

Моделирование DDoS-атак на облачные вычислительные среды

**Борисенко Константин Алексеевич, аспирант
Шоров Андрей Владимирович, к.т.н., ведущий научный сотрудник**

**Санкт-Петербургский государственный
электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) (СПбГЭТУ «ЛЭТИ»)**

Что такое Cloud?



Минусы:

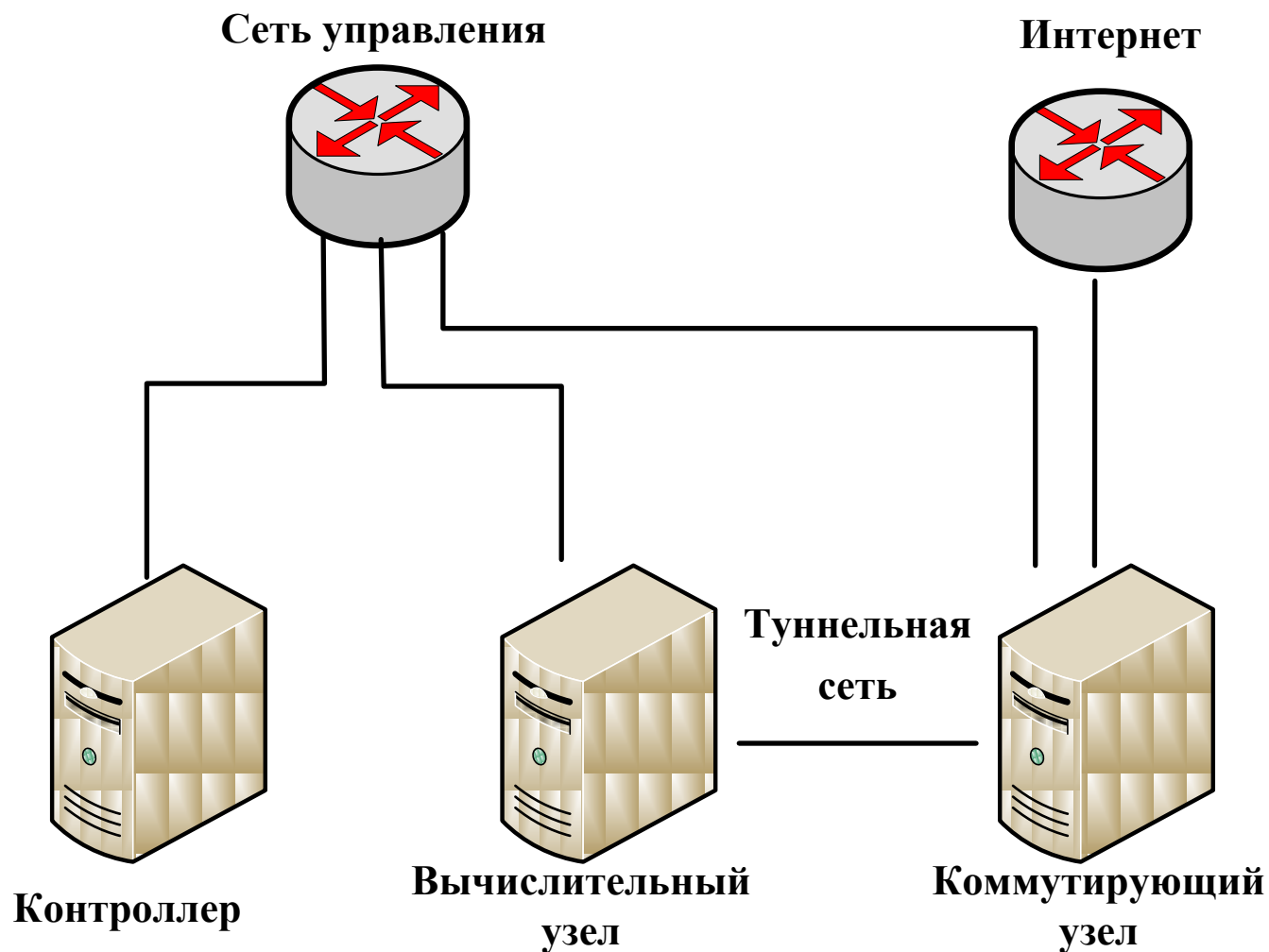
- Сервисы обслуживаются без вашего участия.
- Сложность сетевой инфраструктуры.

Плюсы:

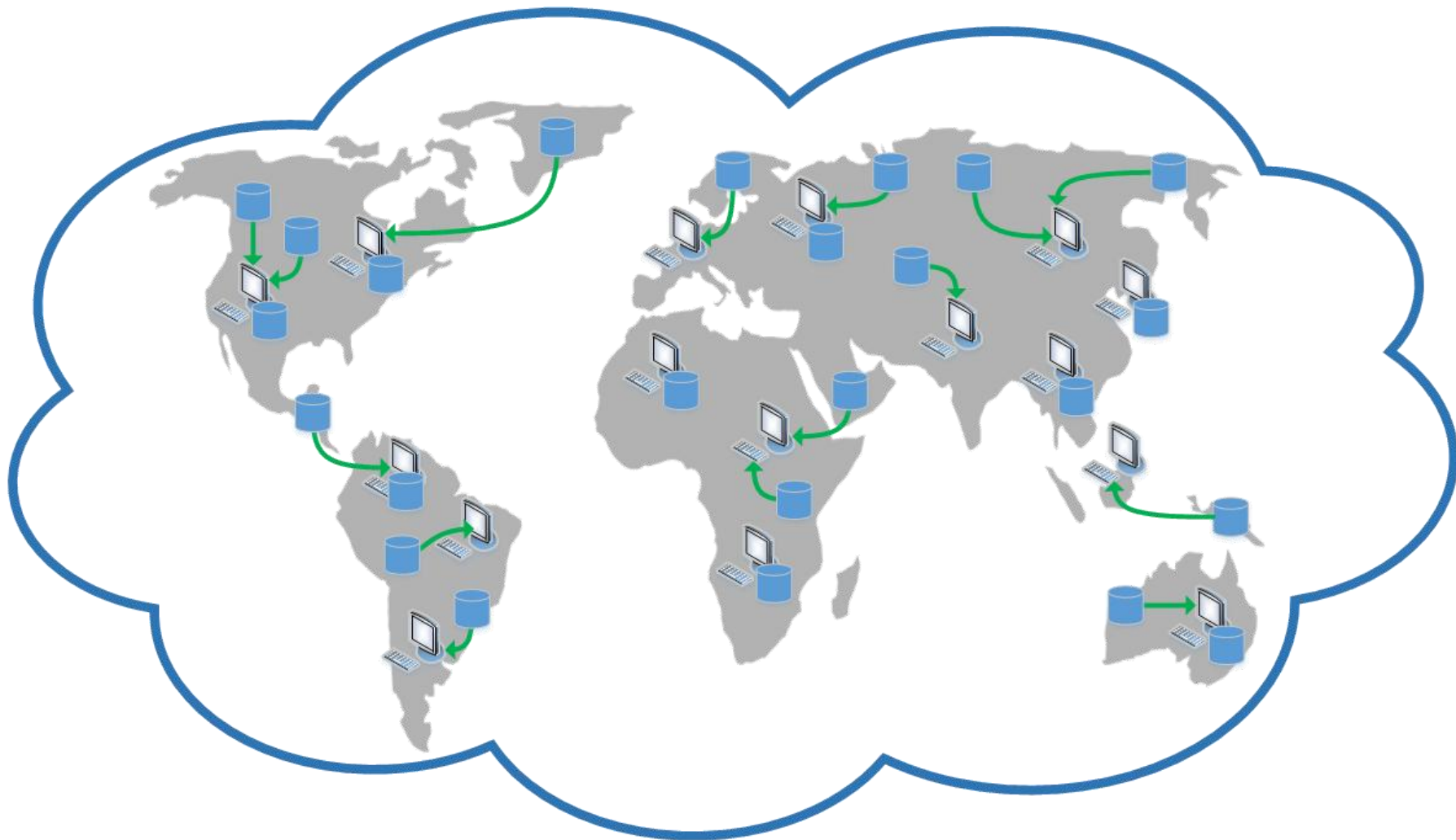
- Сервисы обслуживаются без вашего участия.
- Громадные запасы мощностей, доступные моментально.
- Доступ из любого места.



Обобщенная архитектура Cloud



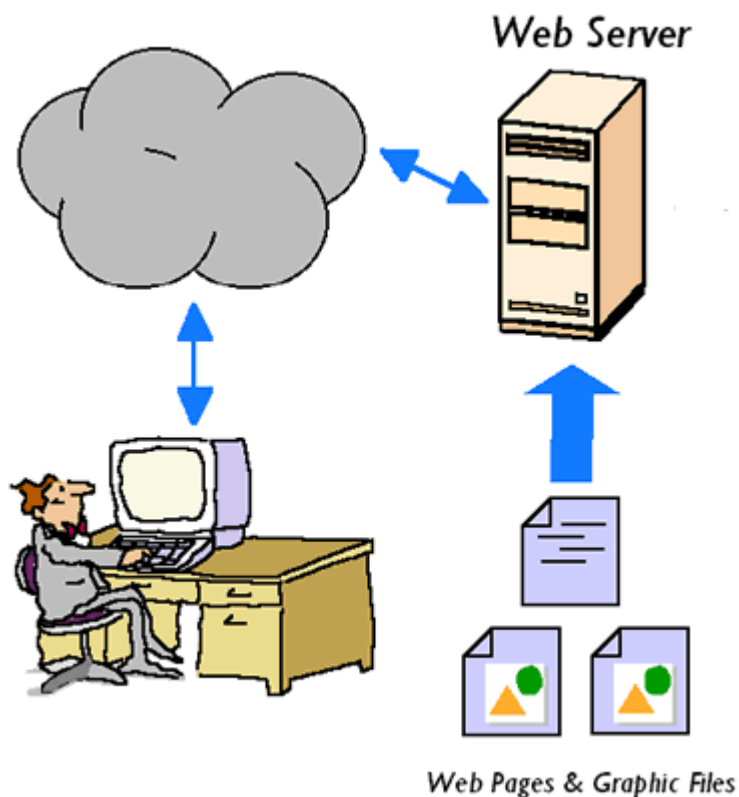
Распределенный Cloud



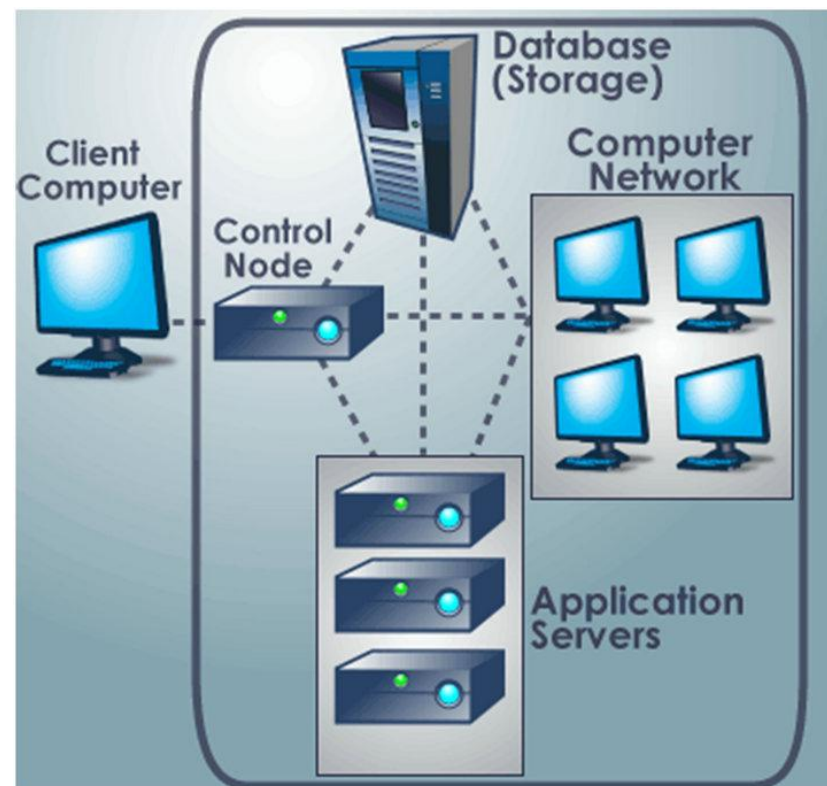
Сложность сетевой инфраструктуры (1/2)



