



Check Point
SOFTWARE TECHNOLOGIES LTD



KAZAKHTELECOM
Business

СЕРВИСЫ **КАЗАХТЕЛЕКОМА** НА БАЗЕ РЕШЕНИЙ **CHECK POINT**

Максут Молдабасов | Руководитель направления по работе с
провайдерами связи, Middle Comm.

НОВАЯ МОДЕЛЬ ПРЕДОСТАВЛЕНИЯ УСЛУГ MSSP

- СЛОЖНО ОБСЛУЖИВАЕМОЕ;
- СЛОЖНО ЗАМЕНЯЕМО;
- УСТАРЕВАЮЩЕЕ;
- CAPEX.



FIREWALL



AntiDDoS

- ЛЕГКО МАСШТАБИРУЕМОЕ;
- ЛЕГКО ОБНОВЛЯЕМОЕ;
- ТЕХНИЧЕСКАЯ ПОДДЕРЖКА 24/7;
- OPEX.



FIREWALL



AntiDDoS



Виртуальные сервисы
на стороне у провайдера

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ



FIREWALL ПО ПОДПИСКЕ Инфраструктура безопасности

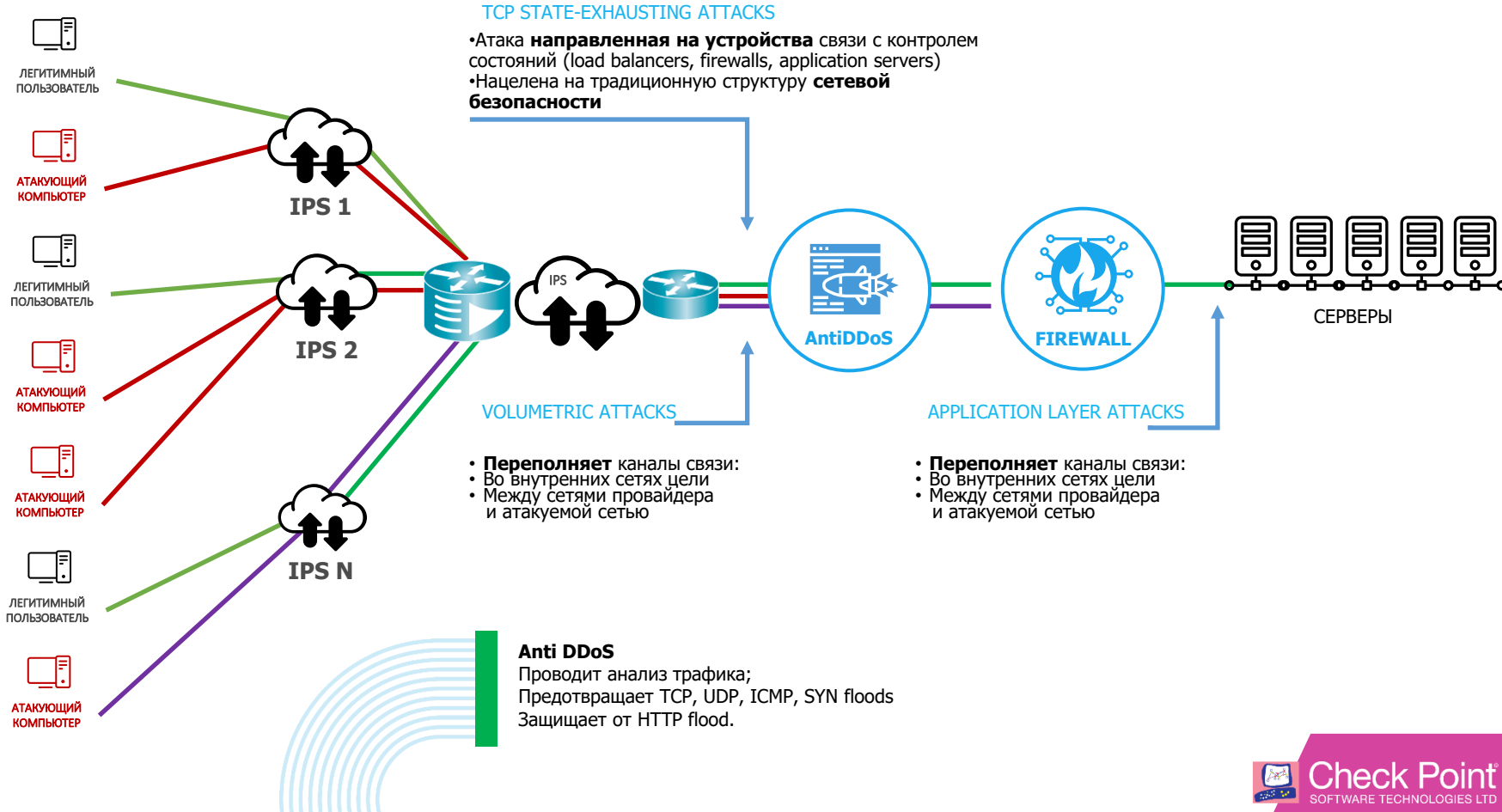
- Межсетевое экранирование (NGFW);
- Обнаружение и предотвращение вторжений (IPS);
- Контроль приложений (APCL);
- Контроль передачи файлов (ContentAwareness);
- Сетевой антивирус (AV);
- Фильтрация URL-адресов (URLF);
- Обнаружение и предотвращение сетевых аномалий и вредоносного трафика (Anti-bot);
- - Расшифровывание HTTPS трафика (HTTPS Inspection).

