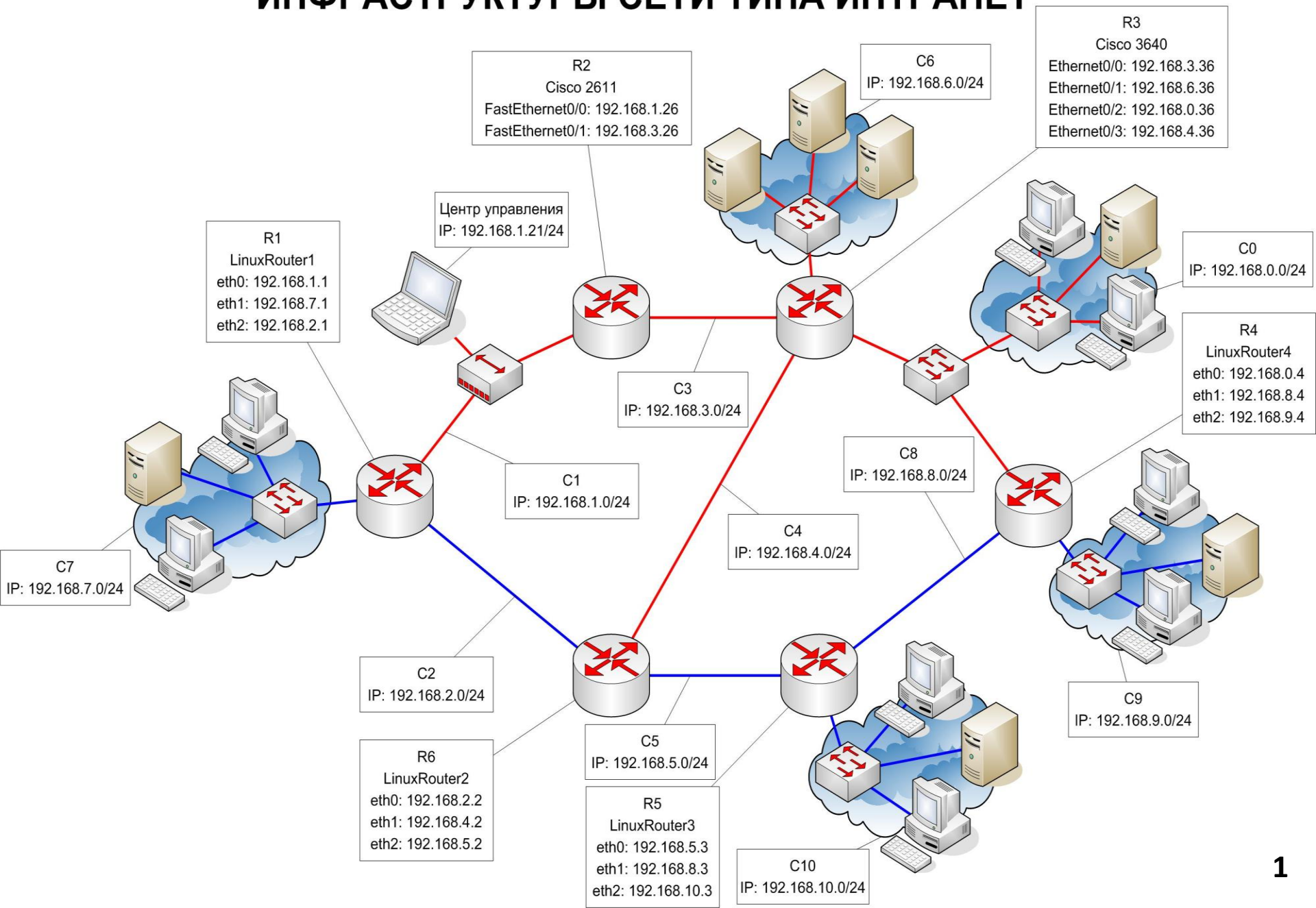
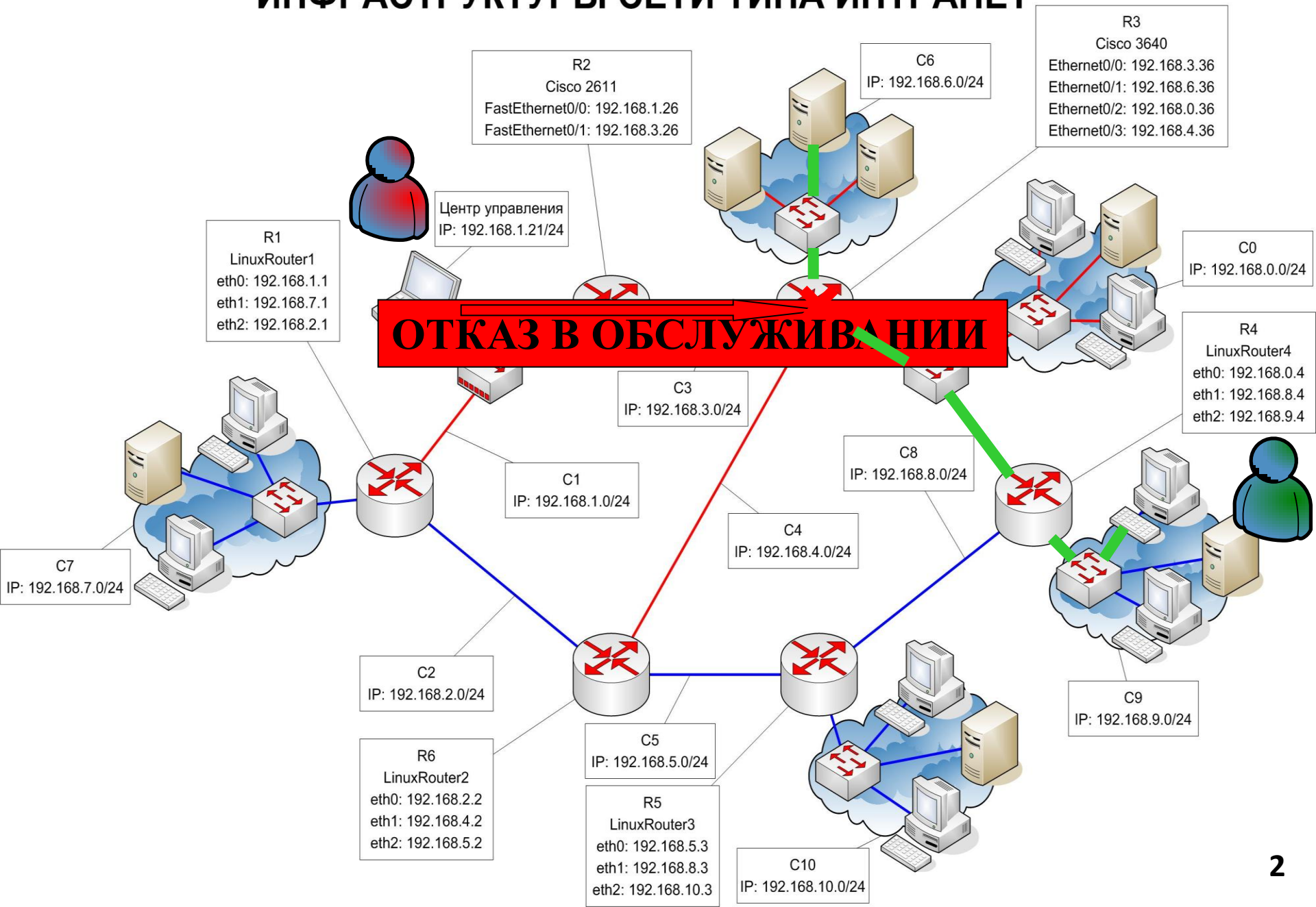
Использование DDoS-атак в качестве средства отвлечения внимания