Обычный веб-сервер



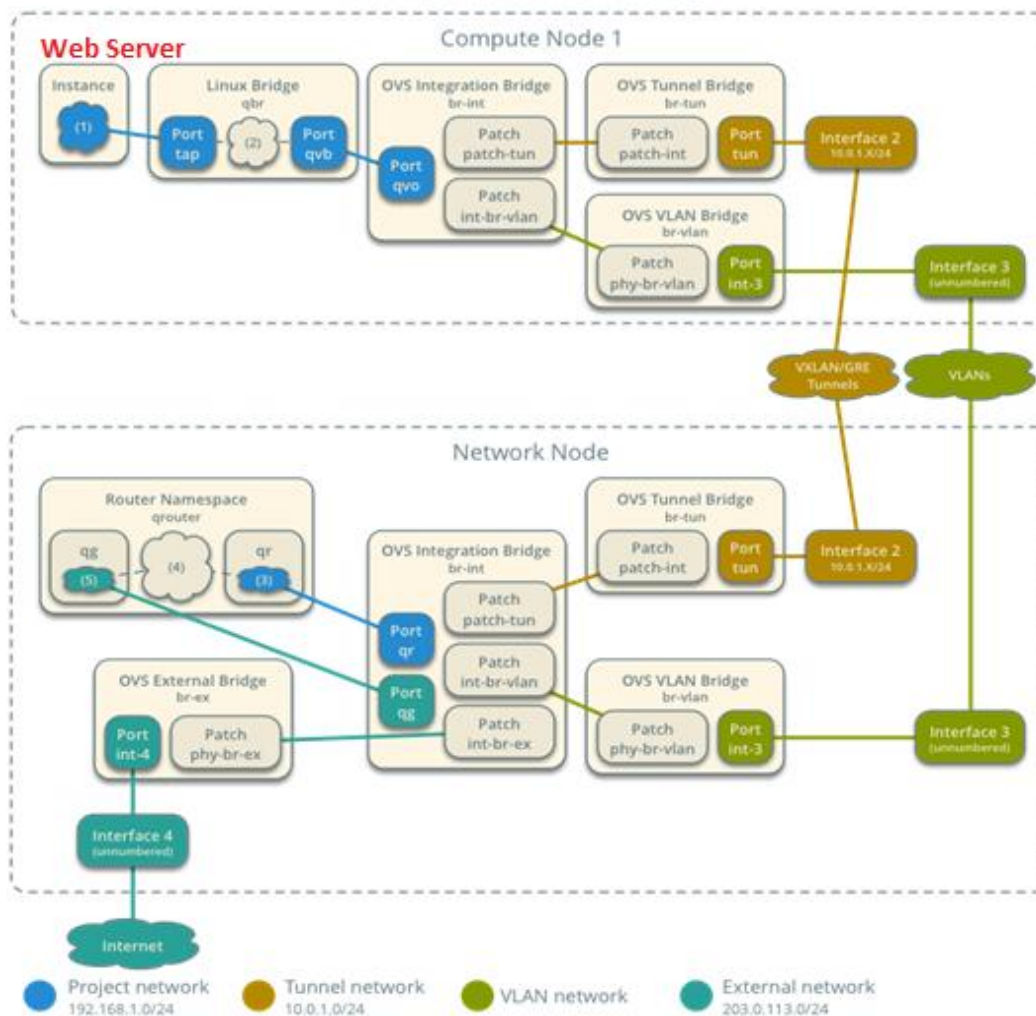
Облачная вычислительная среда



Сложность сетевой инфраструктуры (2/2)



Network Traffic Flow - North/South
Instances with a fixed IP address





Моделирование процессов безопасности в компьютерных сетях

Типы DDoS-атак



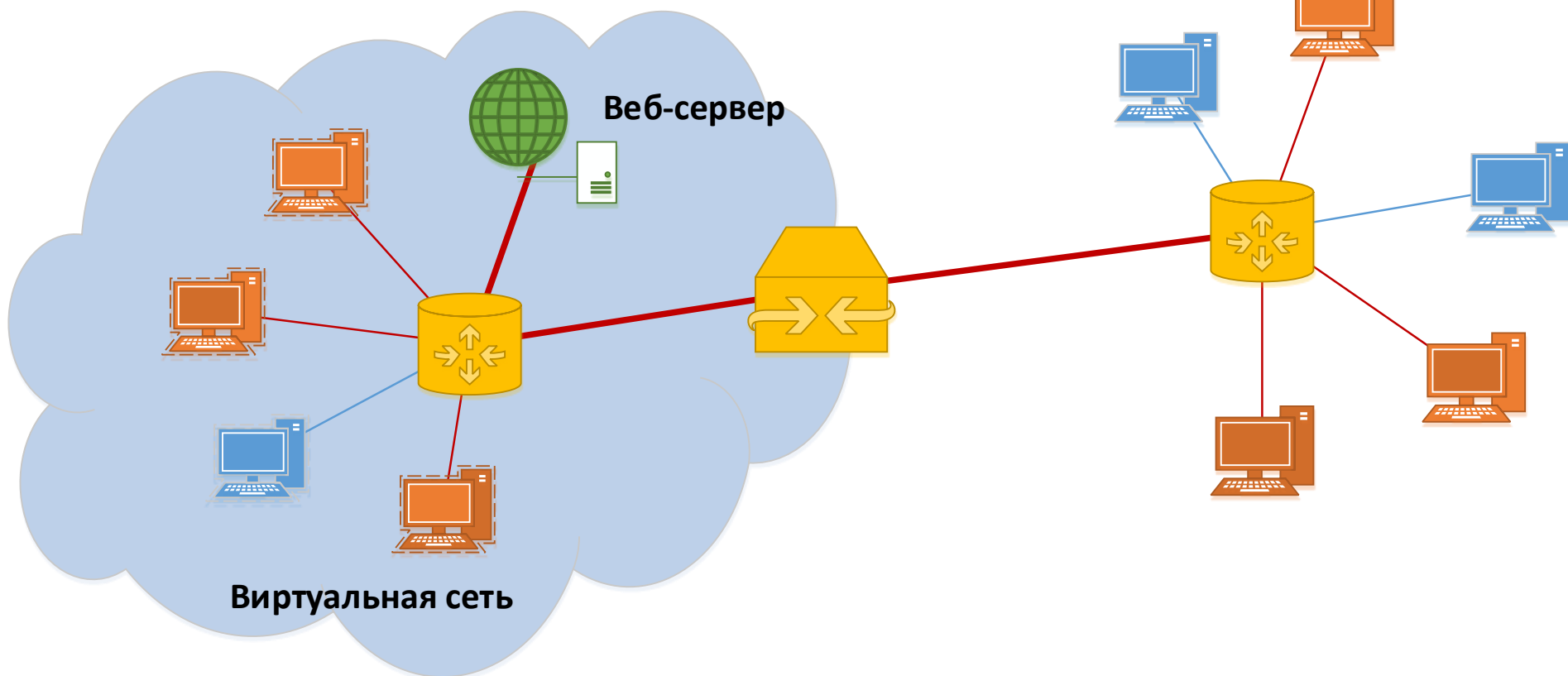
- TCP Flooding (SYN, SYN-ACK, ACK, RST);
- UDP Flooding;
- SMURF;
- HTTP Flooding;
- NTP monlist;
- ECHO;
- Chargen.