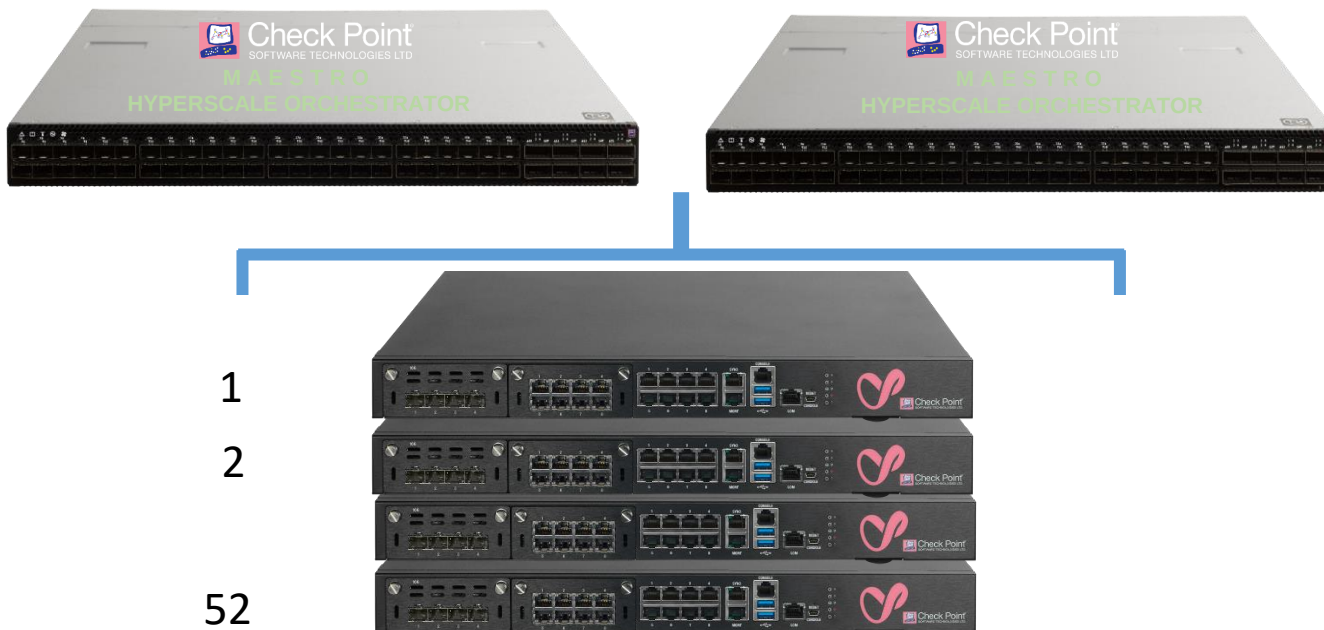


AntiDDoS ПО ПОДПИСКЕ Инфраструктура безопасности

- Мониторинг и обнаружение вредоносного трафика;
- Гибкий механизм обнаружения;
- Поддержка BGP и BGP flow spec или BGP BH Community (RFC 5575);
- Визуализации информации о трафике;
- Защиту от популярных DDoS-атак на уровнях L3–L5 OSI;
- Обеспечение непрерывного функционирования сервисов Клиента в условиях атаки;
- Отчеты о каждой атаке с графиками, статистикой, источниками, примерами атакующего трафика.