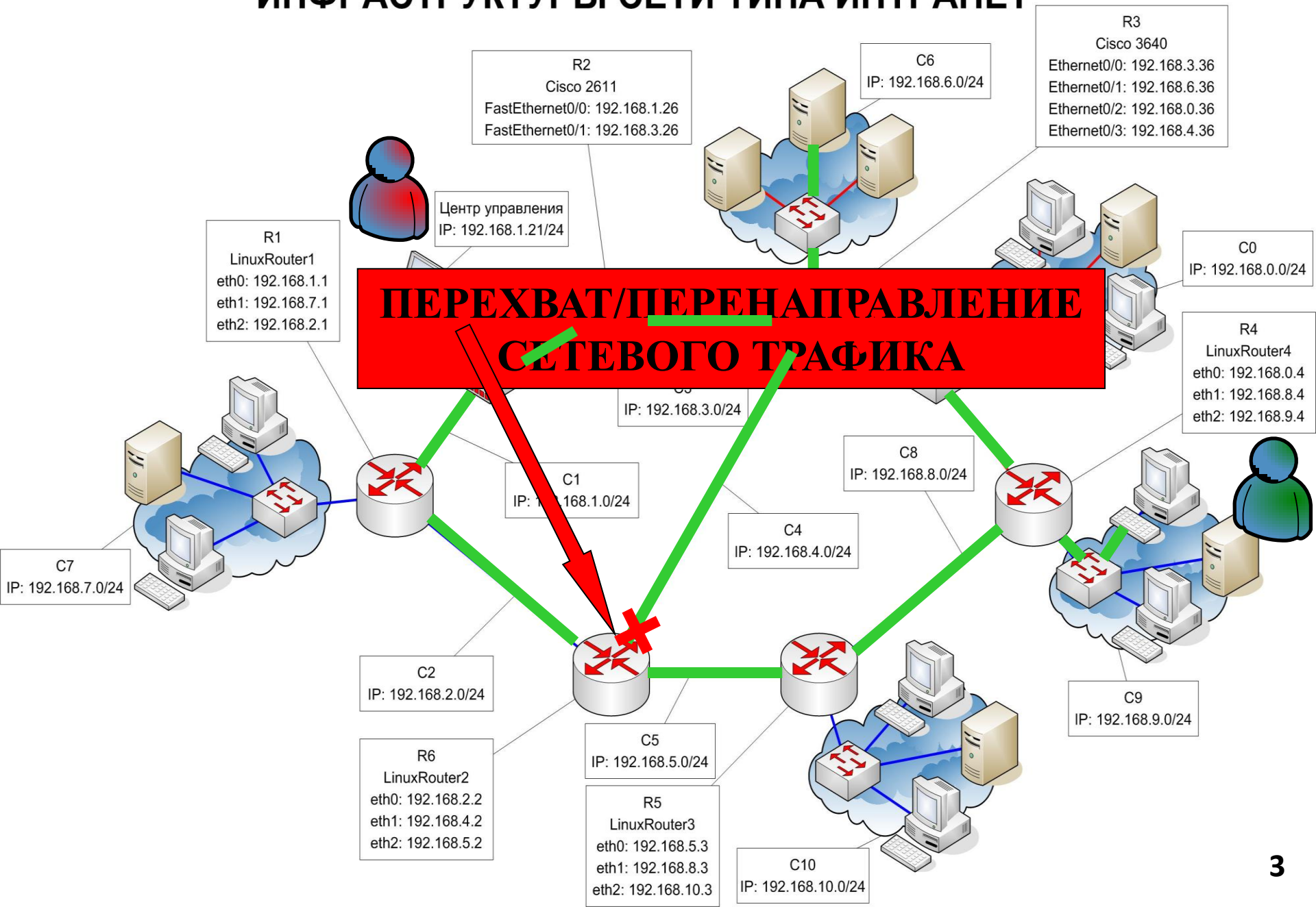
МОДЕЛЬ КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ СЕТИ ТИПА ИНТРАНЕТ



