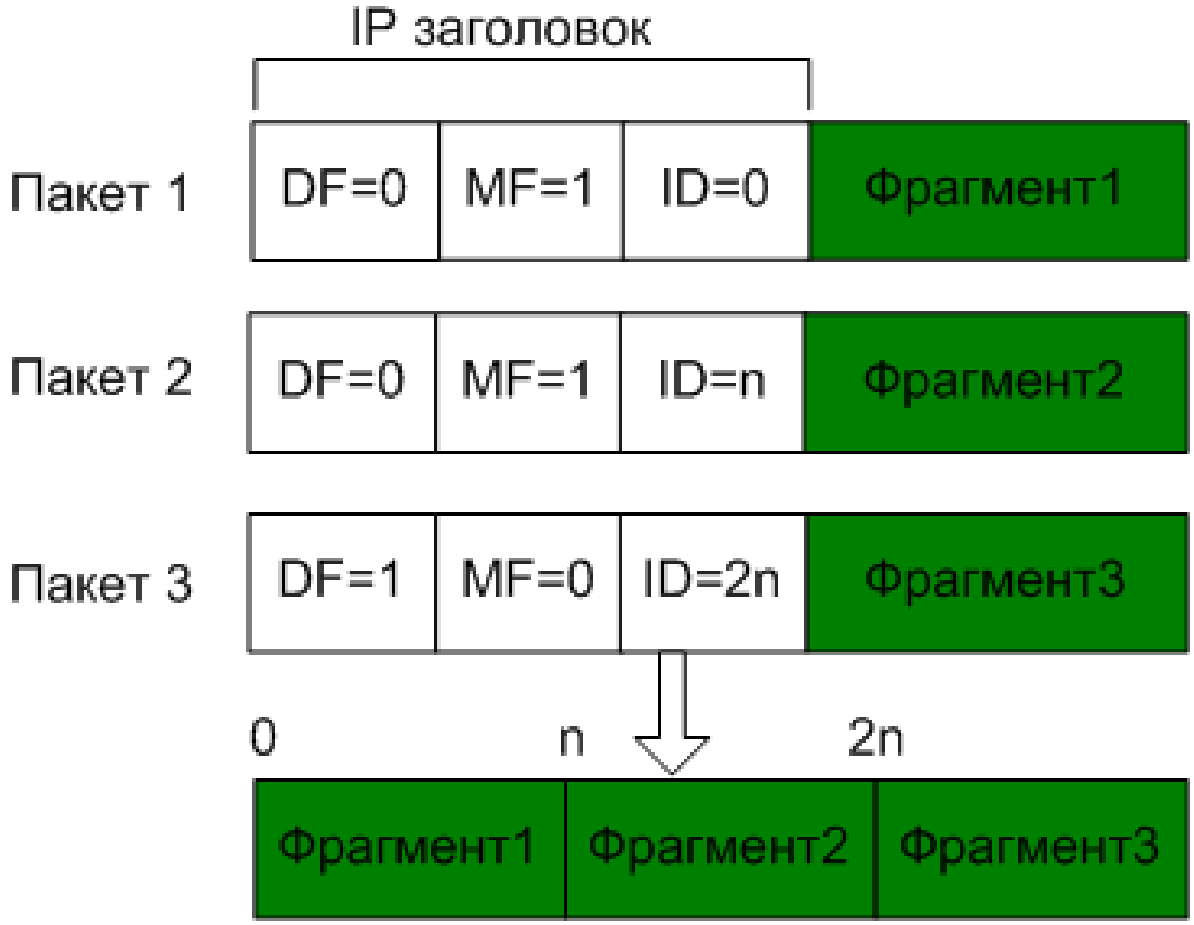
Определение

Разбиение данных полученных от транспортного уровня на IP-пакеты при превышении MTU (maximum translation unit)