СХЕМА ЗАЩИТЫ





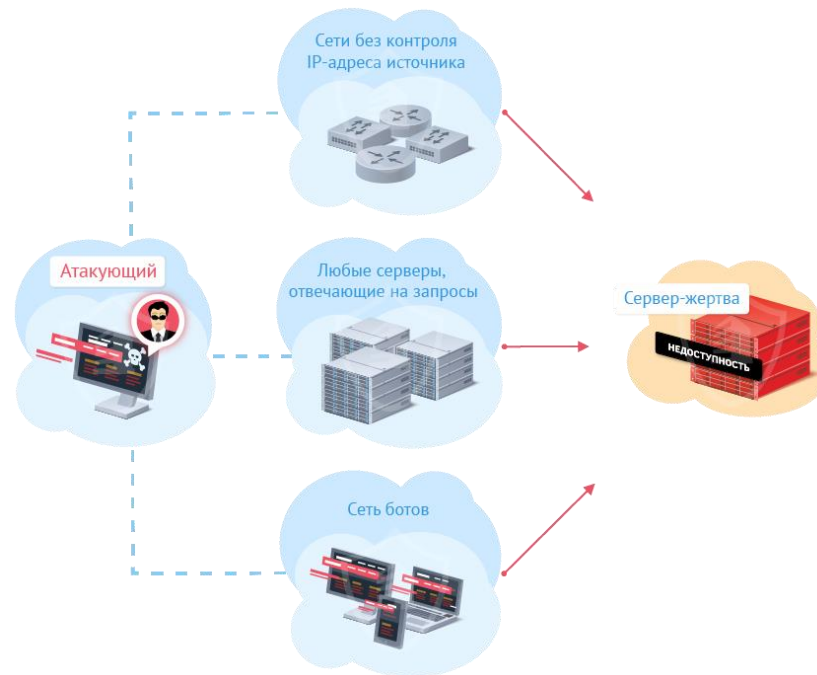
Gateway Consolidation

Управление несколькими логическими шлюзами на основе
ЕДИНОЙ СИСТЕМЫ для МАКСИМАЛЬНОЙ ЭФФЕКТИВНОСТИ

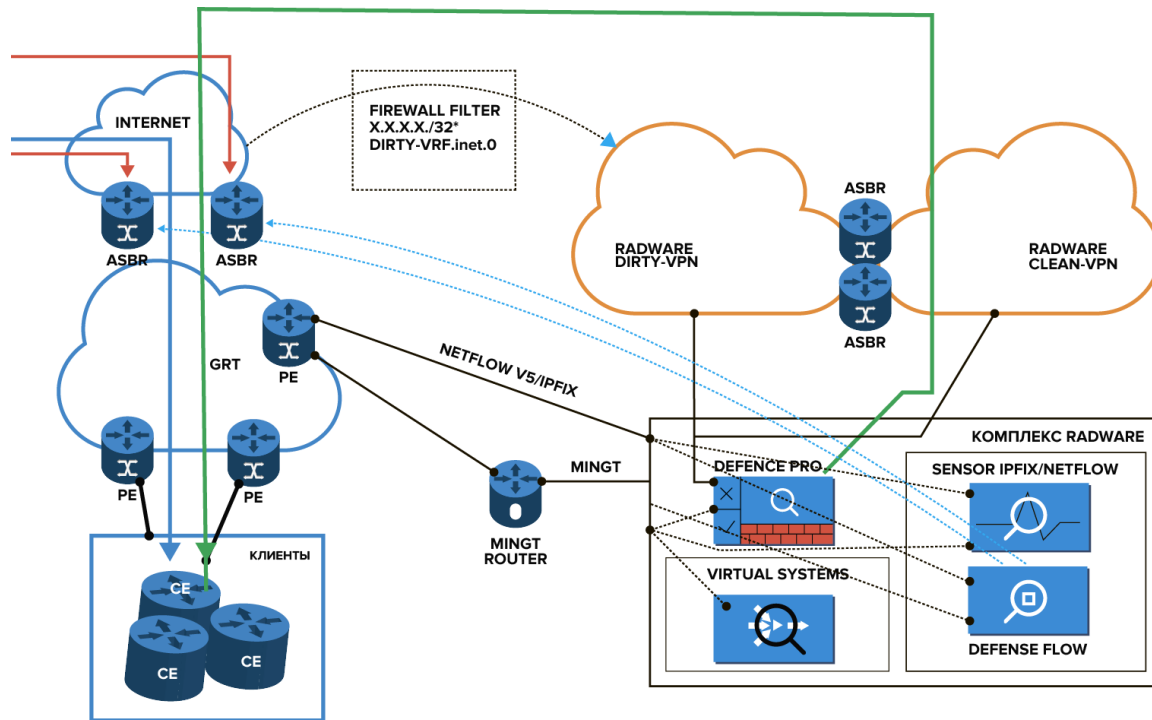
ЧТО ТАКОЕ DDoS АТАКА ?