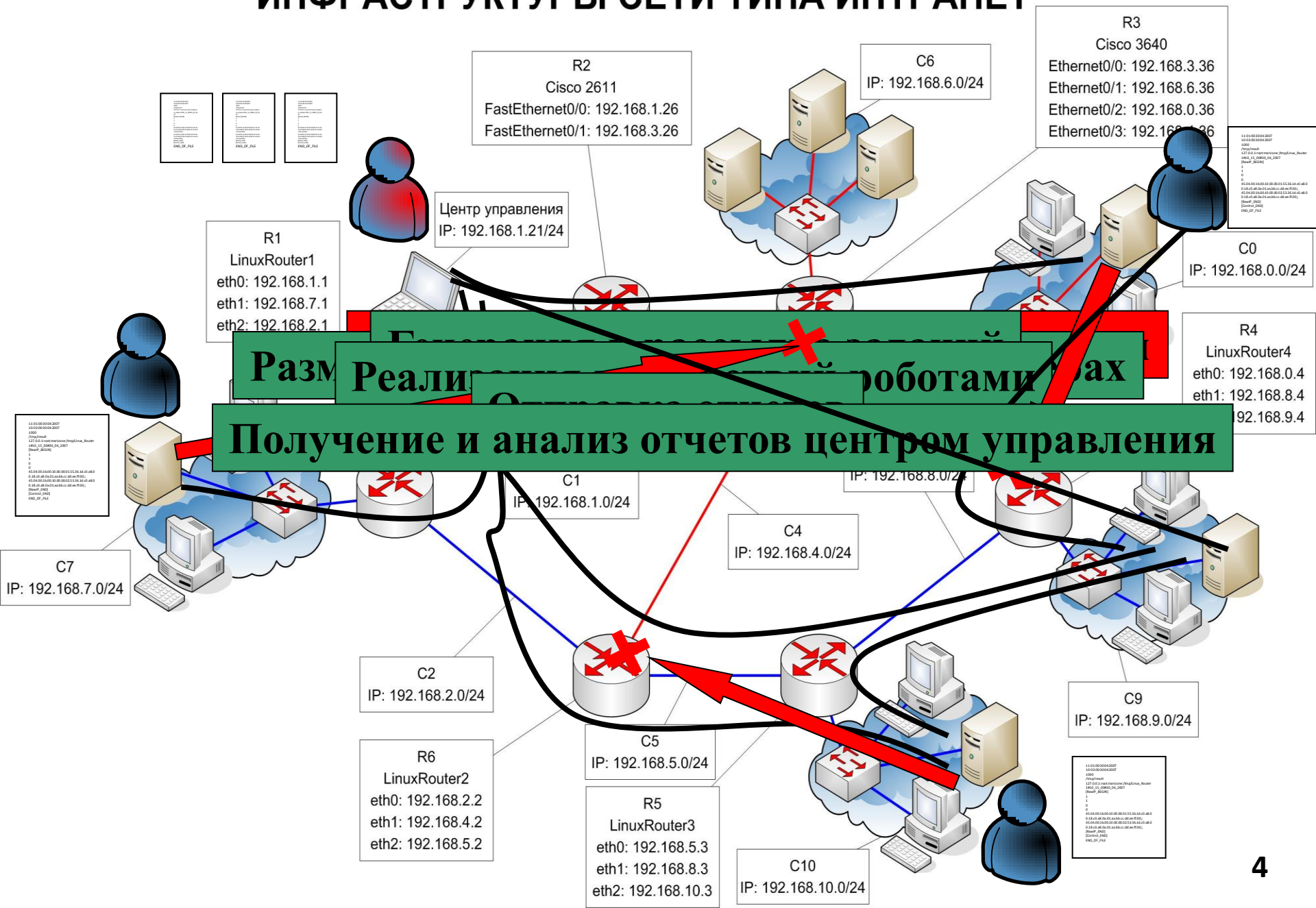
МОДЕЛЬ КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ СЕТИ ТИПА ИНТРАНЕТ