DDoS-атаки на Cloud



Облачная вычислительная среда

Внешняя сеть

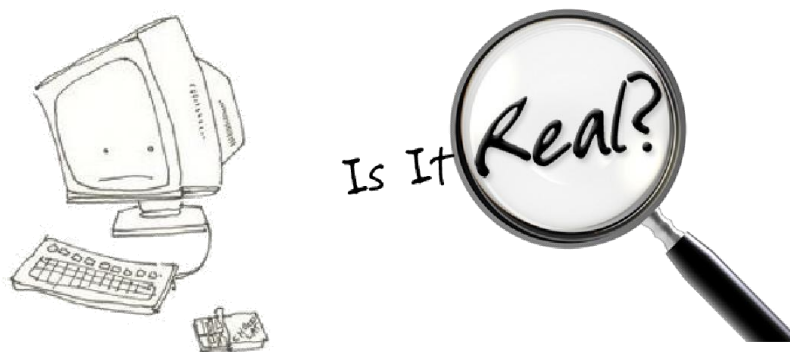


Пути решения

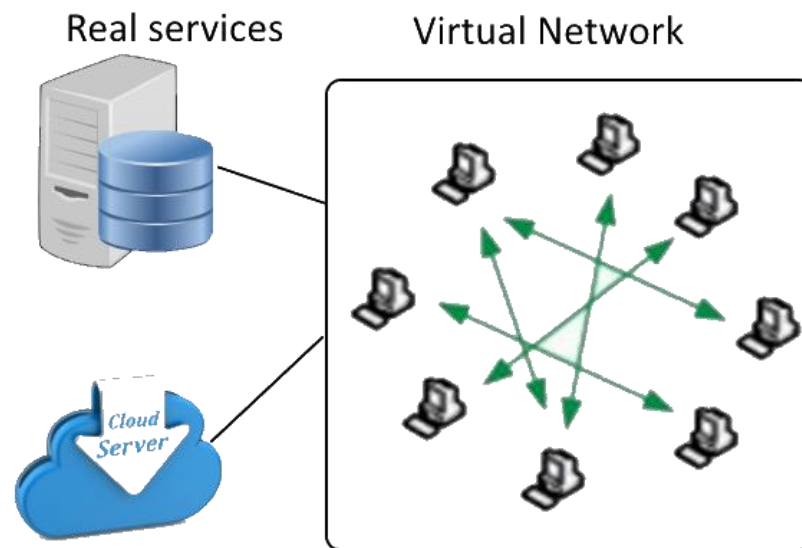
Реальные лаборатории



Имитационное моделирование



Наш подход

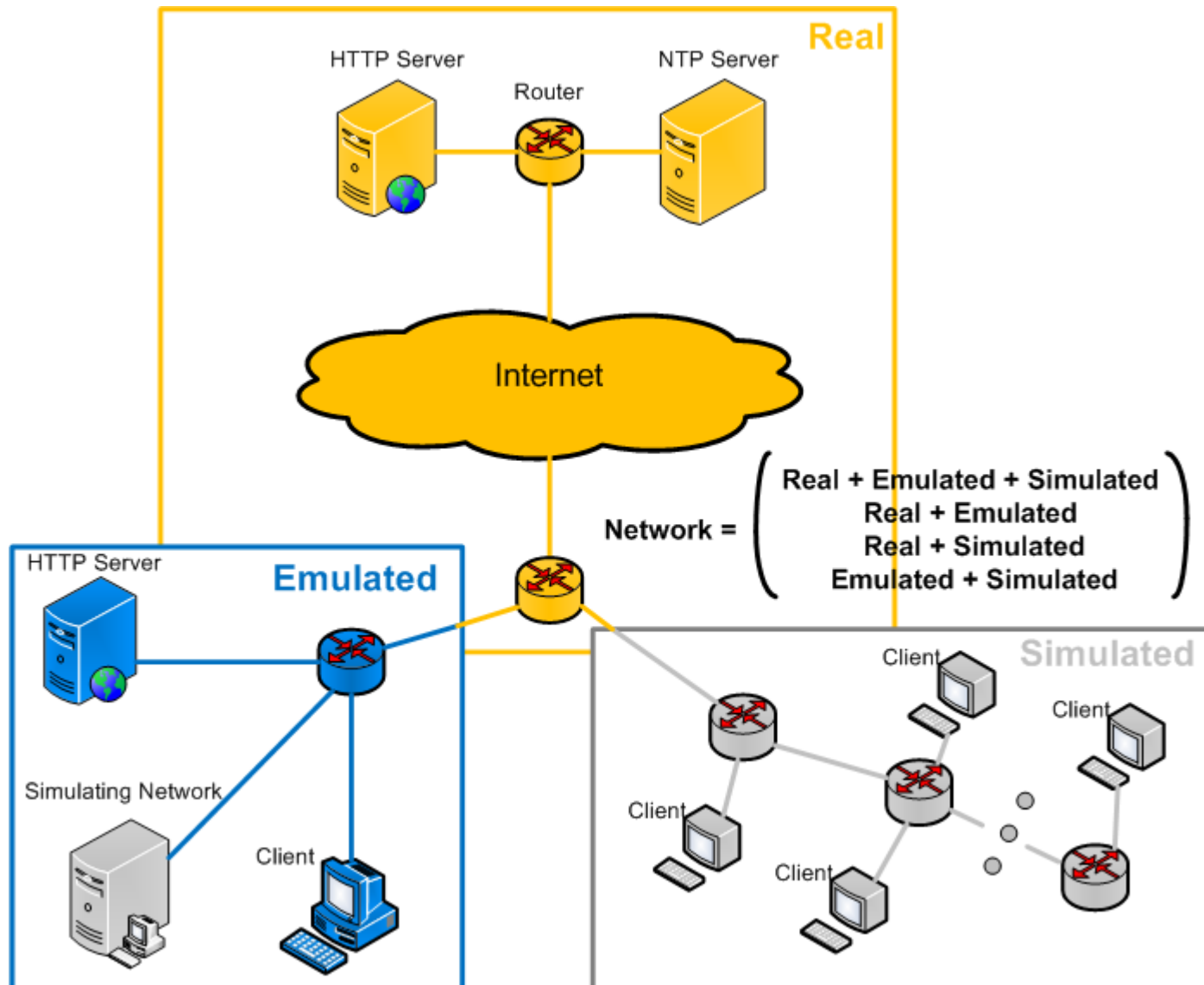


Функционал системы



- Генерация топологий.
- Настройки сценариев поведения клиентов:
 - Используя уже существующие типы атак и защит.
 - Создание новых.
- Подключение к реальным сетям.
- Логирование трафика, окраска пакетов, отладка.

Точки встраивания виртуальной сети



Интерфейс системы моделирования



The screenshot displays the OMNeT++/Tkenv - Inet simulation environment. The main window shows a network diagram with a central router (Inet.sas9) connected to multiple hosts (Inet.sas0 to Inet.sas9). The hosts are connected to a central router (Inet.sas9) which is connected to a central router (Inet.sas9). The hosts are connected to a central router (Inet.sas9) which is connected to a central router (Inet.sas9).

The interface includes several panels:

- Top Panel:** Simulation controls and statistics. It shows the current time (T=49.206128489093), the number of messages scheduled (5124), created (635205), and present (54666). It also displays the number of events per second (n/a) and the number of messages per second (n/a).
- Left Panel:** A tree view of the simulation components, including Inet (Inet), connection, trafficProfile, and various hosts (sas0 to sas9).
- Right Panel:** A detailed view of the Inet.sas9 host, showing its internal components such as notificationBoard, tcpApp, udpApp, and pingApp. It also displays statistics for the host, including the number of packets received (0) and sent (23).
- Bottom Left Panel:** A graph showing the output of the simulation. The x-axis represents time (t) and the y-axis represents a value (value). The graph shows a sharp increase in the value at the end of the simulation.
- Bottom Right Panel:** A table showing the contents of the simulation. It lists 15 objects and their fields, including address, port, connectAddress, connectPort, victimAddress, victimPort, udpEmitterAppNa, and tcpIn.

Алгоритм работы



- Создание топологии.
- Подключение реального сервиса.
- Выбор и настройка сценария атаки.
- Настройки параметров защитных механизмов.
- Настройки точек сбора трафика и параметров сбора.
- Настройки параметров симуляции.
- Проведение эксперимента.
- Анализ результатов.

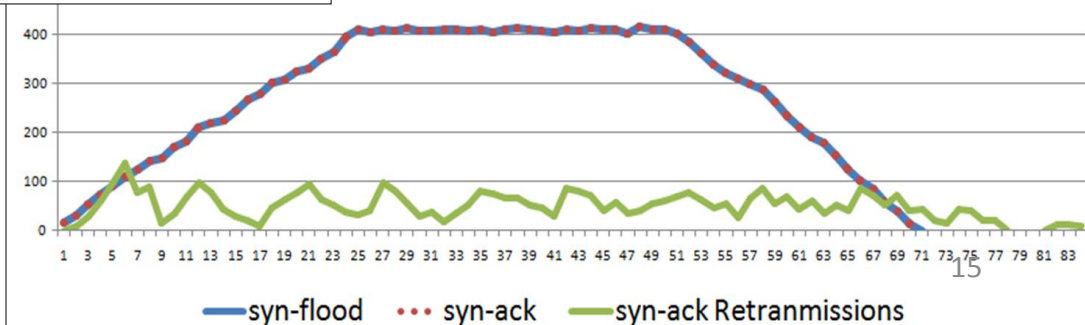
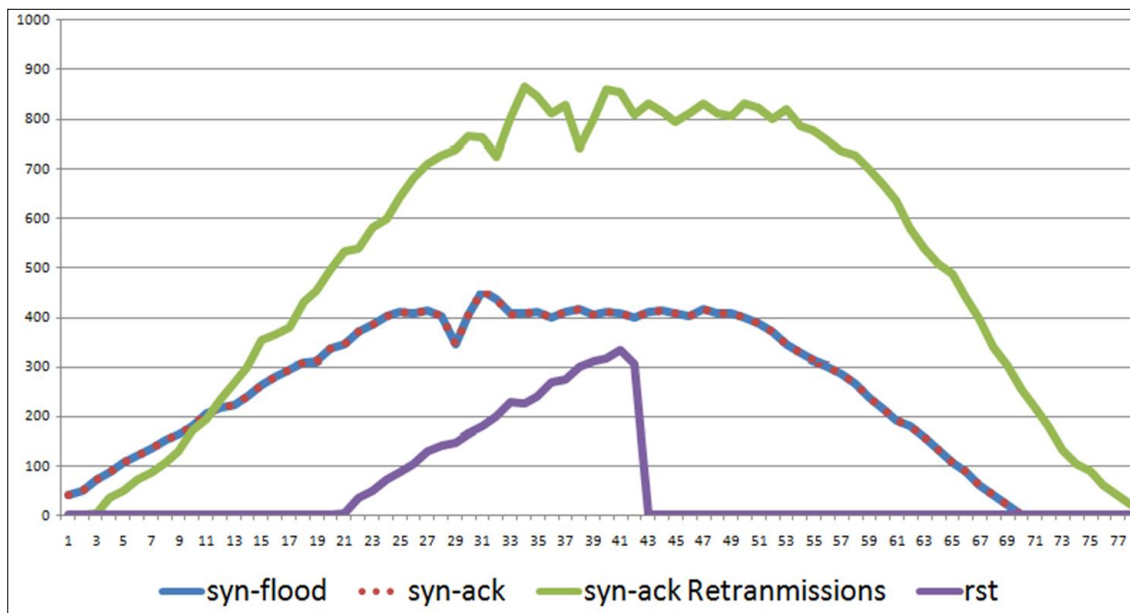
Преимущества использования реальных сервисов-жертв



Windows
Server

VS

Ubuntu
14.04





Моделирование распределенных атак типа «отказ в обслуживании» (DDoS-атак)



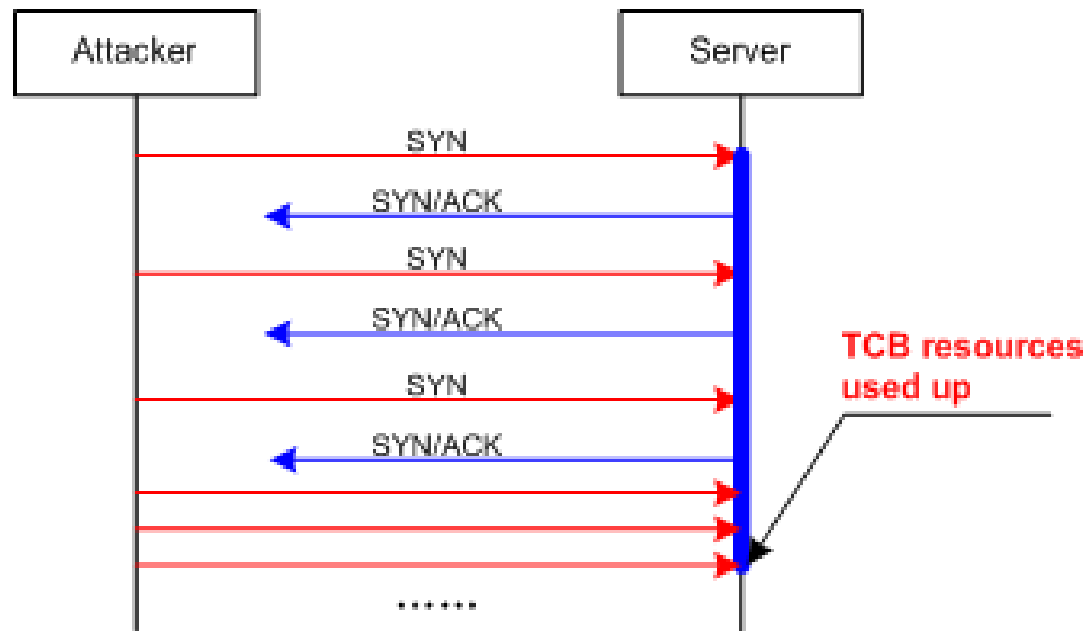
Параметры атак

- Путь к сервису-жертве.
- Тип атаки.
- Мощность атаки.
- Порт источника и назначения.
- Время начала и конца атаки.
- Задержка между пакетами/сессиями.
- Количество пакетов за эксперимент.
- Особые настройки для разных типов атак.