- 1 Злоумышленник отправляет лавинные запросы из нескольких взломанных систем.
- 2 Пытается полностью занять интернет-канал и истощить ресурсы ОЗУ компании-жертвы. Конечная цель состоит в выводе из строя систем такой компании и прерывании ее бизнес-процессов

Распределенная атака типа «отказ в обслуживании», или DDoS— бомбардировка центрального сервера одновременными запросами данных.

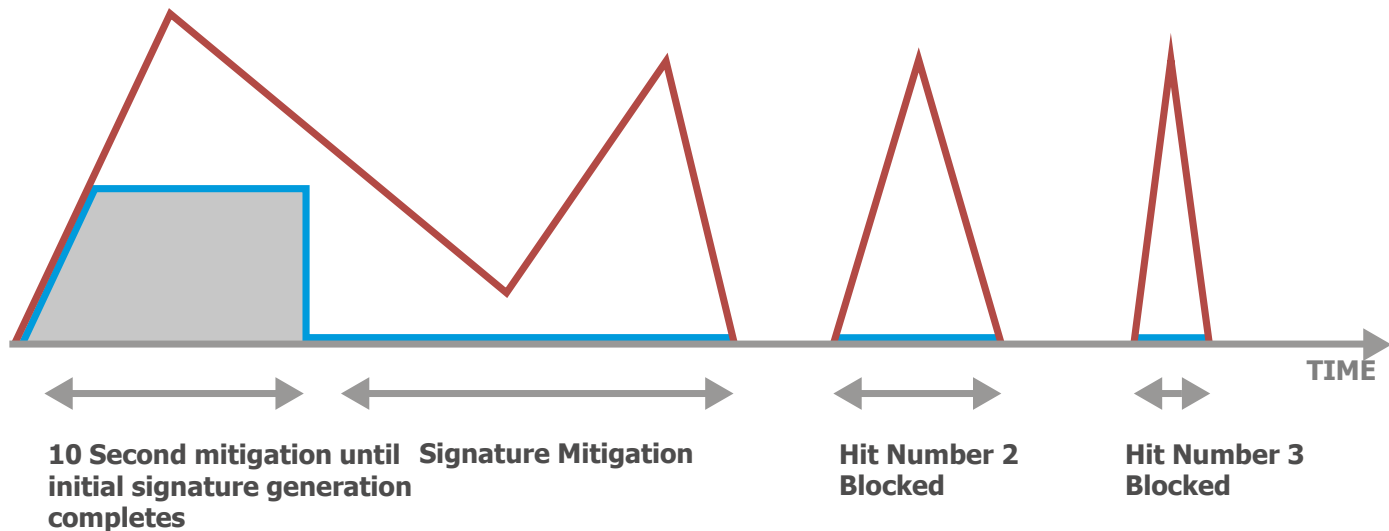


СТРУКТУРНАЯ СХЕМА СЕРВИСА ЗАЩИТЫ ОТ DDOS АТАК В АО «КАЗАХТЕЛЕКОМ»