Сборка IP-фрагментов

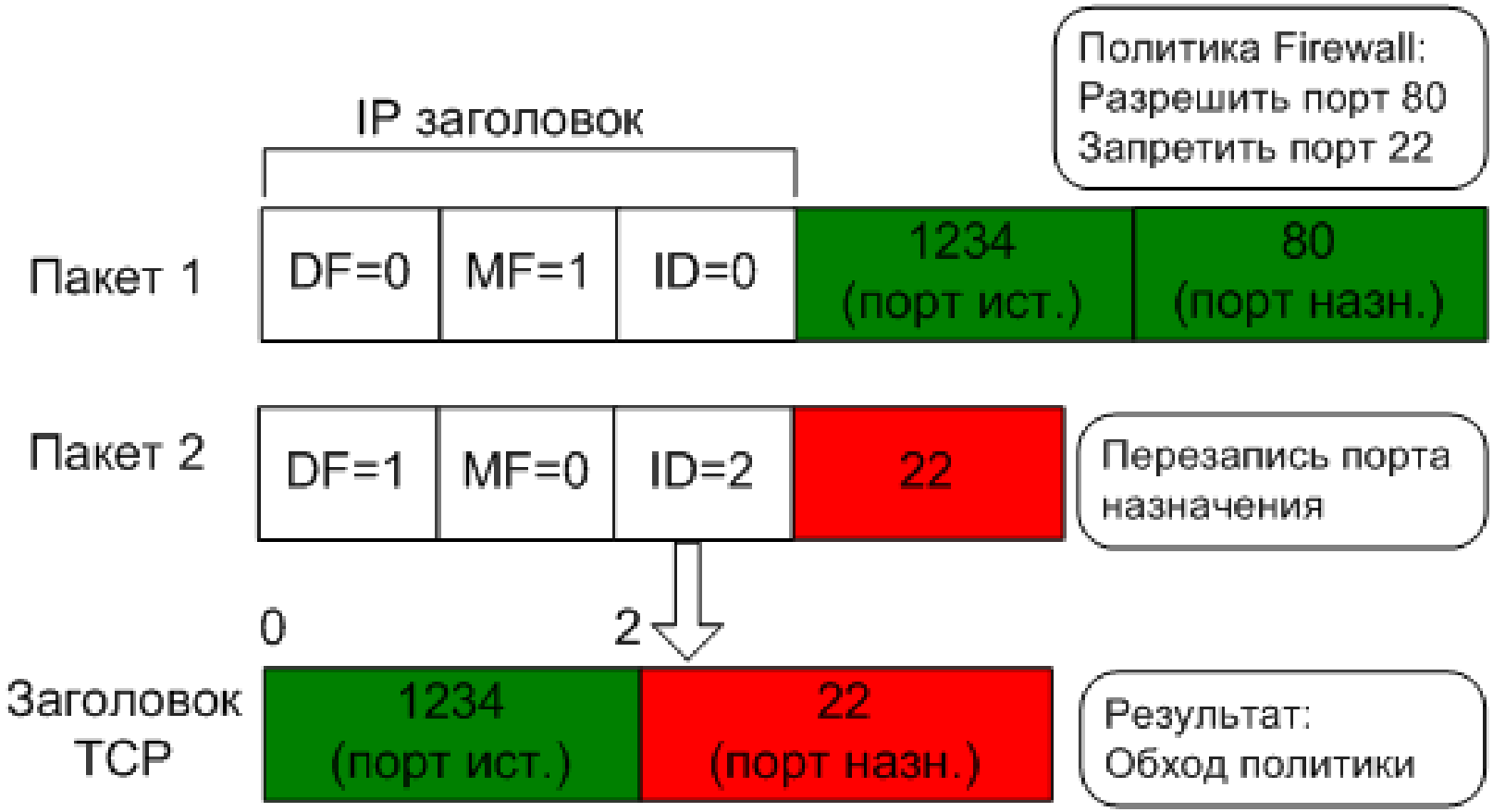
Определение
Сборка пакета транспортного уровня перед передачей транспортному протоколу



