11.07.2022

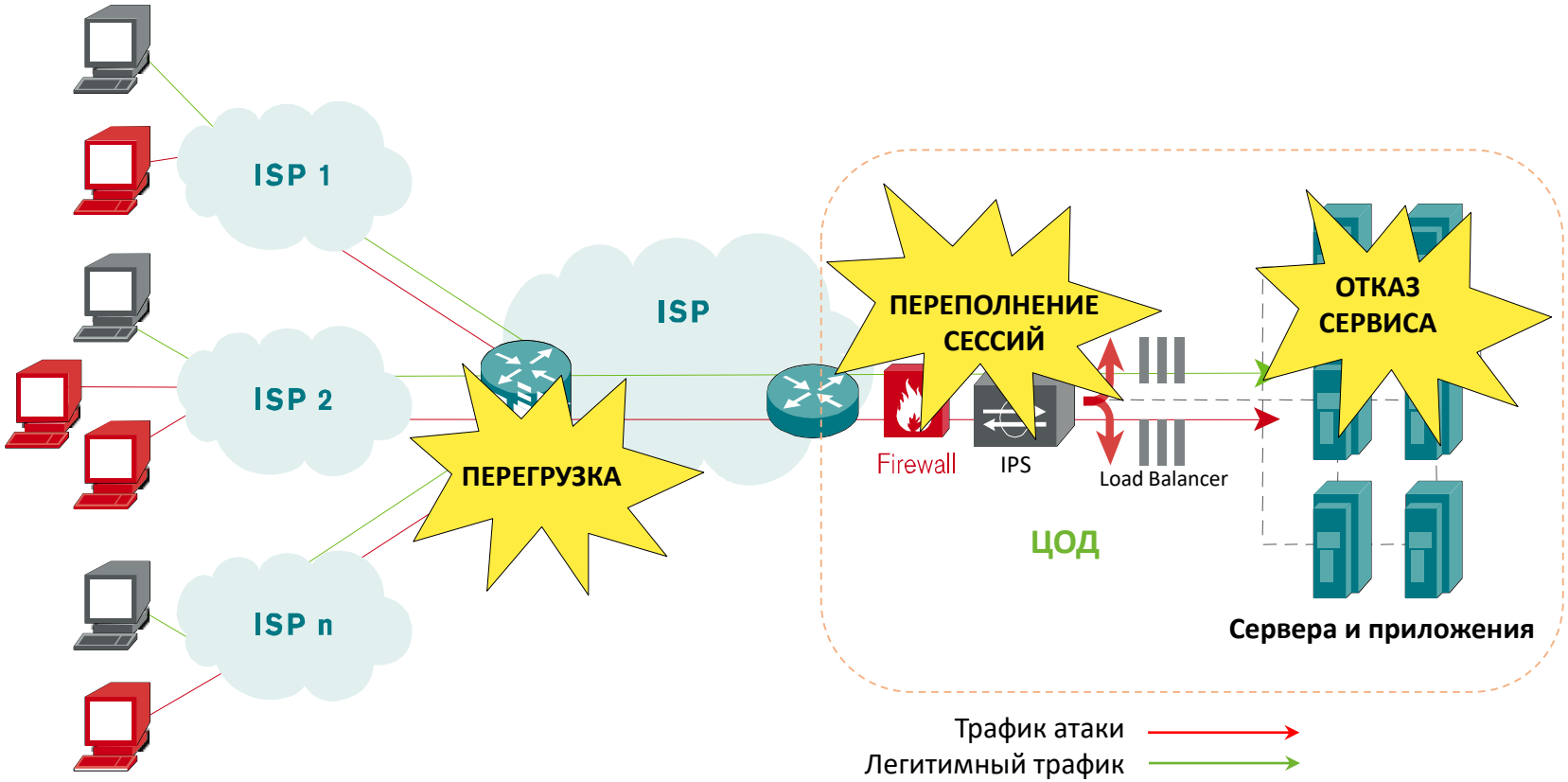
DDoS как инструмент Кибероперации. Цели, подходы, защита

Артем Избаенков

член правления АРСИБ

член ISDEF

Сложность современных DDoS атак



Сегодня DDoS можно классифицировать на 3 типа

1. Перегрузку канала (атака на канальную часть)
2. Переполнений таблиц сессий (атака на сетевое оборудование)
3. Отказ сервиса (атака на приложение)

Кибероперация

•Госструктуры	•Телеком	•Доменные регистраторы	Грузоперевозчики	Нефтегазовая отрасль
Металлургия	Электроэнергетика	Банки	•Платежные системы	Авиакомпании
•Крупный E-comm	Машиностроение	Хостинговые компании	Информационные порталы	Электронные торговые площадки