СТАНДАРТНАЯ DDOS АТАКА
МАСШТАБНАЯ DDOS АТАКА
ОЧИЩЕННЫЙ ТРАФИК
РЕГУЛЯРНЫЙ ТРАФИК

МГНОВЕННОЕ СТРАБАТЫВАНИЕ ЗАЩИТЫ



— **Attack Traffic**

— **Attack Traffic After Mitigation**

Сразу: Фильтр трафика на первые 10 сек для защиты пока генерируется сигнатура

+ 10 секунд: Сигнатура автоматически применяется для блокировки атаки

+ 8 секунд : Сигнатура оптимизируется для уменьшения ложных срабатываний



ПОВЕДЕНЧЕСКИЙ АНАЛИЗ, ОПИРАЮЩИЙСЯ КАК ЗАВИСЯЩИЕ ОТ СКОРОСТИ ПАРАМЕТРЫ, ТАК И НА НЕ ЗАВИСЯЩИЕ

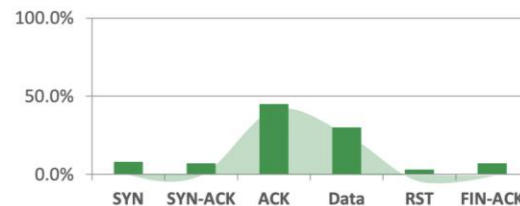
**ВСПЛЕСК
ТРАФИКА**

Анализ скоростей



+

Анализ распределения флагов TCP



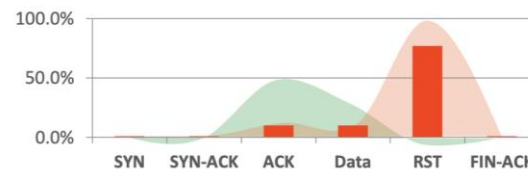
**RST АТАКА
RST FLOOD**

Анализ скоростей



+

Анализ распределения флагов TCP



Forensics View: 1001 Last Generation Date: 19.11.2021, 22:07:10 Forensics Snapshot ID: net_2021-11-19_16407-12

Start Time	End Time	Attack Details	Destination IP Address	Destination Port	Direction
19.11.2021, 22:07:08	19.11.2021, 22:07:08	Initial Attack ID: 21291-16887-101	Multiple	Multiple	Unknown
19.11.2021, 22:06:50	19.11.2021, 22:06:50	Threat Category: Subverted DoS	Multiple	Multiple	Unknown
19.11.2021, 22:06:55	19.11.2021, 22:06:55	Destination IP Address: Subverted DoS	Multiple	Multiple	Unknown
19.11.2021, 22:06:50	19.11.2021, 22:06:50	Destination Port: Subverted DoS	Multiple	Multiple	Unknown
19.11.2021, 22:06:45	19.11.2021, 22:06:45	Source IP Address: Subverted DoS	Multiple	Multiple	Unknown
19.11.2021, 22:06:39	19.11.2021, 22:06:39	Source Port: Subverted DoS	Multiple	Multiple	Unknown
19.11.2021, 22:06:34	19.11.2021, 22:06:34	Attack Name: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:06:23	19.11.2021, 22:06:23	Attack Type: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:06:23	19.11.2021, 22:06:23	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:06:08	19.11.2021, 22:06:08	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:06:23	19.11.2021, 22:06:23	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:06:08	19.11.2021, 22:06:08	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:06:08	19.11.2021, 22:06:08	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:06:08	19.11.2021, 22:06:08	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:06:08	19.11.2021, 22:06:08	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:53	19.11.2021, 22:05:53	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:53	19.11.2021, 22:05:53	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:42	19.11.2021, 22:05:42	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:37	19.11.2021, 22:05:37	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:36	19.11.2021, 22:05:36	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:36	19.11.2021, 22:05:36	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:36	19.11.2021, 22:05:36	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:20	19.11.2021, 22:05:20	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:14	19.11.2021, 22:05:14	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:07	19.11.2021, 22:05:07	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:05:01	19.11.2021, 22:05:01	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown
19.11.2021, 22:04:55	19.11.2021, 22:04:55	Behavioral DoS: network flood IPv4 UDP	Multiple	Multiple	Unknown

рис.1 снимок экрана с отчета Forensics

Forensics View: 1001 Last Generation Date: 19.11.2021, 22:07:10 Forensics Snapshot ID: net_2021-11-19_16407-12