МОДЕЛЬ КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ СЕТИ ТИПА ИНТРАНЕТ



МОДЕЛЬ КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ СЕТИ ТИПА ИНТРАНЕТ



Противодействие DDoS-атакам

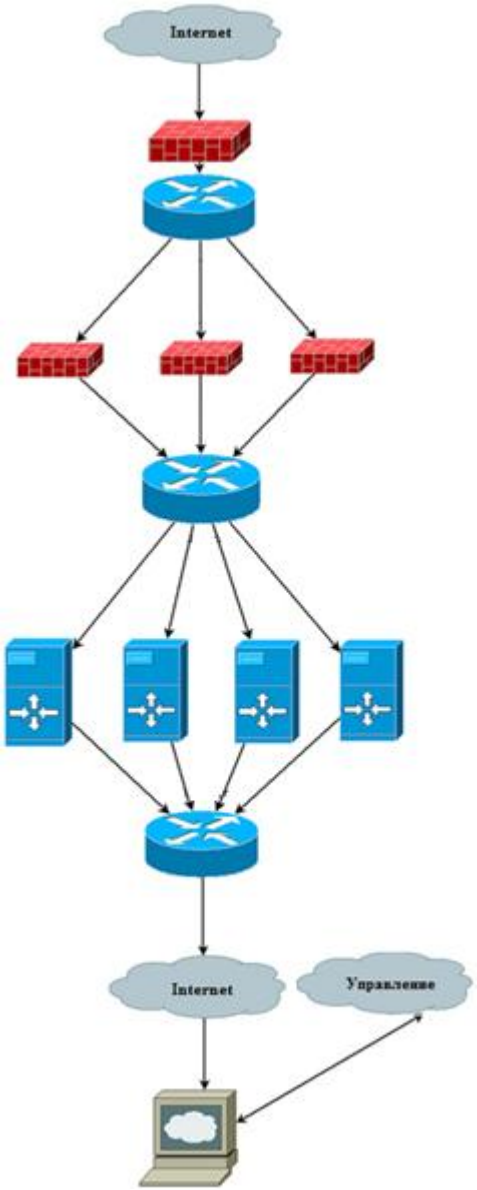
Характеристики удалённых DoS-атак

1) Удаленная эксплуатация ошибок в ПО с целью привести его в нерабочее состояние.
2) Атаки на ресурсы
    1) Переполнение ресурсов канала в интернет.
    2) Превышение максимального количества одновременных соединений сервера (SYN-флуд).
    3) Исчерпание процессорных мощностей сервера (частое запрашивание страниц - HTTP-флуд).

Анализ наиболее распространённых методов защиты

1) Модификация стека TCP/IP (использование SYN-cookies).
2) Настройка фильтров межсетевых экранов и параметров стека TCP/IP операционной системы.
3) Обновление используемого ПО.
4) Использование специализированных аппаратных решений для очистки трафика.
5) Построение инфраструктуры ЛВС, защищённой от DDoS (резервные интерфейсы доступа к серверам, системы анализа трафика, DMZ).
6) Резервирование дополнительных мощностей (каналы и сервера).
7) Использование тарифных планов с защитой от DDoS.

Комплексное решение на основе кластеризации



Отсюда идёт DDoS

Пакетный фильтр на пограничном маршрутизаторе обеспечивает защиту от сетевого флуда.
Пограничный маршрутизатор для балансировки нагрузки на межсетевой экран с анализом состояний.

Кластер межсетевых экранов с анализом состояний.