DF – не фрагментировать
0 – да, 1 – нет
MF – есть ещё фрагменты
0 - последний,1 - есть ещё
ID – смещение фрагмента

Атака с перекрытием IP-фрагментов

Описание. Перезапись порта назначения в TCP-заголовке при сборке IP-фрагментов



Межсетевые экраны уровня приложения

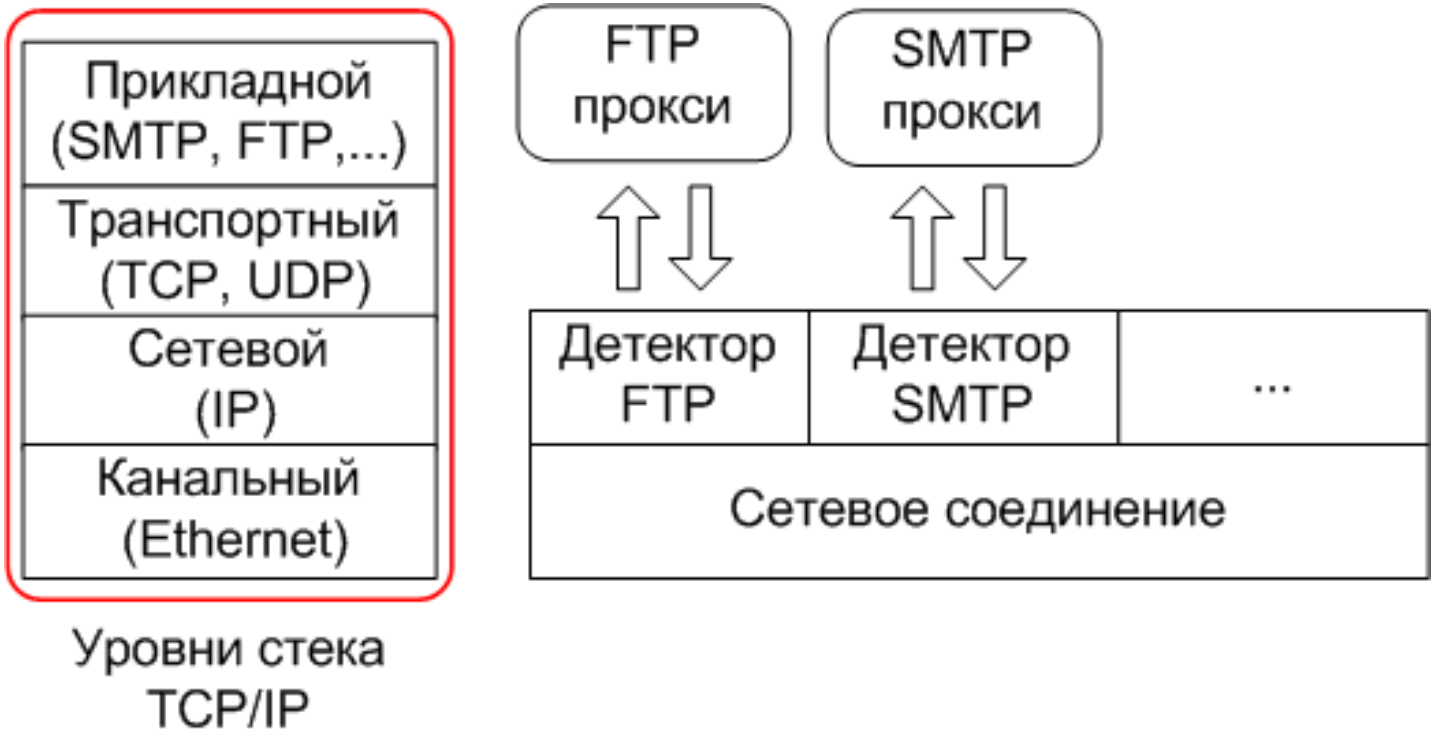
Обрабатывают сообщения уровня приложения

Примеры:

- Сканеры почты и почтовых вложений (SMTP)
- Web-сканеры WAF (HTTP)
- Прокси-серверы (HTTP, FTP, …)

Проксирование отдельных приложений

Алгоритм детектора. Обнаружение нового соединения целевого протокола, создание отдельного прокси для него. Передача следующих пакетов прокси для обработки.