Start Time	End Time	Time	Source IP Address	Source Port	Destination IP Address	Destination Port	Direction
19.11.2021, 22:07:08	19.11.2021, 22:07:08						Multiple
19.11.2021, 22:06:50	19.11.2021, 22:06:50		173.194.79.102	443		52451	Multiple
19.11.2021, 22:06:55	19.11.2021, 22:06:55		173.194.79.102	443		52451	Multiple
19.11.2021, 22:06:50	19.11.2021, 22:06:50						Multiple
19.11.2021, 22:06:45	19.11.2021, 22:06:45						Multiple
19.11.2021, 22:06:39	19.11.2021, 22:06:39						Multiple
19.11.2021, 22:06:34	19.11.2021, 22:06:34						Multiple
19.11.2021, 22:06:23	19.11.2021, 22:06:23						Multiple
19.11.2021, 22:06:23	19.11.2021, 22:06:23						Multiple
19.11.2021, 22:06:08	19.11.2021, 22:06:08						Multiple
19.11.2021, 22:06:23	19.11.2021, 22:06:23						Multiple
19.11.2021, 22:06:08	19.11.2021, 22:06:08						Multiple
19.11.2021, 22:06:08	19.11.2021, 22:06:08						Multiple
19.11.2021, 22:06:08	19.11.2021, 22:06:08						Multiple
19.11.2021, 22:05:53	19.11.2021, 22:05:53						Multiple
19.11.2021, 22:05:53	19.11.2021, 22:05:53						Multiple
19.11.2021, 22:05:42	19.11.2021, 22:05:42						Multiple
19.11.2021, 22:05:37	19.11.2021, 22:05:37						Multiple
19.11.2021, 22:05:36	19.11.2021, 22:05:36						Multiple
19.11.2021, 22:05:36	19.11.2021, 22:05:36						Multiple
19.11.2021, 22:05:36	19.11.2021, 22:05:36						Multiple
19.11.2021, 22:05:20	19.11.2021, 22:05:20						Multiple
19.11.2021, 22:05:14	19.11.2021, 22:05:14						Multiple
19.11.2021, 22:05:07	19.11.2021, 22:05:07						Multiple
19.11.2021, 22:05:01	19.11.2021, 22:05:01						Multiple
19.11.2021, 22:04:55	19.11.2021, 22:04:55						Multiple

рис.2 снимок экрана вкладки "Sampled Data" отчета Forensics

На примере ниже рассмотрим атаку, которая была 19 ноября на защищаемый объект в системе anti-DDoS (рис.1, рис.2). Атака содержала UDP Flood и продолжалась более 10 минут. Всё это время система отражала атаку и защищала объект от потери интернет соединения во время прямой трансляции.

LoT BOTNETS



Информация в реальном времени для блокировки активных злоумышленников

Machine learning



Защита от взрывных атак на основе поведения

ENCRYPTED ATTACKS



Встроенная многоуровневая защита SSL-Flood с нулевой задержкой

DNC ATTACKS



Автоматическая поведенческая защита DNS для авторитетных и рекурсивных DNS

ПРЕИМУЩЕСТВА РЕШЕНИЯ CHECK POINT

ОПТИМИЗАЦИЯ ЗАТРАТ, ПЕРЕМЕЩЕНИЕ ЗАТРАТ ИЗ КАПИТАЛЬНЫХ В ОПЕРАЦИОННЫЕ, ДОСТУПНАЯ ЗАЩИТА МАЛЫХ ОФИСОВ И ФИЛИАЛОВ.



- ОПТИМИЗАЦИЯ ЗАТРАТ НА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВОГО ПЕРИМЕТРА, ОТСУТСТВИЕ КАПИТАЛЬНЫХ ЗАТРАТ;



- ОПТИМИЗАЦИЯ ЗАТРАТ НА СОДЕРЖАНИЕ ВЫСОКОКВАЛИФИЦИРОВАННЫХ ИНЖЕНЕРОВ И АДМИНИСТРАТОРОВ;



- ВОЗМОЖНОСТЬ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ СЕТЕВОГО ПЕРИМЕТРА ОФИСОВ, УДАЛЕННЫХ ФИЛИАЛОВ БЕЗ УСТАНОВКИ ДОРОГОСТОЯЩЕГО ОБОРУДОВАНИЯ И ЗАТРАТ НА ЕГО ОБСЛУЖИВАНИЕ;



- ЗАЩИТА ПЕРИМЕТРА ПО ПОДПИСКЕ, БЕЗ ДОПОЛНИТЕЛЬНЫХ ЗАТРАТ НА ВНЕДРЕНИЕ ОБОРУДОВАНИЯ, ПОЛУЧАЯ РЕШЕНИЕ СРАЗУ А ОПЛАЧИВАЯ ПОМЕСЯЧНО.