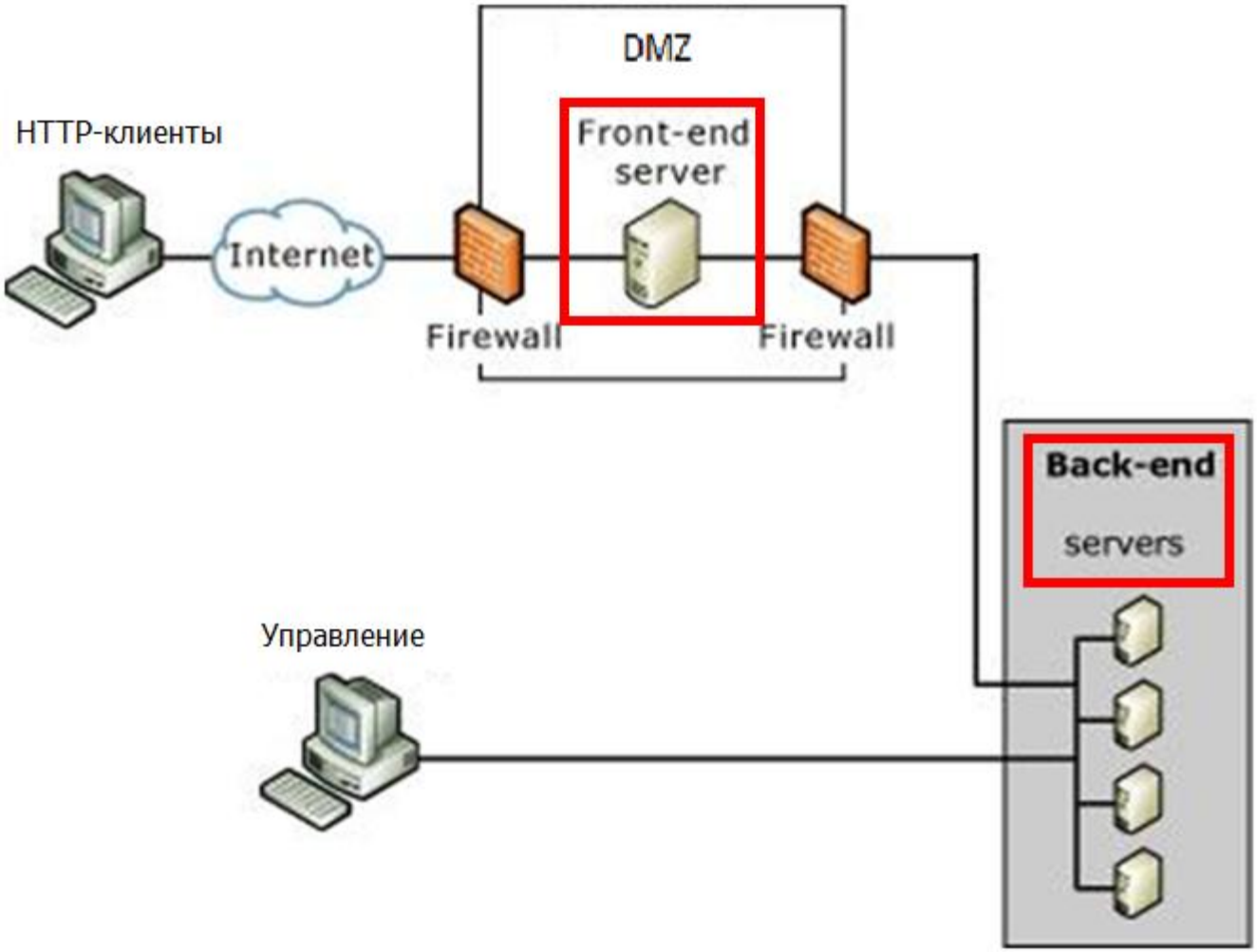
Маршрутизатор для балансировки нагрузки на proxy-сервера.

Proxy-сервера для отсеивания http-флуда.