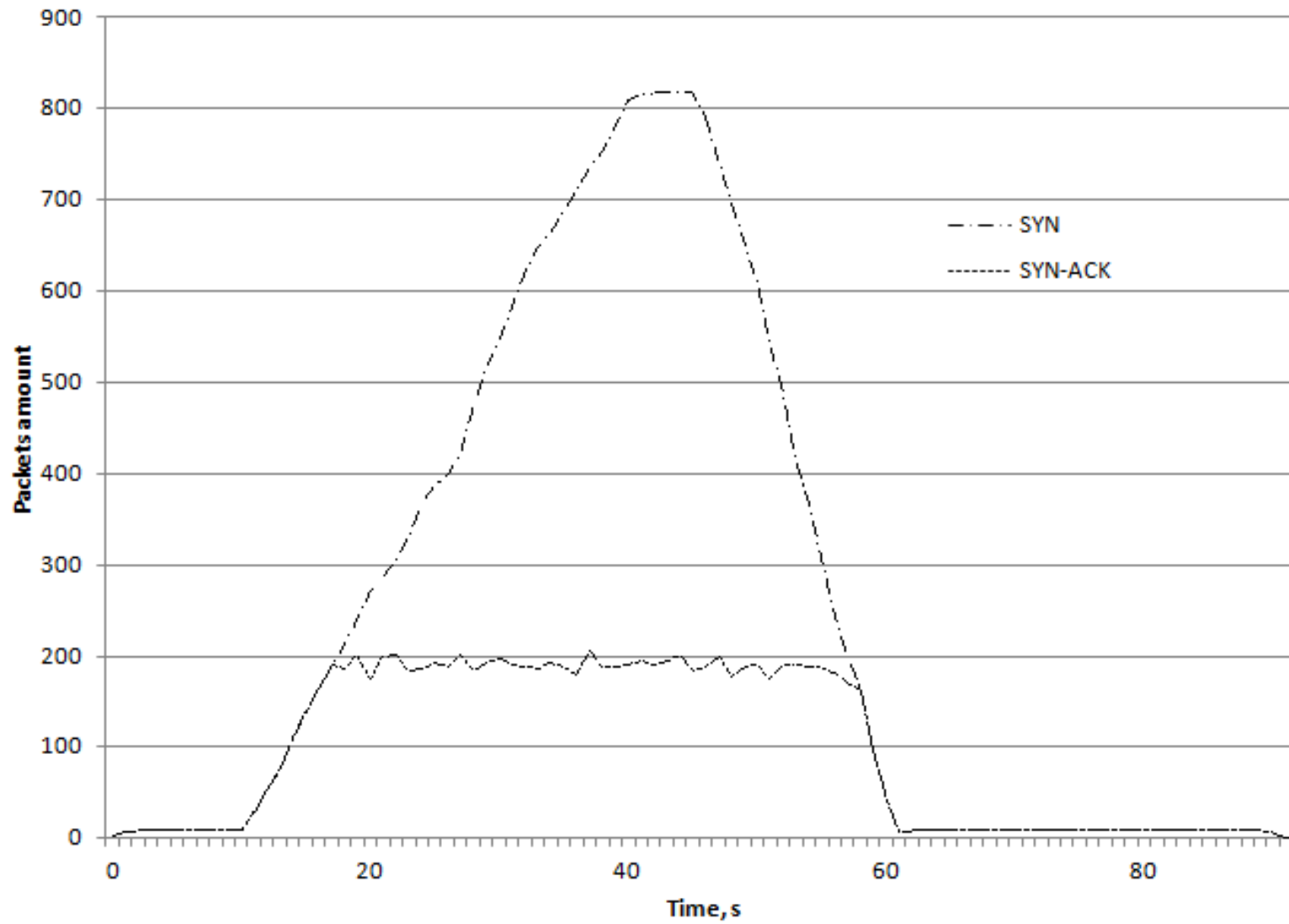


SYN Flooding

- Серия из 10 экспериментов.
- 200 клиентов в топологии.
- Задержка между пакетами 500 мс.
- SYN cookies были отключены.

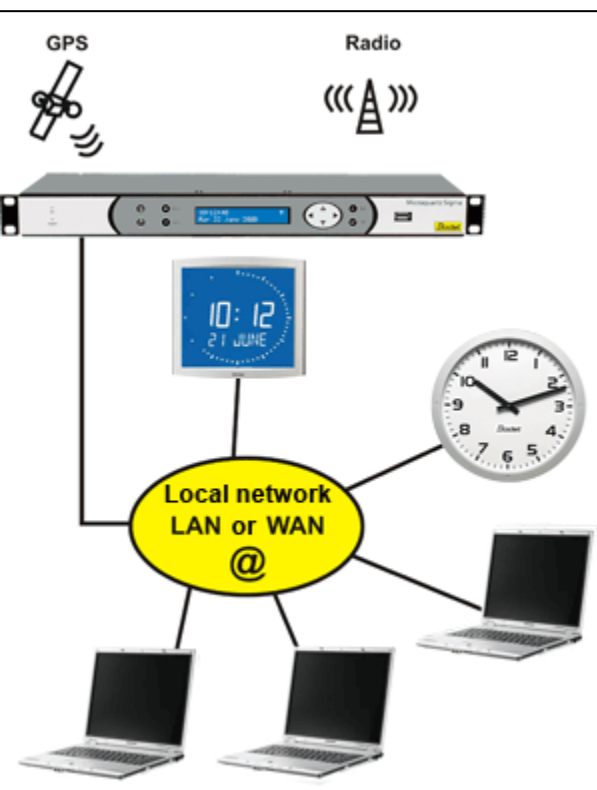


SYN Flooding

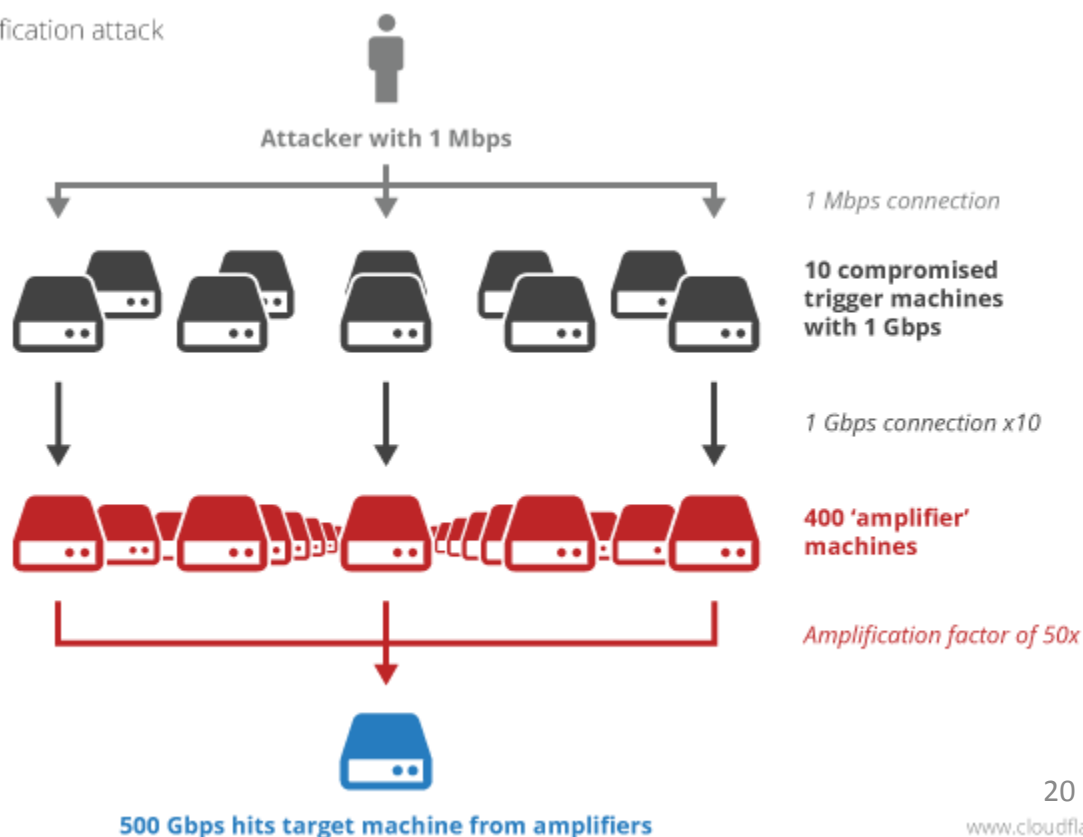


NTP-атака

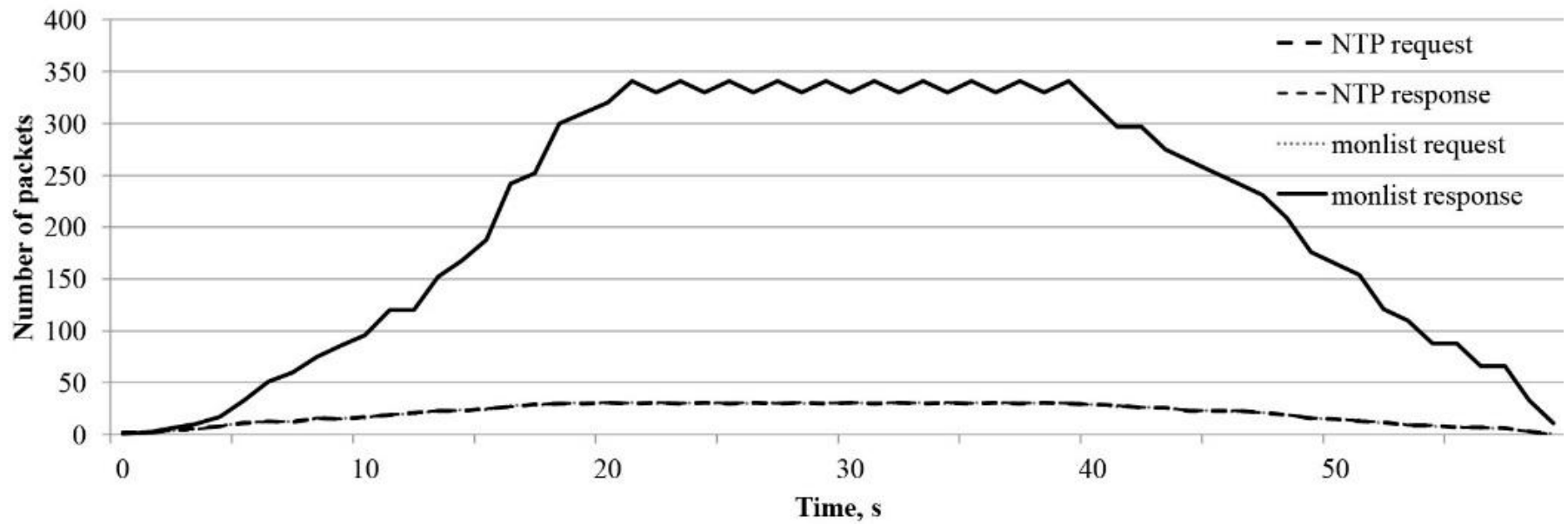
- 106 клиентов. Уязвимость get_monlist.
- Задержка между пакетами – 500 мс.
- Старт 1-20 сек, конец 40-60 сек.