Виды сетевых атак сейчас

DDoS

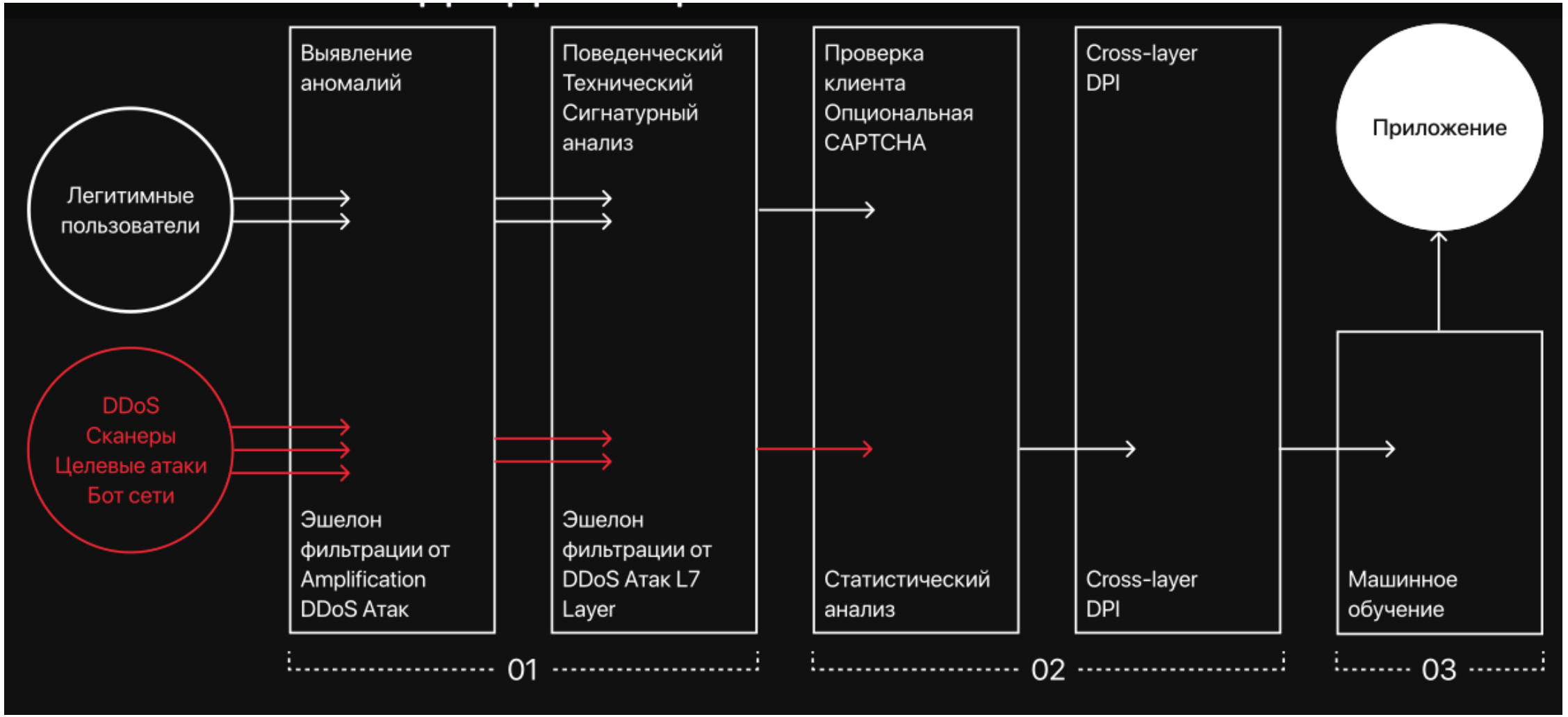
- каналов связи
- DNS сервисов
- веб-сайтов
- мобильных API

Ботовая активность

- Content/Web Scraping
- Parsing
- Brute force
- Credential Stuffing
- Cookie Stuffing