Маршрутизатор для нефильрованных запросов

Backend-сервер

Решение на основе front-end/back-end



Архитектура

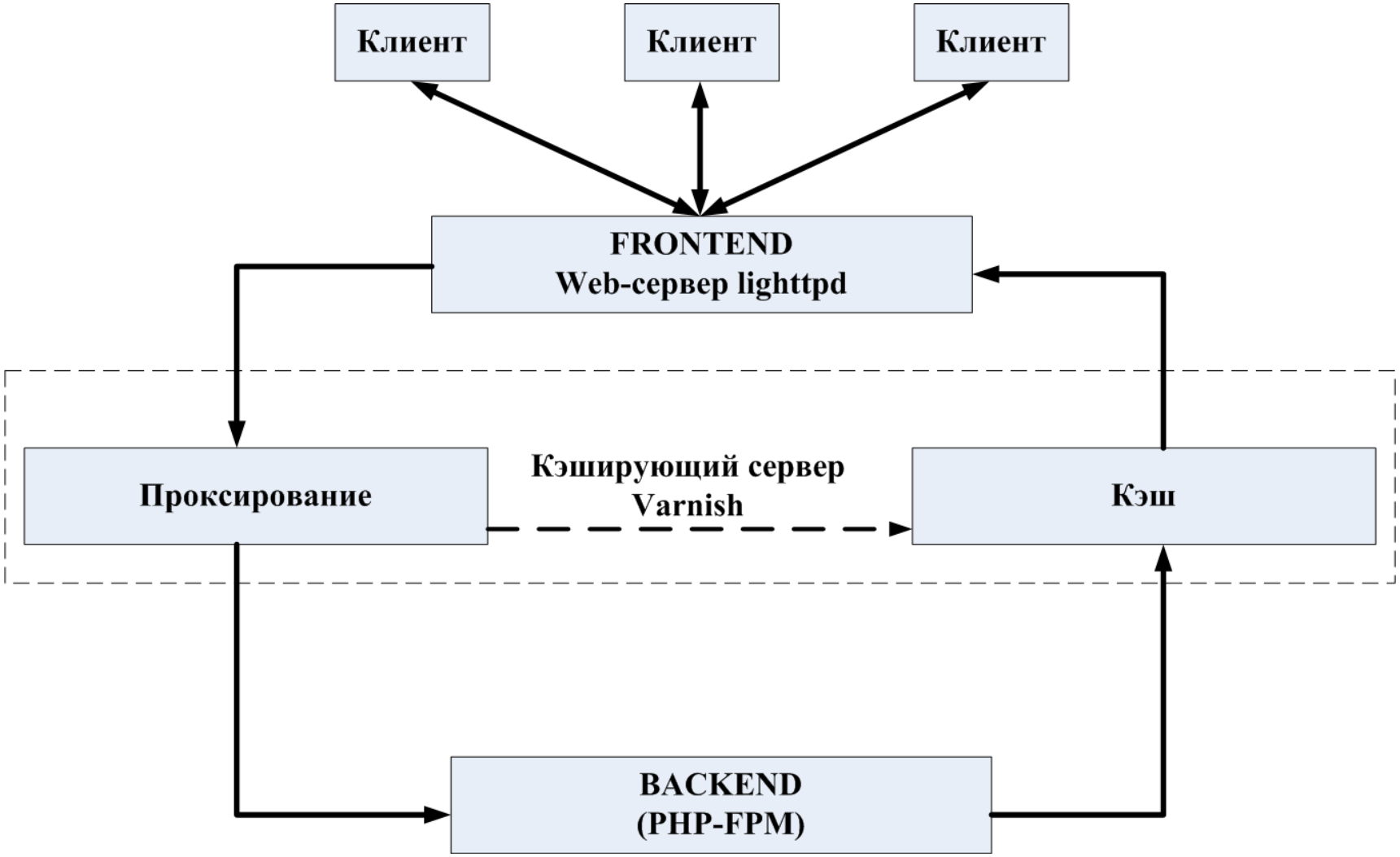
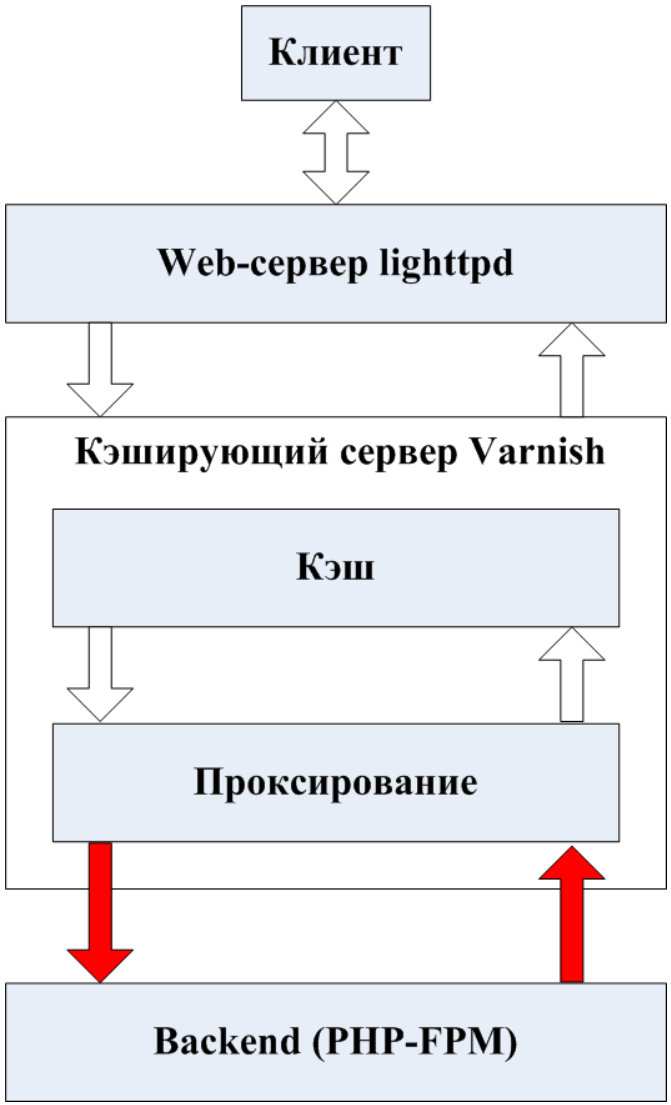
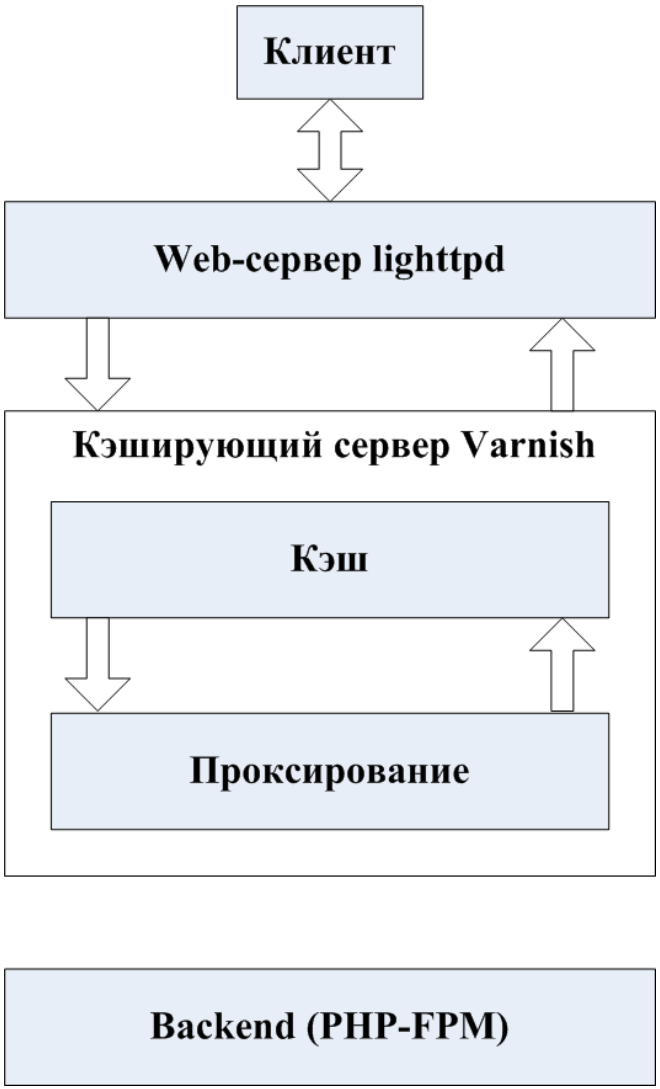