1403

СИСТЕМЫ ЗАЩИТЫ ОТ ВТОРЖЕНИЙ.

Системы обнаружения и предотвращения вторжений

В отличие от межсетевых экранов доступно содержимое сообщения уровня приложения.

Могут анализироваться произвольные приложения.

Два основных подхода:

- На основе правил и политик
- На основе обнаружения аномалий

Критерии оценки:

- Доля ложных срабатываний
- Доля обнаруженных атак

Системы на основе политик

Используют заранее заданные правила.

Основные формы правил:

- Регулярные выражения (Snort)
- Криптографический хеш (tripwire, snort)

Пример правил Snort:

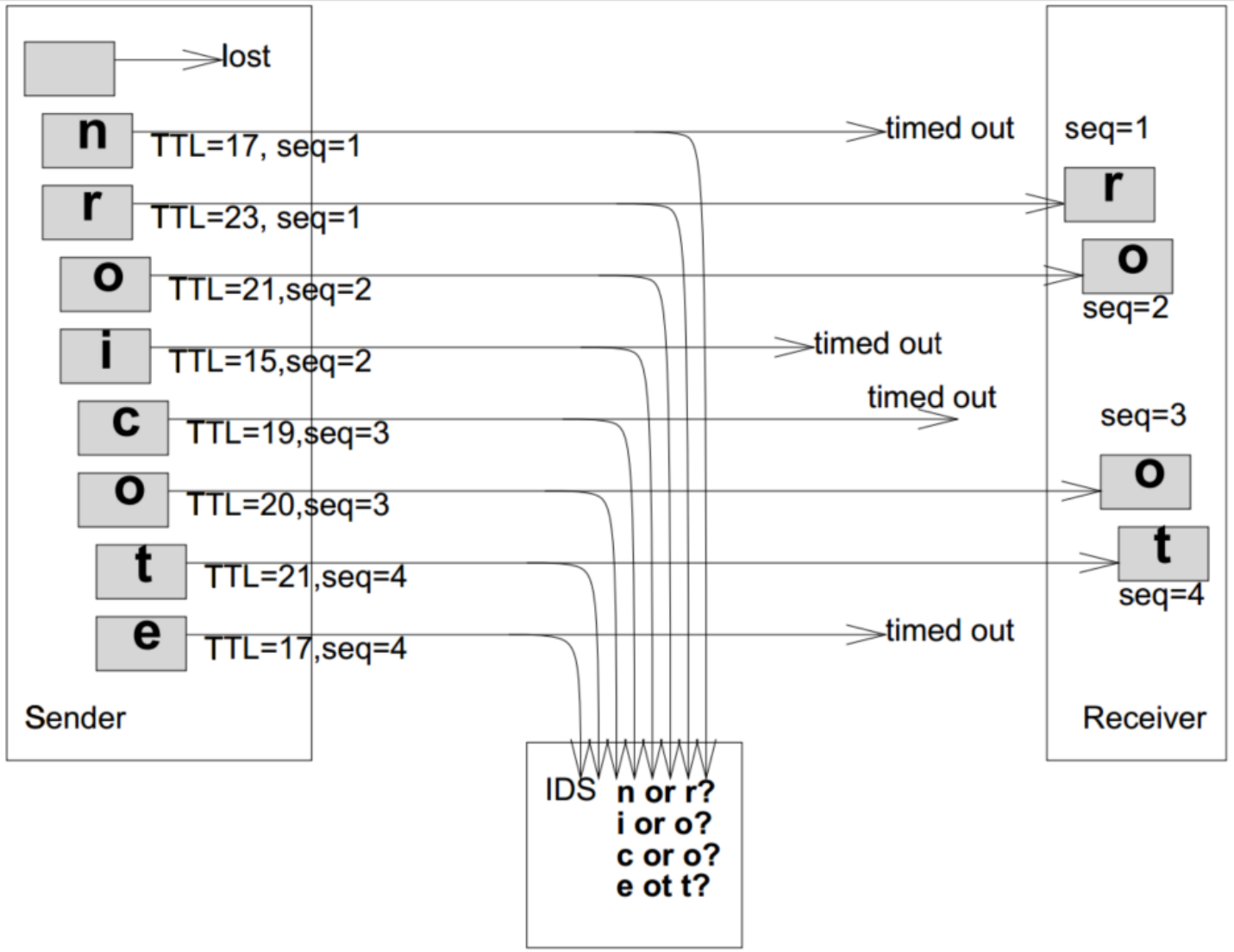
Detect any fragments less than 256 bytes

```
alert tcp any any -> any any (minfrag: 256; msg:
  "Tiny fragments detected, possible hostile activity";)
```

