Инфозащита

Эффективные решения для защиты информации

Защита от DDoS-атак – анализ примеров из практики

www.itprotect.ru

МОСКВА, CNEWS FORUM 2014

KASPERSKY lab
ENTERPRISE PARTNER

Информация о Компании

- ✓ **Компания «Инфозащита»** – системный интегратор в области информационной безопасности
- ✓ **6+** лет на рынке
- ✓ **2000+ клиентов**
- ✓ **Широкий спектр услуг** по обеспечению ИБ
- ✓ **Сертификация системы менеджмента качества услуг** (ISO 9001)
- ✓ «Инфозащита» имеет все необходимые **лицензии ФСБ России и ФСТЭК России** для осуществления деятельности по защите информации, в том числе с использованием криптографических средств

KASPERSKY lab
ENTERPRISE PARTNER

DDoS атака

Объекты атак	Типы DDoS атак	Средства DDoS атак
▪ Канал ▪ Сетевое оборудование ▪ Приложение	▪ TCP connection ▪ Volumetric ▪ Fragmentation ▪ Application	▪ Ботнеты ▪ Выделенные сервера ▪ Усиление (Amplification)

DDoS =(Количество устройств) x (Производительность) x (скорость соединения с Интернет)

Цена атаки уменьшается, мощность увеличивается

Решения по защите от DDoS атак

Аппаратно-программный комплекс	Сервис от провайдера	Специализированный сервис
▪ Arbor ▪ Radware	▪ Ростелеком ▪ Акадо ▪ Мегафон	▪ Kaspersky DDoS Prevention ▪ Prolexic ▪ Qrator

KASPERSKY
ENTERPRISE PARTNER

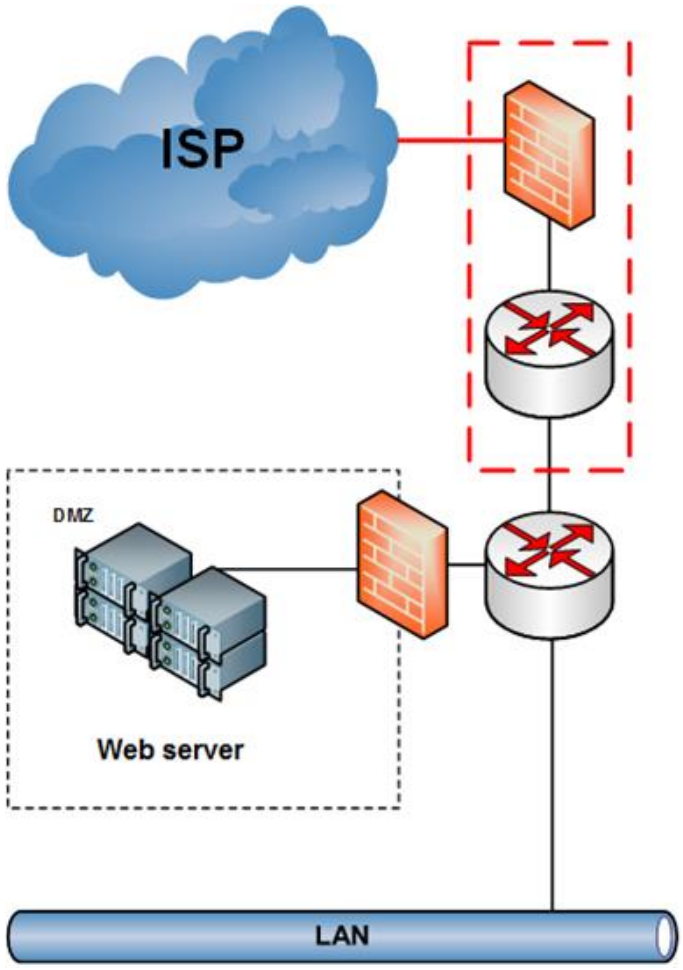
Реальный пример DDoS атаки

Клиент – крупная ритейл организация

Дата – сентябрь 2014 года

- ✓ **Веб-ресурс не доступен внешним пользователям**
- ✓ **Внешние ИТ сервисы (почта, Интернет) не работали**
- ✓ **Блокировка зарубежного трафика дала эффект, но не надолго**

- **Канал загружен на 60-70%**
- **Нагрузка на межсетевом экране 100%**
- **Комбинированная атака UDP flood + Application**