- SMS Leak
- SQL инъекции
- XSS атаки
- Click fraud
- Spam

Комплексный подход к защите сетевого периметра



Конкурентный анализ облачного решения

Эталон	Решение 1	Решение 2	Решение 3	Решение 4
Собственное разработанное для себя решение	-	-	Netscout Arbor	АПК Периметр, Netscout Arbor
Возможность организации «выделенного облака» с выделенными ресурсами под конкретного клиента	-	Только общее облако	Только общее облако	Только общее облако
Множество точек присутствия по России, присутствие в Европе	Множество точек присутствия в России, присутствие в Европе	Множество точек присутствия в России, присутствие в Европе	Только Россия	Только Россия
Уникальный конструктор правил позволяющий создать даже самые сложные технические решения для защиты критически-важных сервисов, без модификации программного кода	-	-	Ограничения обусловленные сторонним вендорским решением, его контрмерами и функционалом	Ограничения обусловленные сторонним вендорским решением, его контрмерами и функционалом
Возможность постоянной фильтрации, сброс вредоносного трафика за <1 секунду*	Возможность постоянной фильтрации	Возможность постоянной фильтрации	Ограниченная возможность постоянной фильтрации обусловленная ограничениями оборудования	Ограниченная возможность постоянной фильтрации обусловленная ограничениями оборудования
Тонкая очистка до 900 Gbps и 900 Mpps*	-	-	-	-
Грубая очистка до 5 Тбит/с*	-	-	-	-
Возможность гибридных инсталляций, on-premise решений	-	Только облачное решение	Только облачное решение	Только облачное решение

Конкурентный анализ вендорского решения

Эталон	Решение 1	Решение 2	Решение 3	Решение 4
Может поставляться как программное обеспечение, АПК, облачный сервис	АПК или облачный сервис	АПК или облачный сервис	АПК или облачный сервис	Программное обеспечение или АПК
До 400 ГБит/с и 200Mpps на 1RU	До 40 ГБит/с и 20Mpps на 2RU	До 380 ГБит/с и 110Mpps на 1RU, самая дорогая модель на рынке сегодня	До 400 ГБит/с и 230Mpps на 2RU*	До 100 ГБит/с и 140Mpps на 1RU
Расширенный конструктор правил с готовыми контрмерами	Ограниченное кол-во контрмер и опций взаимодействия	Ограниченное кол-во контрмер и опций взаимодействия	Ограниченное кол-во контрмер и опций взаимодействия	Ограниченное кол-во контрмер и опций взаимодействия
Статистика в любой части системы, в любом правиле	Только глобальная и статистика на каждую контрмеру	Только глобальная и статистика на каждую контрмеру	Только глобальная и статистика на каждую контрмеру	Только глобальная и статистика на каждую контрмеру
Работает на стандартизированном серверном оборудовании	Работает только на вендорском оборудовании	Работает только на вендорском оборудовании	Работает только на вендорском оборудовании	Работает на стандартизированном серверном оборудовании
Поддержка любого user-space приложения (NGINX, BGP, etc.)	Серверные мощности выделяются только под ПО вендора	Серверные мощности выделяются только под ПО вендора	Серверные мощности выделяются только под ПО вендора	Серверные мощности выделяются только под ПО вендора
До 150 000 000 одновременно активных правил в системе	До XX активных профилей защиты	До 60 000 000 одновременно частично-активных правил*		
Множество вариантов применения помимо ДДоС-защиты за счет расширенного конструктора правил	Только ДДоС-защиты с помощью ограниченного кол-ва контрмер	Только ДДоС-защиты с помощью ограниченного кол-ва контрмер	Только ДДоС-защиты с помощью ограниченного кол-ва контрмер	Только ДДоС-защиты с помощью ограниченного кол-ва контрмер
Возможность глобальной кластеризации в 10 ТБит/с+	До 400 ГБит/с в активном кластере	До 3 ТБит/с в активном кластере		
Упрощенная внешняя интеграция за счет API, возможности запуска любых user-space приложений на том-же оборудовании	Ограниченная интеграция осуществляемая за счет REST API	Ограниченная интеграция осуществляемая за счет REST API	Ограниченная интеграция осуществляемая за счет REST API	Ограниченная интеграция осуществляемая за счет REST API
On-Premise, In-Cloud, Hybrid — все возможные варианты инсталляции	On-Premise, In-Cloud, Hybrid — все возможные варианты инсталляции	On-Premise, In-Cloud, Hybrid — все возможные варианты инсталляции	On-Premise, In-Cloud, Hybrid — все возможные варианты инсталляции	Только on-premise, отсутствует собственное облако

Кейсы

- Пивоваренный завод
- Химическая промышленность
- Хлебокомбинат
- Машиностроительный завод
- Нефтегазовая компания
- Крупная металлургическая компания

11.07.2022

Спасибо за внимание!

Артем Избаенков
член правления АРСИБ
член ISDEF

+7 (969) 280-21-59
Telegram @dnk_arty

it.tula@gmail.com
izbaenkov.ru