Detect IMAP buffer overflow

```
alert tcp any any -> 192.168.1.0/24 143 (
  content: "|90C8 C0FF FFFF|/bin/sh";
  msg: "IMAP buffer overflow!";)
```

Атака с перекрытием TCP-сегментов

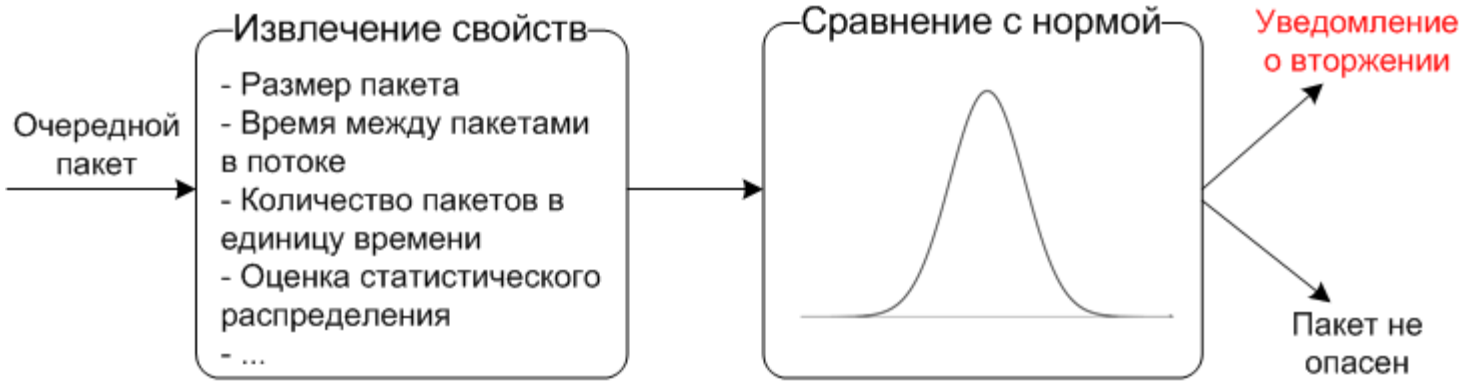


Системы на основе аномалий

Две стадии:

1.Обучение на рабочем множестве, не содержащем атак, описание области «нормы»