Amplification attack



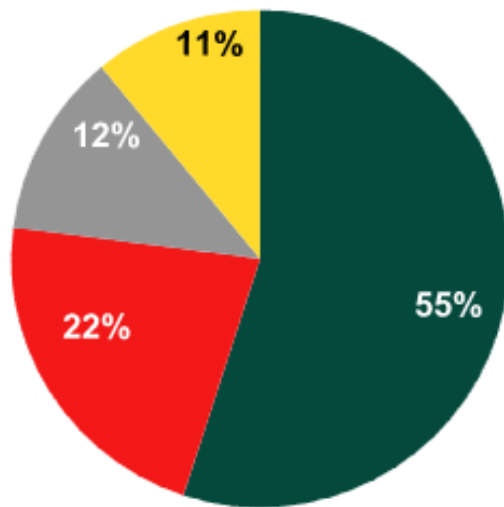
NTP-атака



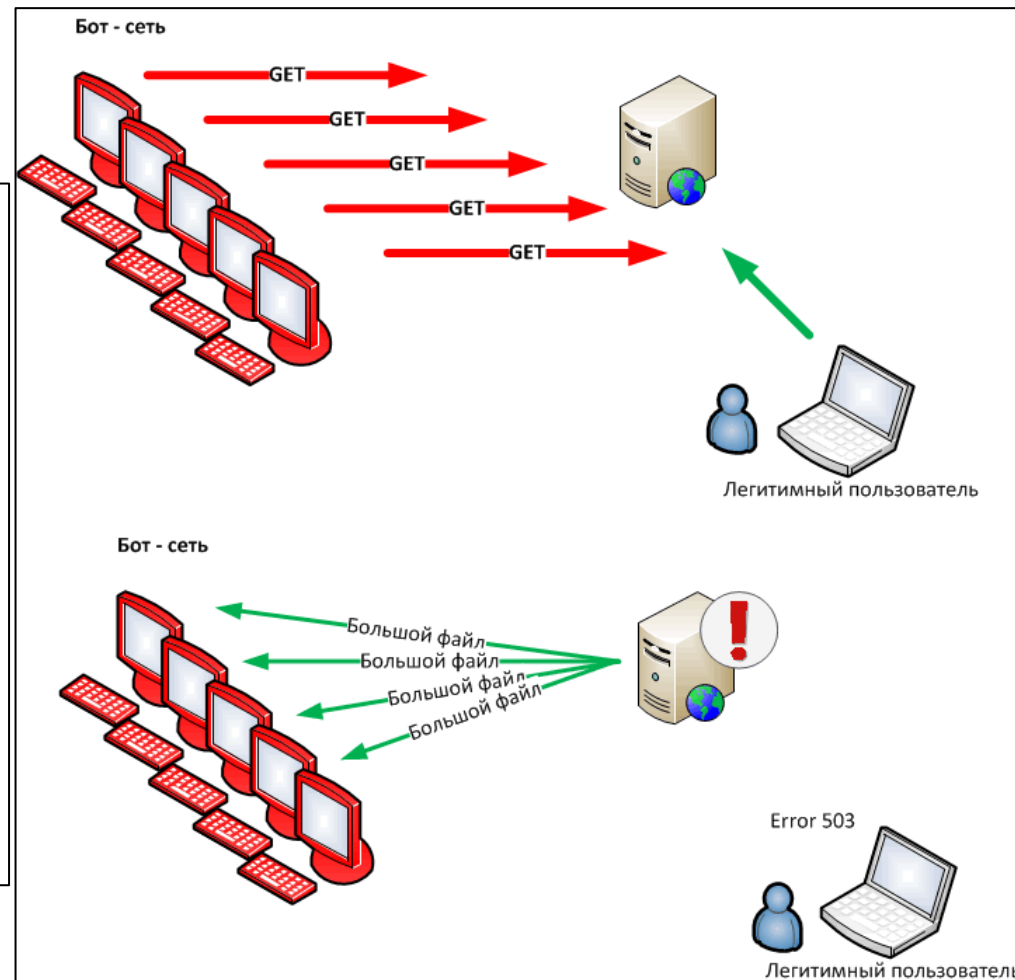


HTTP-атака

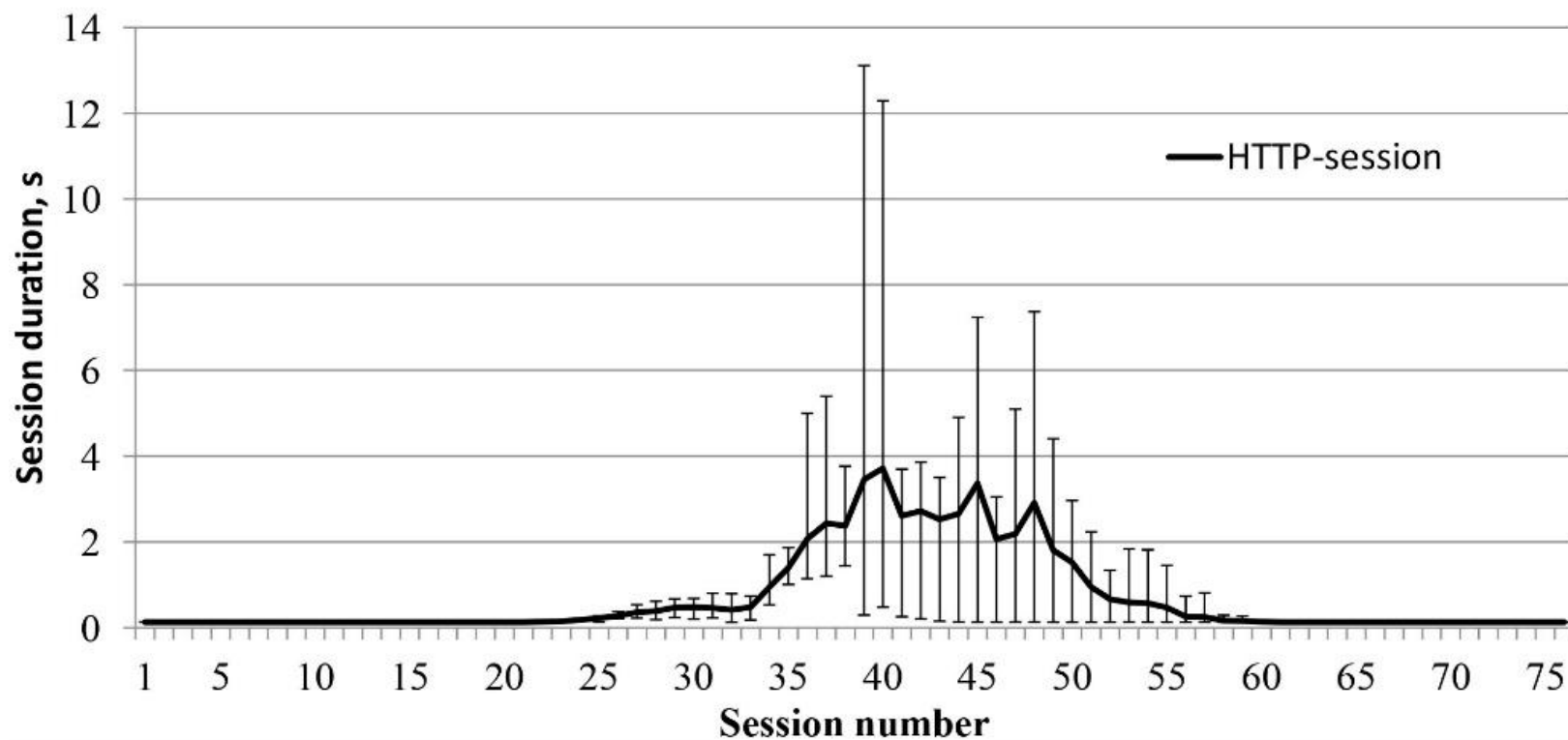
- Sending GET requests;
- 200 clients;



- запрос главной страницы или одной страницы
- атака на формы авторизации или поиска
- download флуд
- атака с попыткой эмуляции действий пользователя