Схема работы

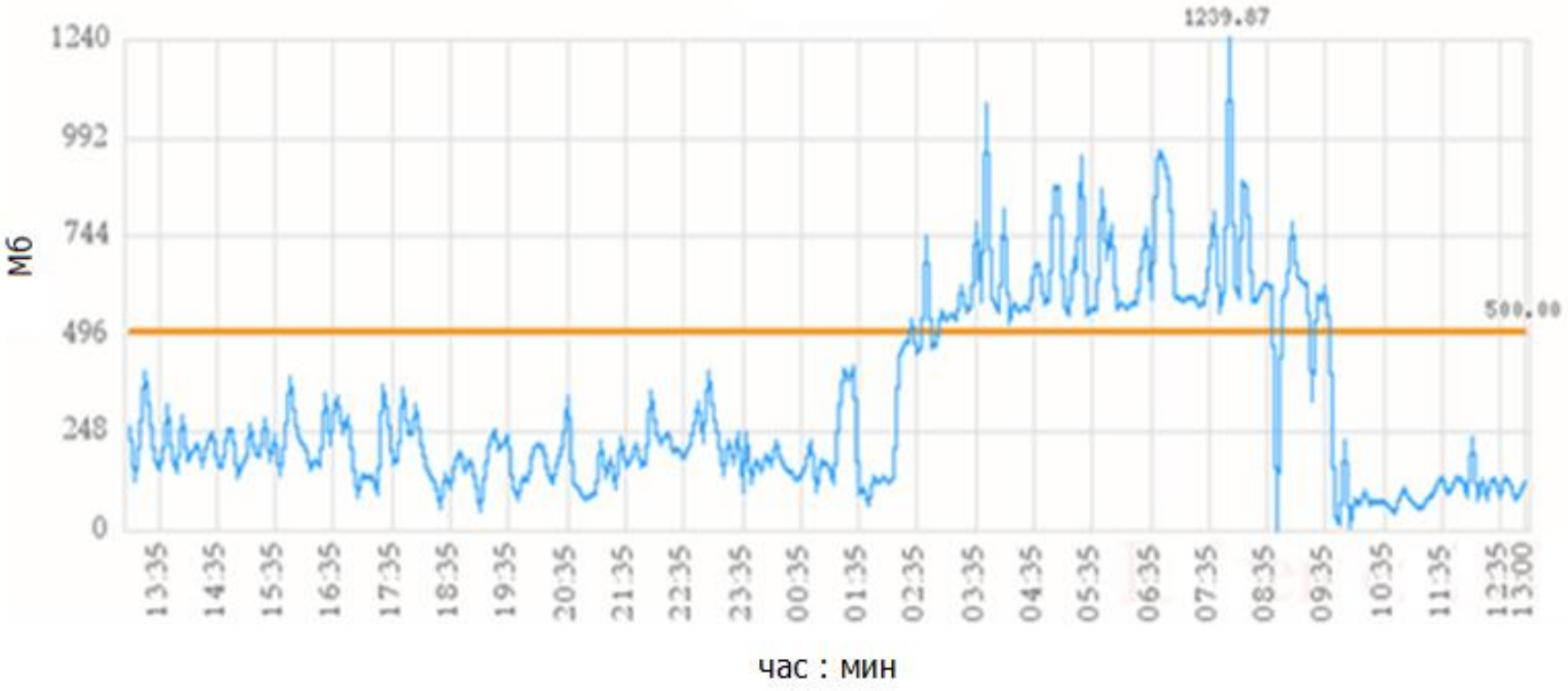


Для первого HTTP-запроса



Для последующих HTTP-запросов

Результат применения



Интенсивность DDoS-запросов (10 подключений в секунду с 2000 адресов) к backend при включённом и выключенном ПАК