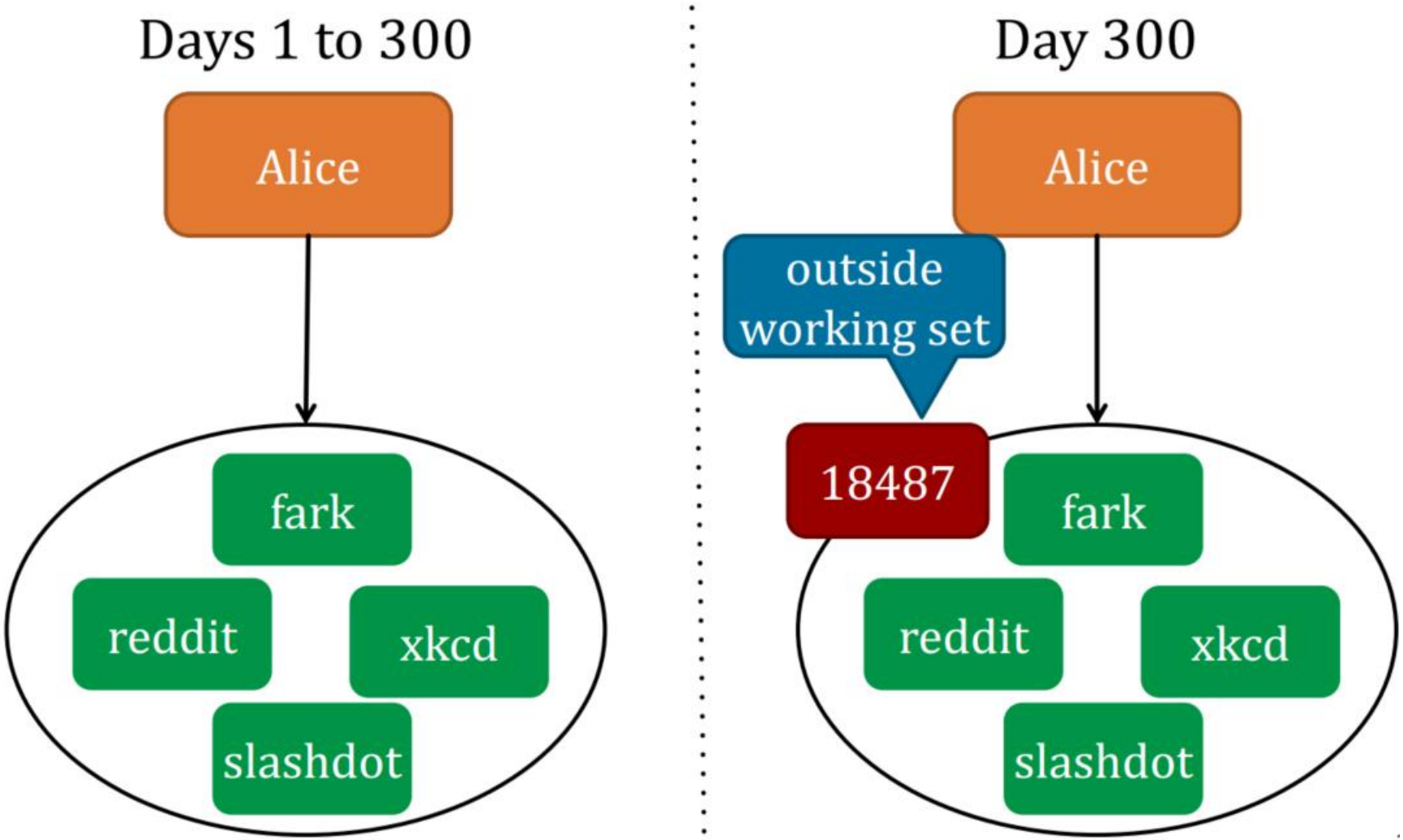
2. Работа на реальном сетевом трафике



Преимущества – возможность обнаружения ранее неизвестных атак, не нужно задавать правила

Недостатки – сложность обучения, более высокий уровень ложных срабатываний

Аномалии на основе рабочего множества



Литература к лекции

Основные источники

1. M. Roesch. Snort - lightweight intrusion detection for networks, in Proceedings of LISA99, the 13th Systems Administration Conference. 1999.
2. M. Handley, V. Paxson. Network Intrusion Detection: Evasion Traffic Normalization And End-to-End Protocol Semantics, 2001
3. T.H.Ptacek, T.N. Newsham. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, 1998