HTTP-атака



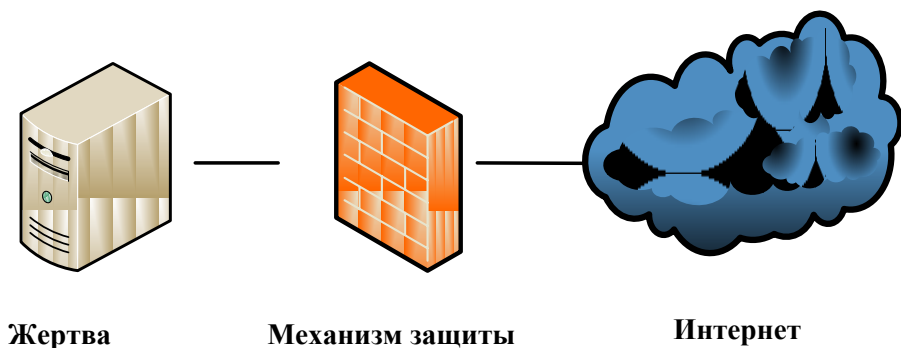


Методы защиты от DDoS-атак

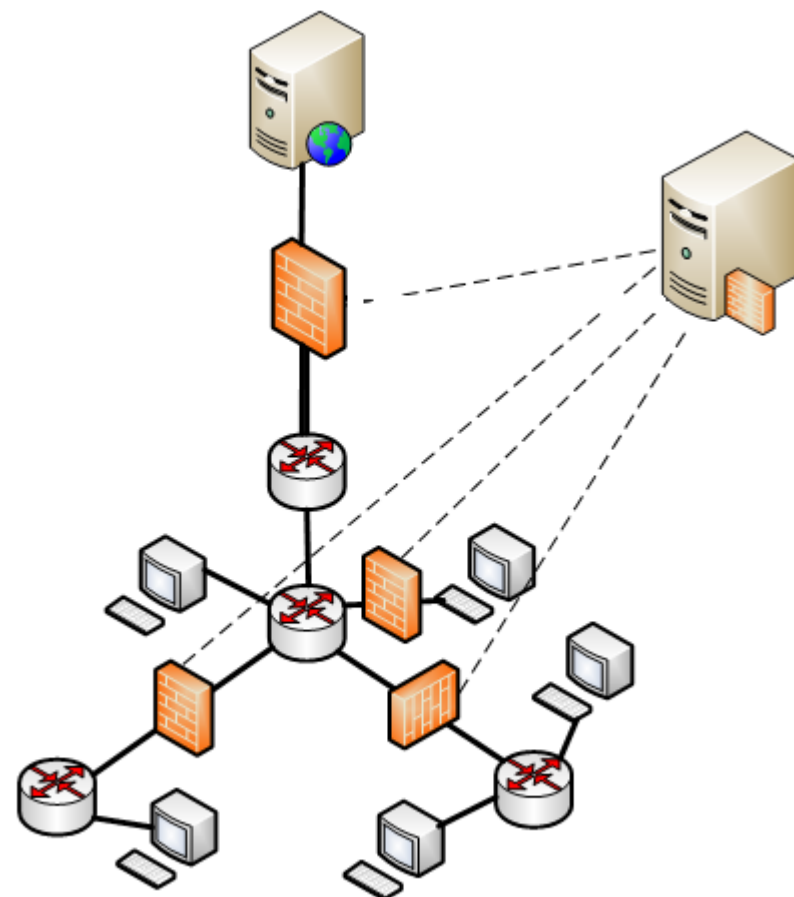
Распределенные механизмы защиты



Обычные механизмы

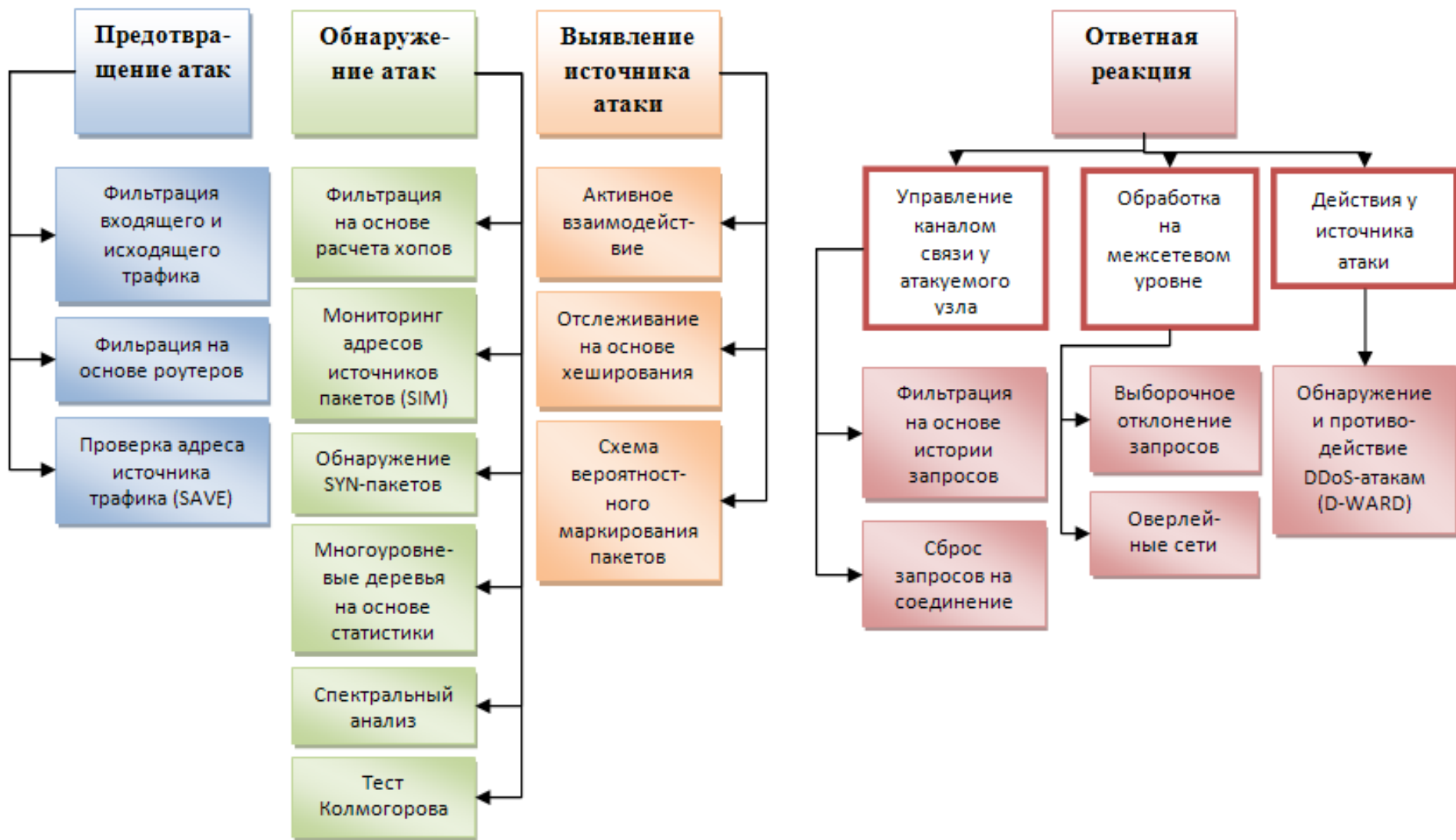


Распределенные механизмы



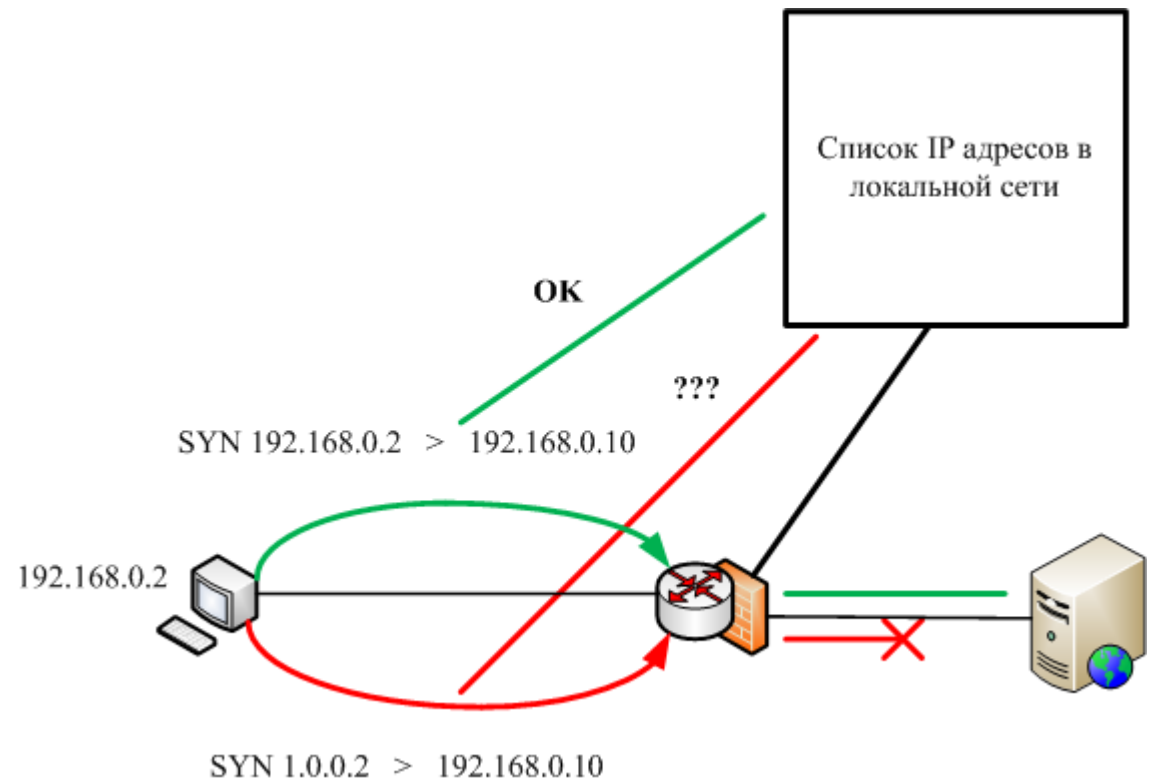
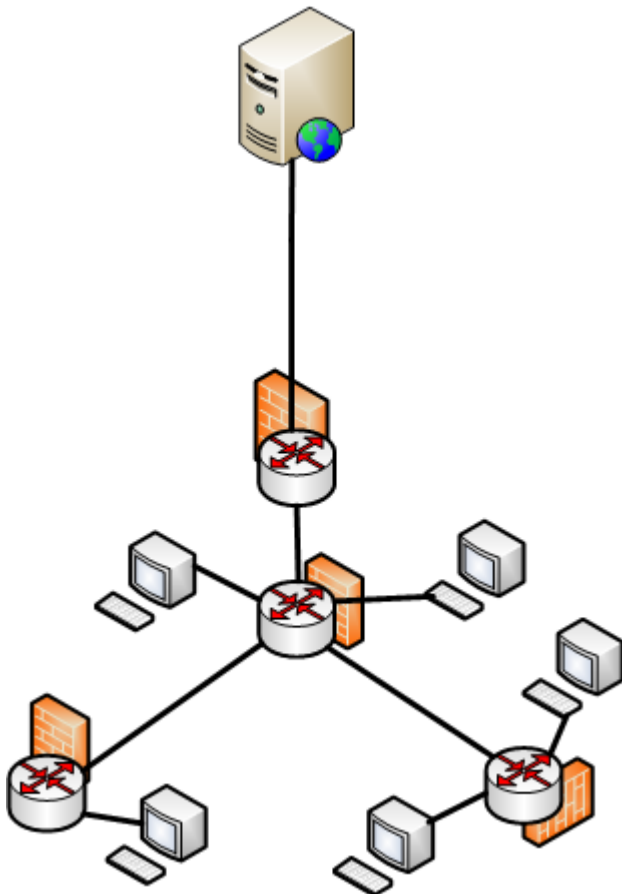


Классификация механизмов защиты от DDoS-атак

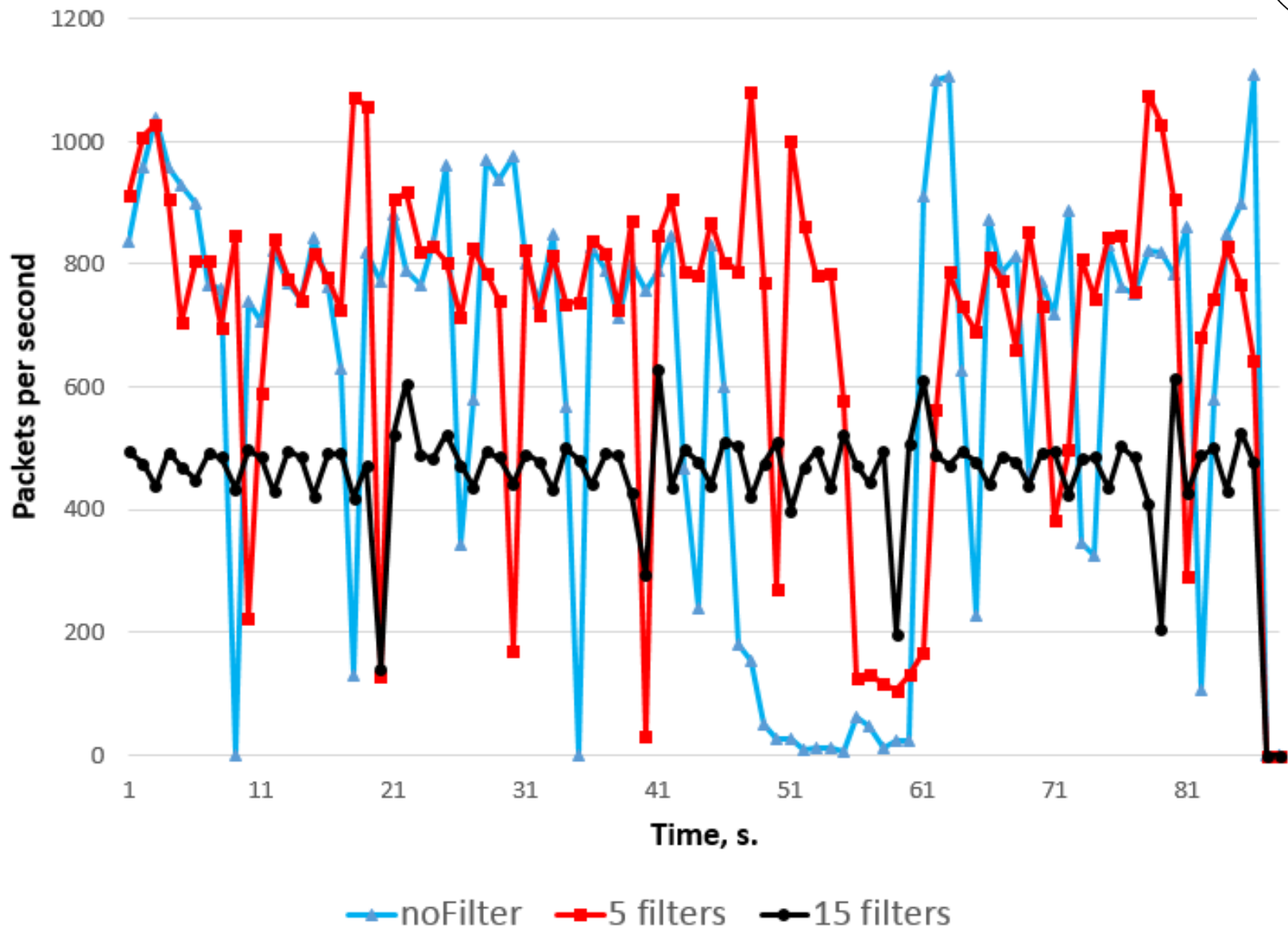


Egress Filtering

- 500 клиентов.
- 20 маршрутизаторов.