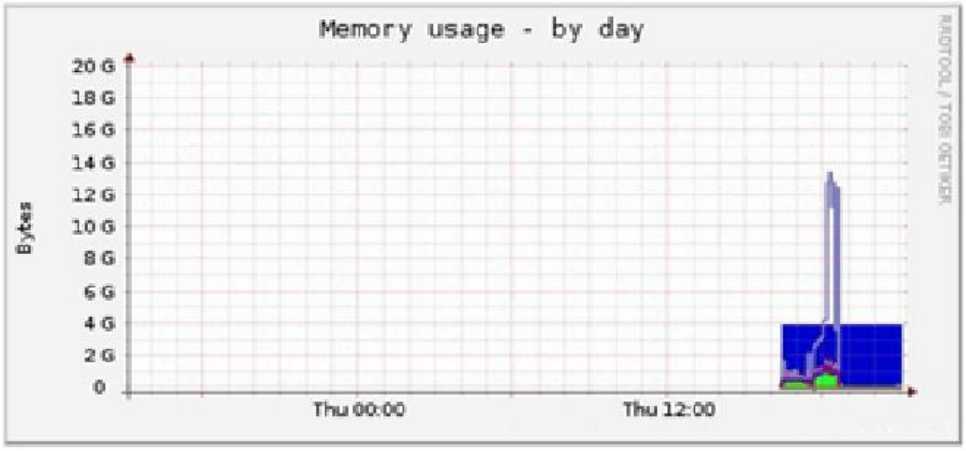
Методика оценки

Разработанный ПАК на базе Varnish + lighttpd + PHP-FPM сравнивался с распространенным практическим решением для Web-серверов малых компаний Apache2 Prefork + mod_php.

Имитируется ситуация сайта под DDOS-атакой в течение часа.
Сайт обслуживает 5000 легальных пользователей.
20000 ботов постоянно обращались к главной странице сайта.

Для этого использованы:
- **Apache Bench** – утилита для создания фоновой нагрузки на веб-сервер.
- **Siege** - утилита для пикового тестирования веб-серверов.

Экспериментальное исследование ПАК



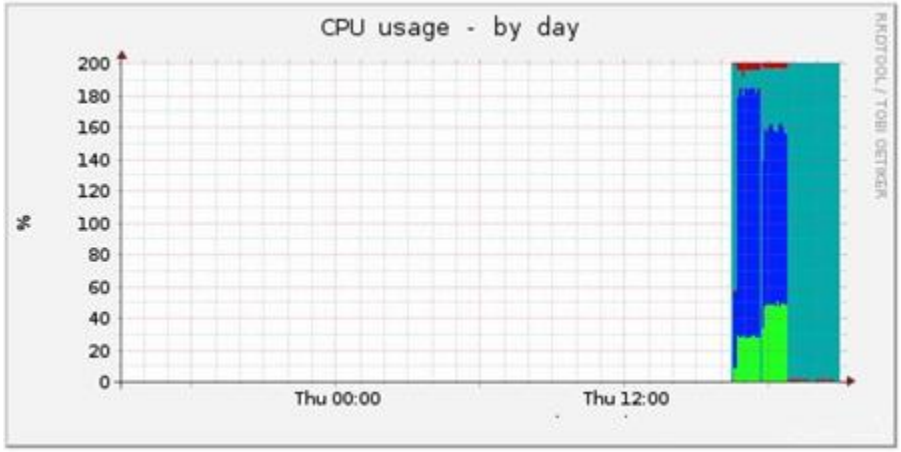


График использования памяти

График использования процессора

- Apache2 Prefork + mod_php

- Varnish + lighttpd + PHP-FPM

Анализ log-файлов доступности сервисов

```
# grep -c Failed lighttpd.log
38
# grep Failed lighttpd.log | grep -v 'Failed
requests:        0'
Failed requests:        10629
```

```
# grep -c Failed apache.log
23
# grep  Failed apache.log | grep -v
'Failed requests:        0'
Failed requests:        8730
Failed requests:        2124
Failed requests:        10539
Failed requests:        7599
Failed requests:        6027
Failed requests:        1986
Failed requests:        7578
Failed requests:        270
Failed requests:        9819
Failed requests:        60
Failed requests:        9369
Failed requests:        8193
Failed requests:        10248
Failed requests:        684
Failed requests:        7968
```

Лог lighttpd+varnish
38 итераций, одно падение сервиса,
вызвано пиковой нагрузкой

Лог Apache
23 итерации, 15 падений сервиса,
Только 2 вызваны пиковыми нагрузками