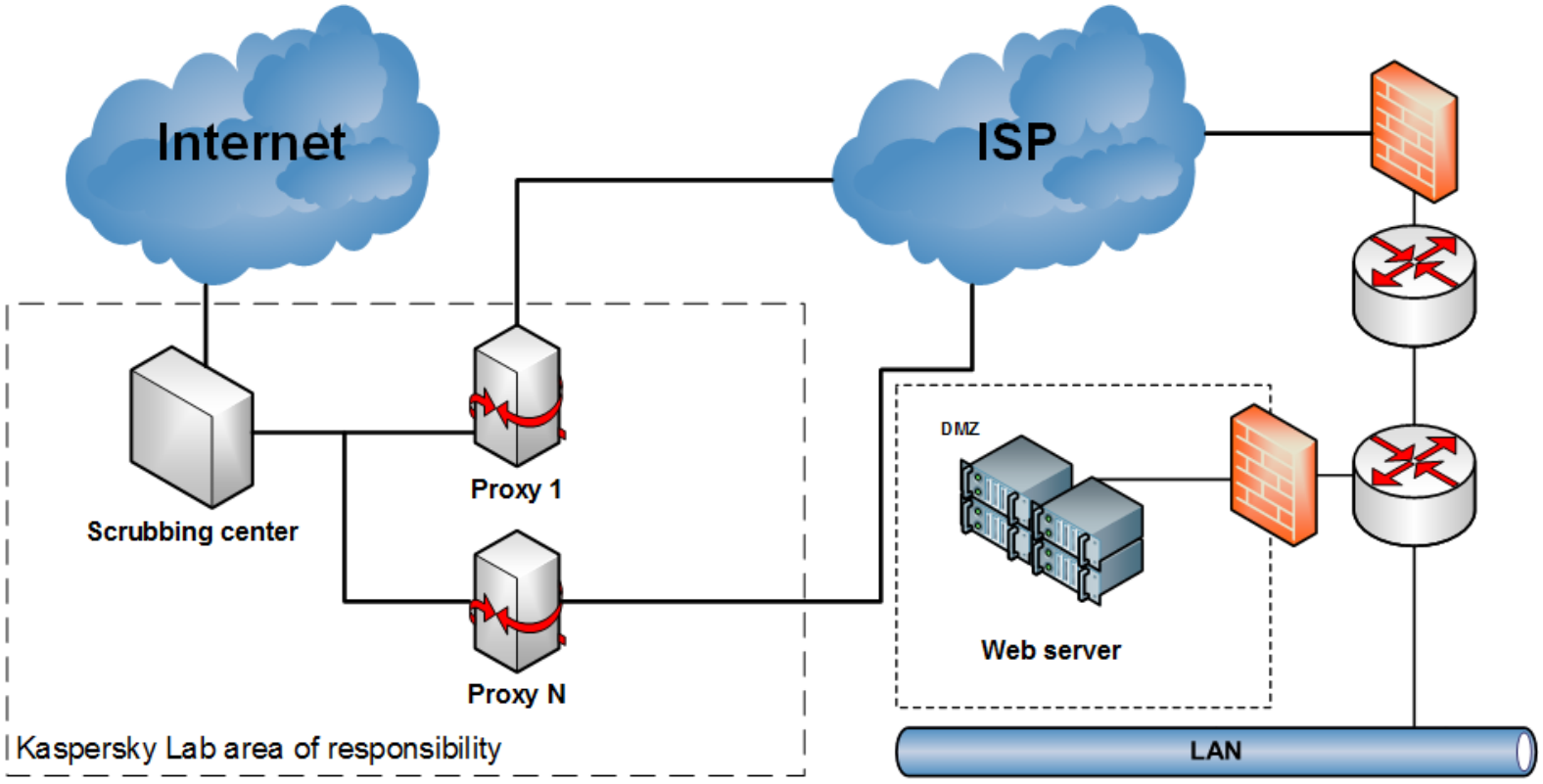
KASPERSKY
ENTERPRISE PARTNER

Подключение к KDP – экстренная схема

Применение схемы экстренного подключения с перенаправлением трафика на ЦОТ KDP по DNS и доставкой очищенного трафика методом проксирования:

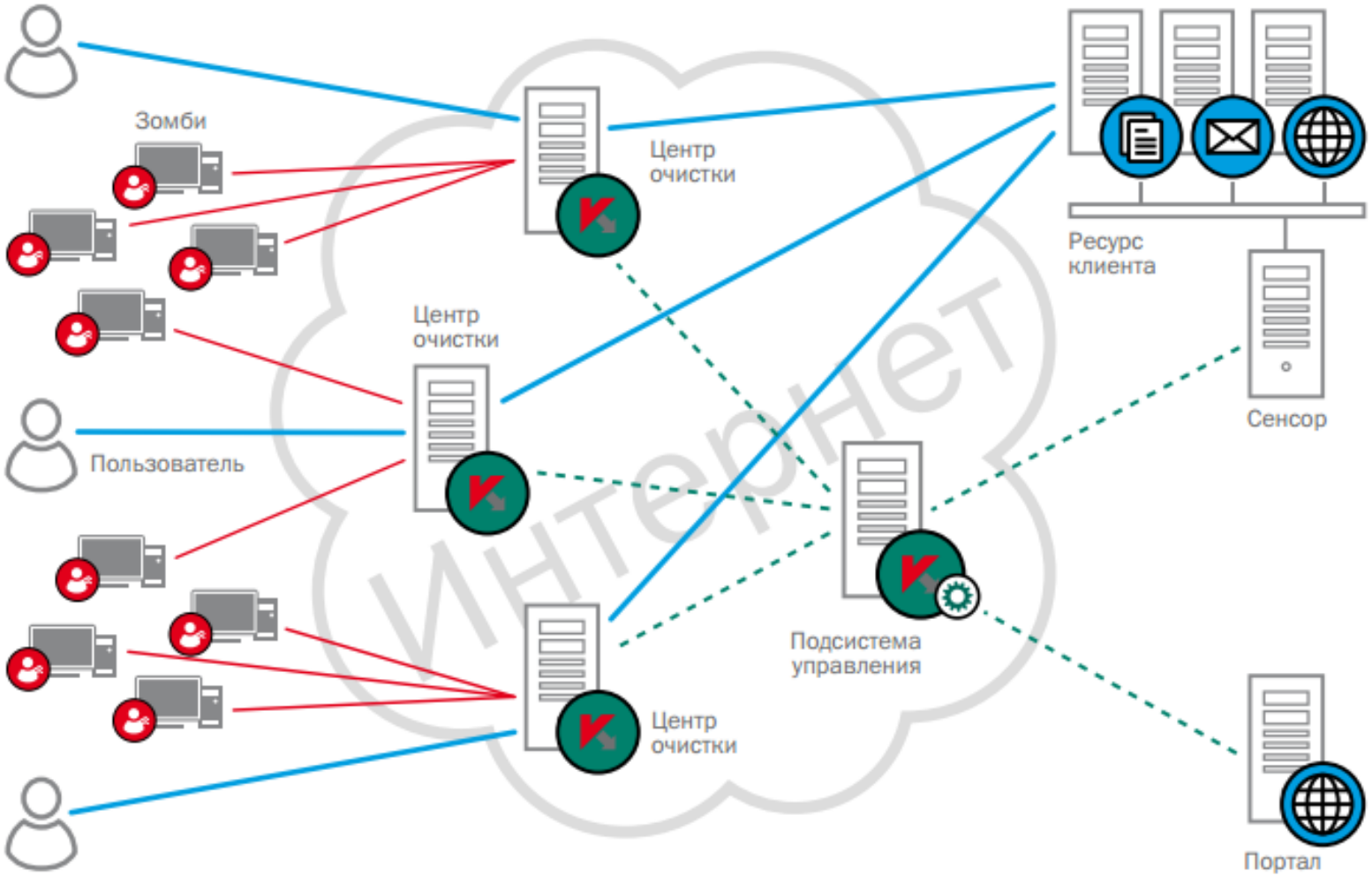
Использование решения KDP

- ✓ Затраченное время на подключение: 1.5 часа
- ✓ Оперативное восстановление работоспособности ресурса после переключения на KDP



KASPERSKY
ENTERPRISE PARTNER

Архитектура KDP



KASPERSKY
ENTERPRISE PARTNER

Результат

- ✓ Предотвращены существенные потери Заказчика
- ✓ Восстановлена работоспособность внешних сервисов Заказчика
- ✓ Проведено расследование по инциденту DDoS атаки, информация предоставлена Службе безопасности Заказчика
- ✓ Заказчик использует решение KDP (BGP)
- ✓ На протяжении всего периода использования KDP отказов в доступности внешних ресурсов Заказчика в следствии DDoS атак не зафиксировано

KASPERSKY ENTERPRISE PARTNER

Преимущества KDP

Собственная разработка

Решение регулярно обновляется, не зависит от вендоров

Поддержка 24x7

Фильтры настраиваются под каждого клиента, при необходимости обновляются

Защищаем ресурсы, а не каналы

Мониторинг трафика, при необходимости оперативно переводим ресурс под защиту

Партнерство с ISP

В том числе фильтрация на стороне провайдера

KL DDoS Intelligence

Расследование DDoS

Экспертиза и своевременная защита на ранних стадиях

✓ **ЗАО «Инфозащита» - Enterprise Partner Kaspersky Lab**

KASPERSKY lab
ENTERPRISE PARTNER

Спасибо за внимание!

Михаил Магун

Руководитель направления информационной безопасности

ЗАО «Инфозащита»

m.magun@itprotect.ru