Egress Filtering





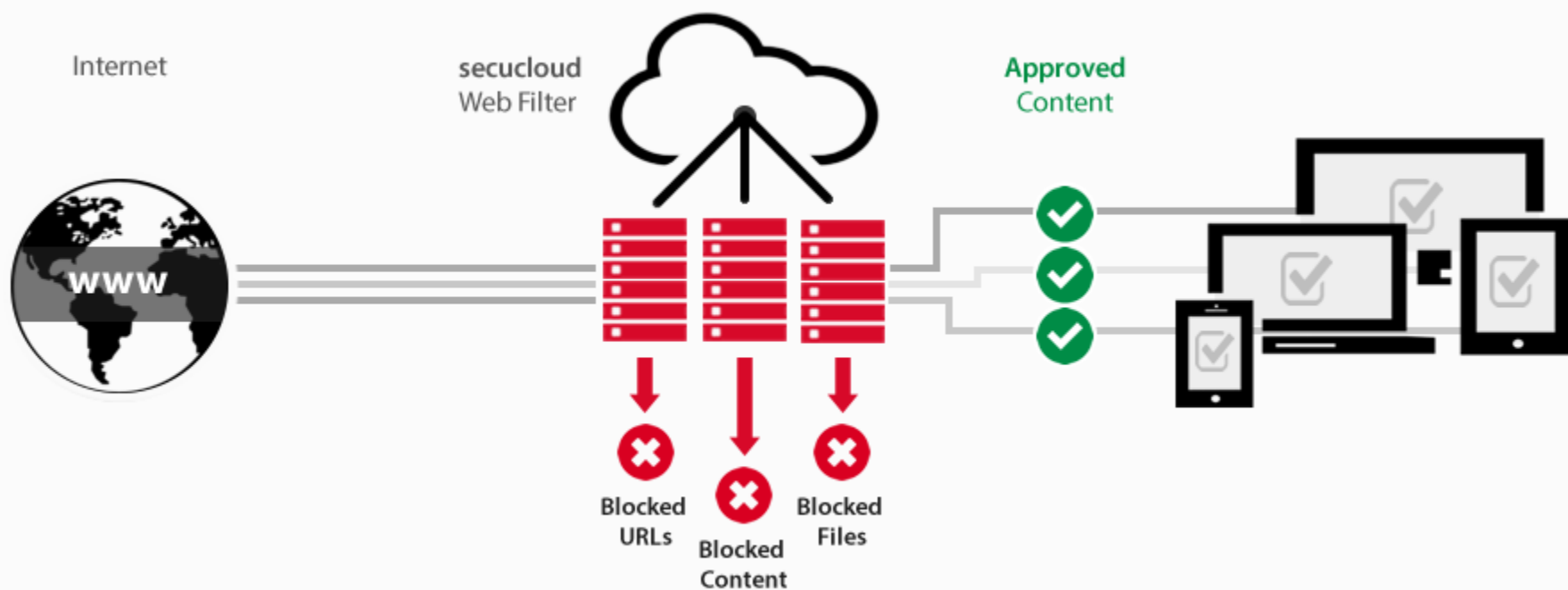
Разработка механизмов защиты облачных вычислительных сред

Механизмы защиты.

Существующие решения



- Web-filter
- IDS/IPS
- Firewall
- Antibot
- Apps filter
- IP reputation
- Antivirus



Защита облачных вычислительных сред



- Разработка защитных методик, работающих в режиме реального времени с применением технологий интеллектуального анализа данных.

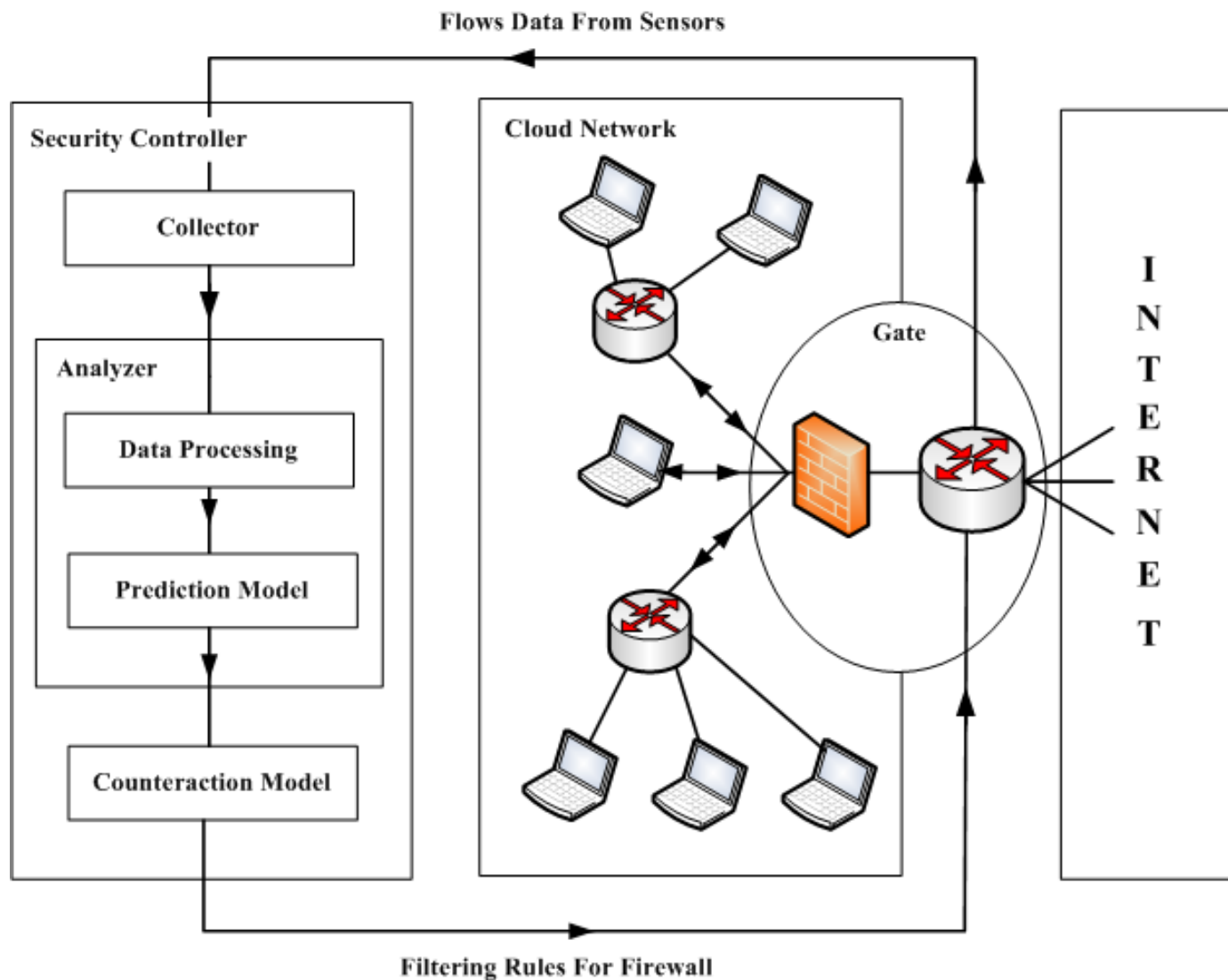


Задачи к механизмам защиты



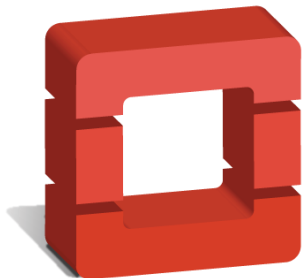
- Защита от инфраструктурных атак на Cloud.
- Разработать универсальную архитектуру.
- Не затрагивать клиентскую часть.
- Постараться избежать увеличения промежуточных узлов для трафика.

Универсальная архитектура





OpenStack



openstack™
CLOUD SOFTWARE

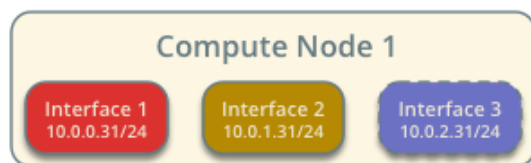
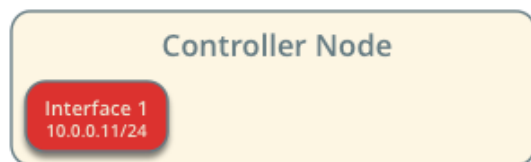
2010: Старт проекта.

2011: Основная облачная платформа Ubuntu.

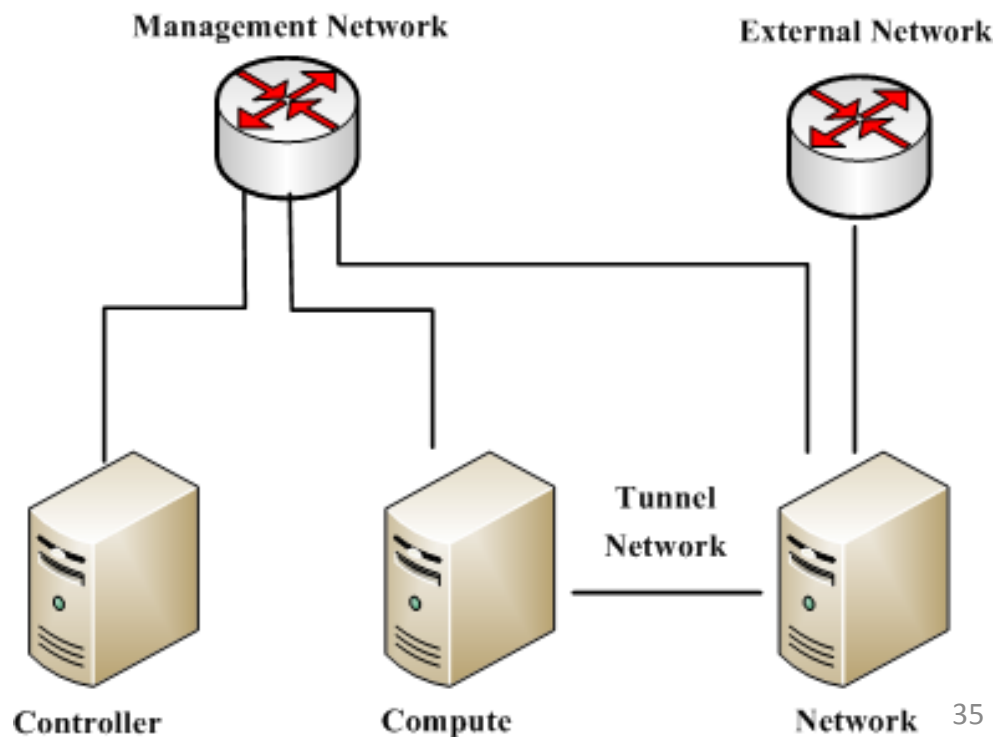
Примеры компаний, использующих OpenStack, как свою облачную платформу:



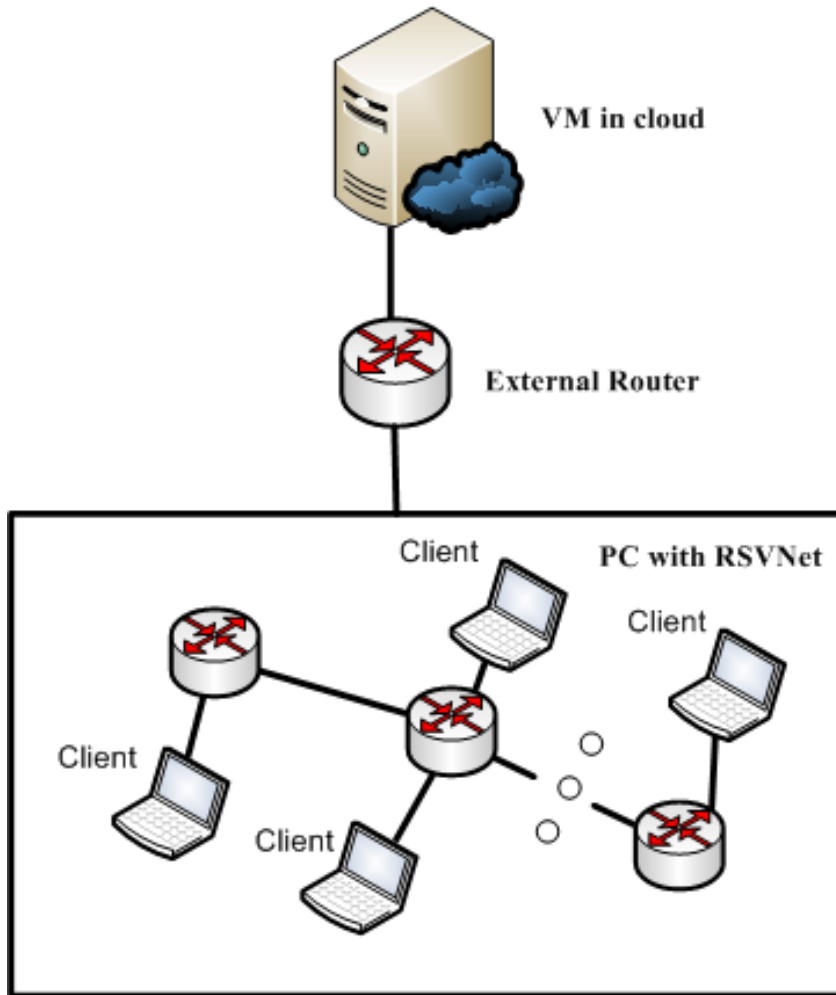
Архитектура OpenStack



- Management network
10.0.0.0/24
- Tunnel network
10.0.1.0/24
- External network
203.0.113.0/24
- Storage network
10.0.2.0/24



Топология для экспериментов



- Ubuntu 14.04. Apache2
- Dlink DIR-615
- Виртуальная сеть.

Механизмы защиты на основе методов интеллектуального анализа данных (Data Mining)

Машинное обучение. Data Mining



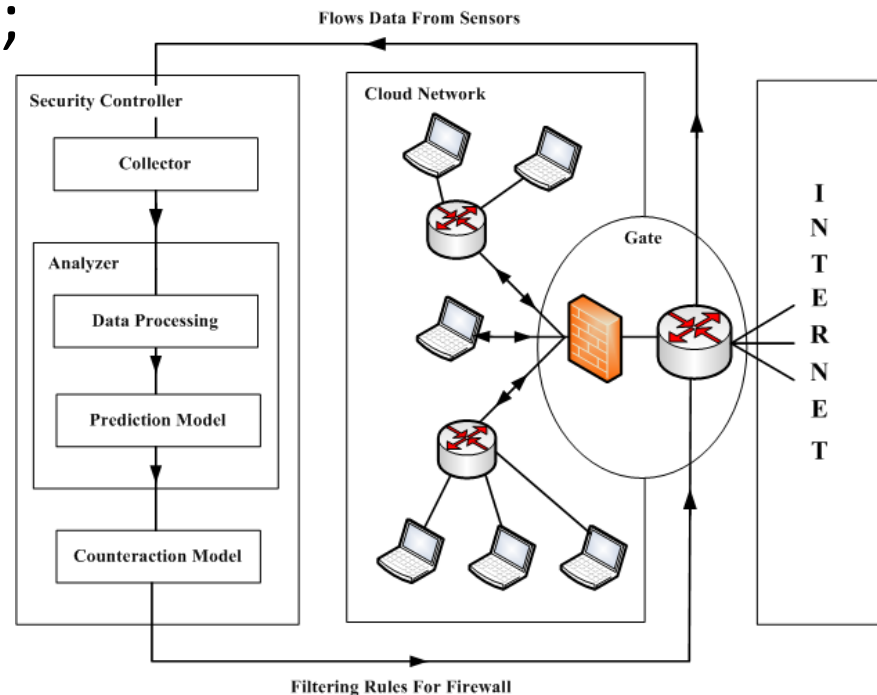
Сырые разрозненные
данные



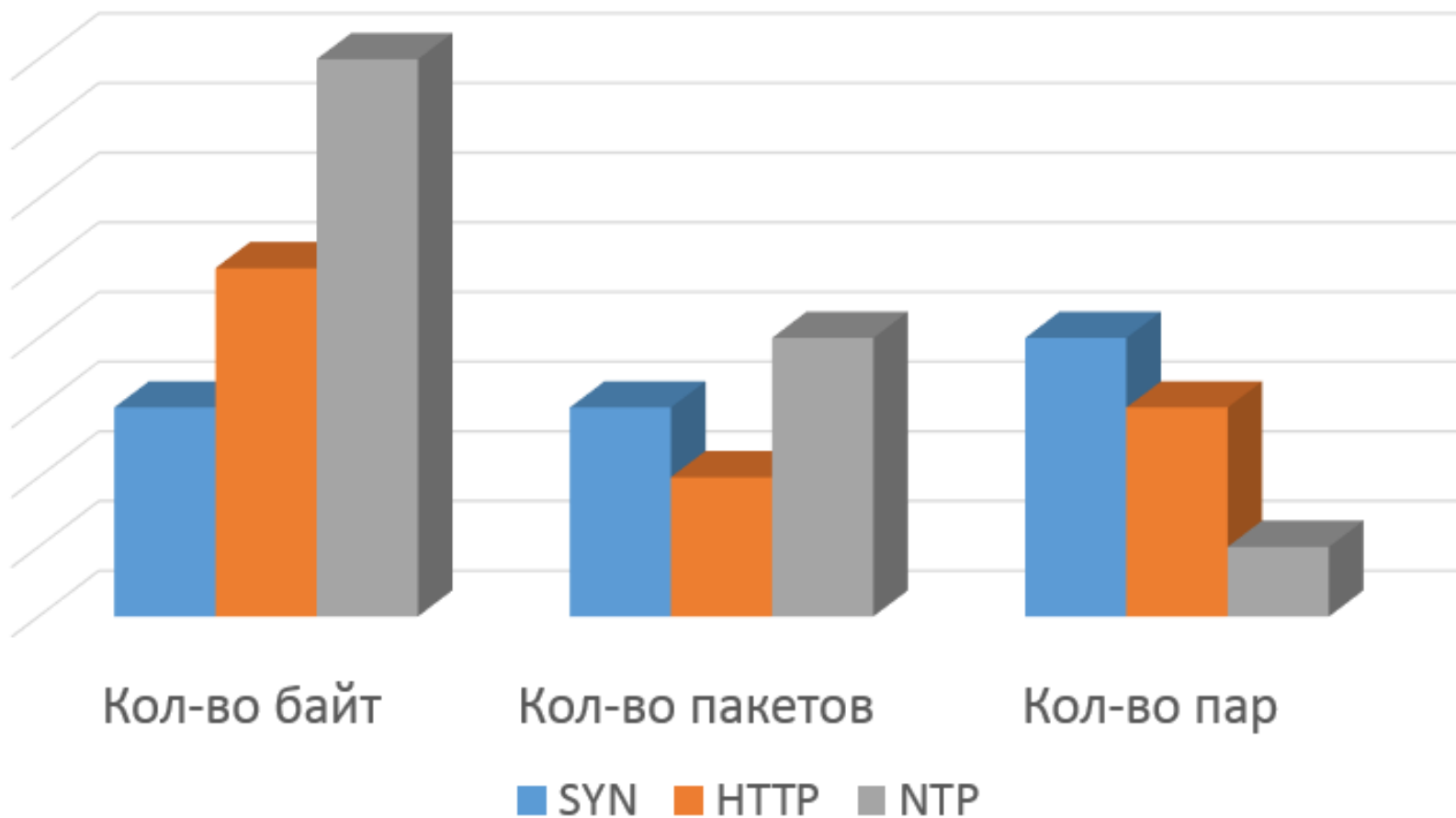
Интерпретация знаний для
принятия решений

Процесс ИАД

- анализ предметной области ;
- постановка задачи;
- подготовка данных;
- построение моделей;
- проверка и оценка моделей;
- выбор модели;
- применение модели;
- коррекция и обновление модели.



Сравнение значений атрибутов



Пример полученной выборки



Кол-во байт	Кол-во пакетов	Кол-во уникальных пар	Тип атаки
6100827	6207	1237	HTTP Flooding
21001332	20961	4131	HTTP Flooding
21245059	21148	4163	HTTP Flooding
21573832	21409	4227	HTTP Flooding
21084490	20991	4139	HTTP Flooding
20701543	20568	4056	HTTP Flooding
20937148	20850	4094	HTTP Flooding
20697609	20656	4064	HTTP Flooding

Проведенные эксперименты



- 3 типа атаки:
 - SYN Flooding.
 - HTTP Flooding.
 - NTP Flooding.
- Время эксперимента: 80 мин.
- Топология: 500 клиентов.
- Модели ИАД:
 - k-NN.
 - Neural Network.
 - Decision Tree.
 - SVM.
 - Naïve Bayes.

Пример результатов



	true Legitimate	true SYN	true HTTP	true NTP	class precision
pred. Legitimate	1199	0	0	0	100.00%
pred. SYN	0	1185	0	0	100.00%
pred. HTTP	0	0	1199	0	100.00%
pred. NTP	0	15	0	1200	98.77%
class recall	100.00%	98.75%	100.00%	100.00%	

Дальнейшая работа



- Создание компонент защиты, работающих в режиме реального времени.
- Создание сценариев противодействия различным типам атак.
- Анализ и оценка разработанных компонент.

Спасибо за внимание

Вопросы?

Константин Борисенко
borisenkoforleti@mail.ru

Андрей Шоров
ashxz@mail.ru