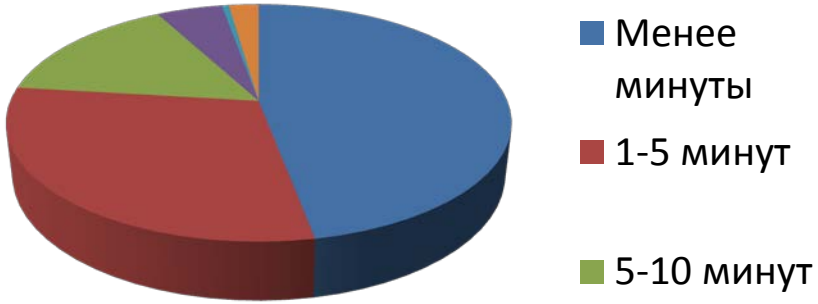
Механизм реализации защиты от DDoS-атак в ПАО «ВымпелКом».

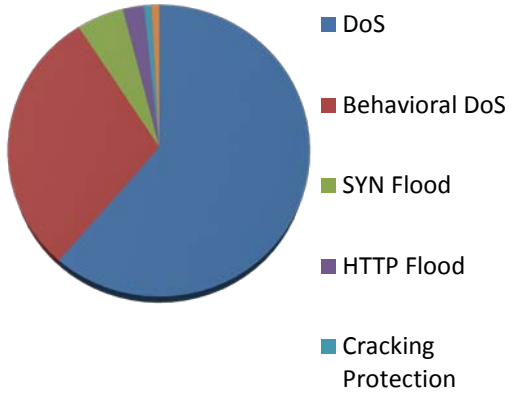
Центр очистки интернет-трафика

Статистические данные

Всего более 9 миллионов событий за год

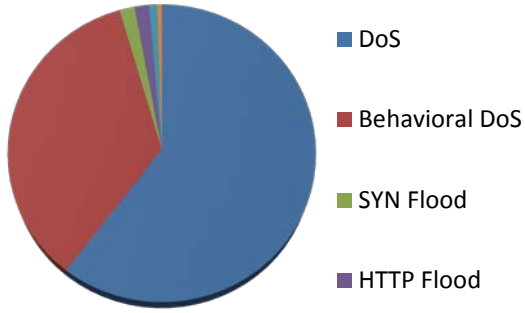


Распределение по количеству пакетов



Тип атаки	Количество пакетов	Объем траффика
Anomalies	34,624,569,158	101,335 Терабит
DoS	2,686,412,544	3,966 Терабит
Behavioral DoS	1,299,009,374	2,299 Терабит
SYN Flood	225,990,839	106 Терабит
HTTP Flood	101,428,453	103 Терабит
Cracking Protection	36,614,420	57 Терабит
Anti Scanning	36,236,841	32 Терабит
Intrusions	145,475	0.5 Терабит
Всего	**407,478,650,675**	**1,078,983 Терабит**

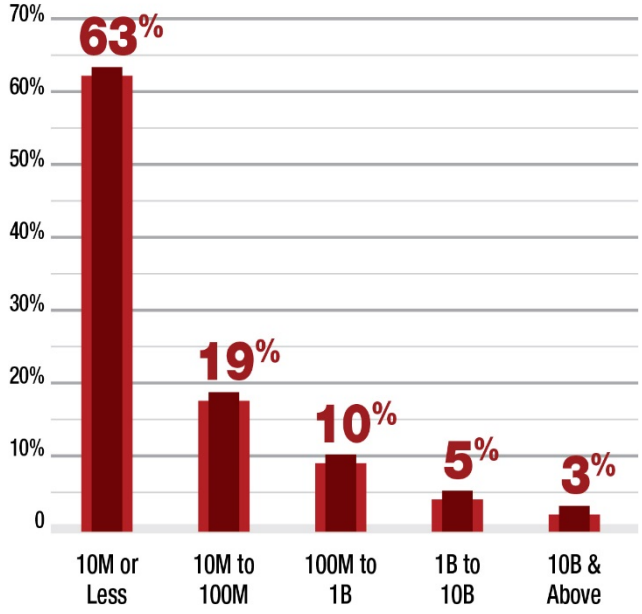
Распределение по объему траффика



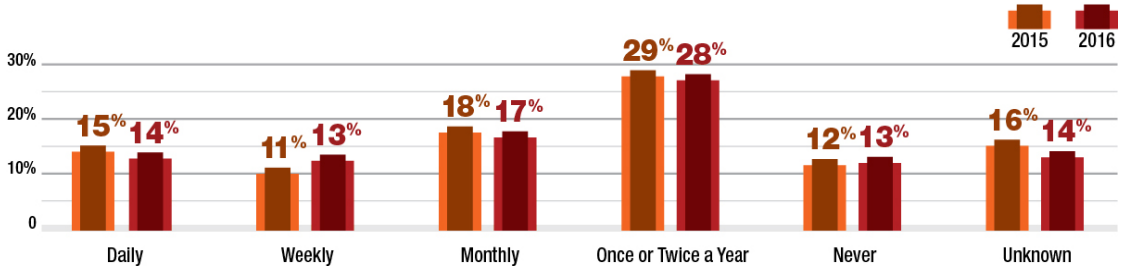
***Приведены усредненные данные по 1 клиенту за год.**

Мировая статистика

Распределение атак (количество) по полосе



Распределение атак (количество) по частоте



На сколько времени хватает человеческих ресурсов (опрос по миру)

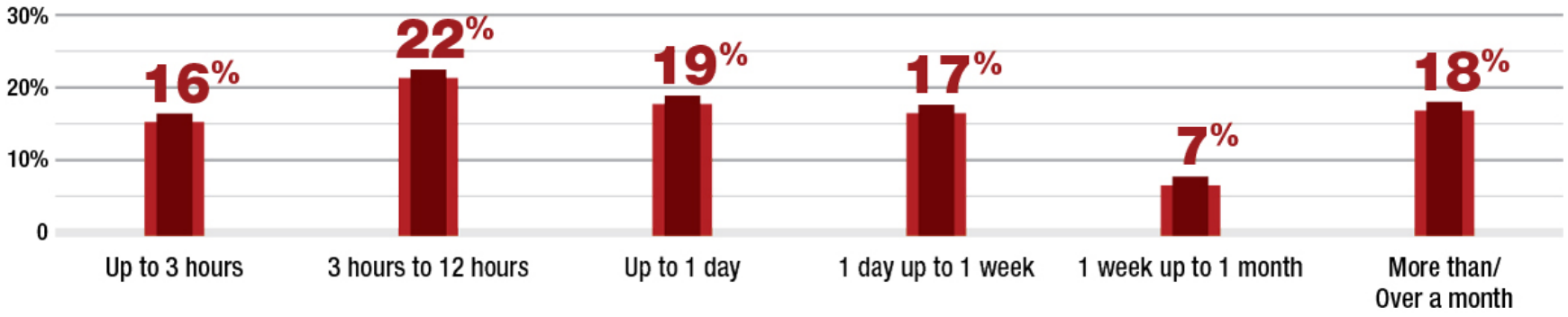
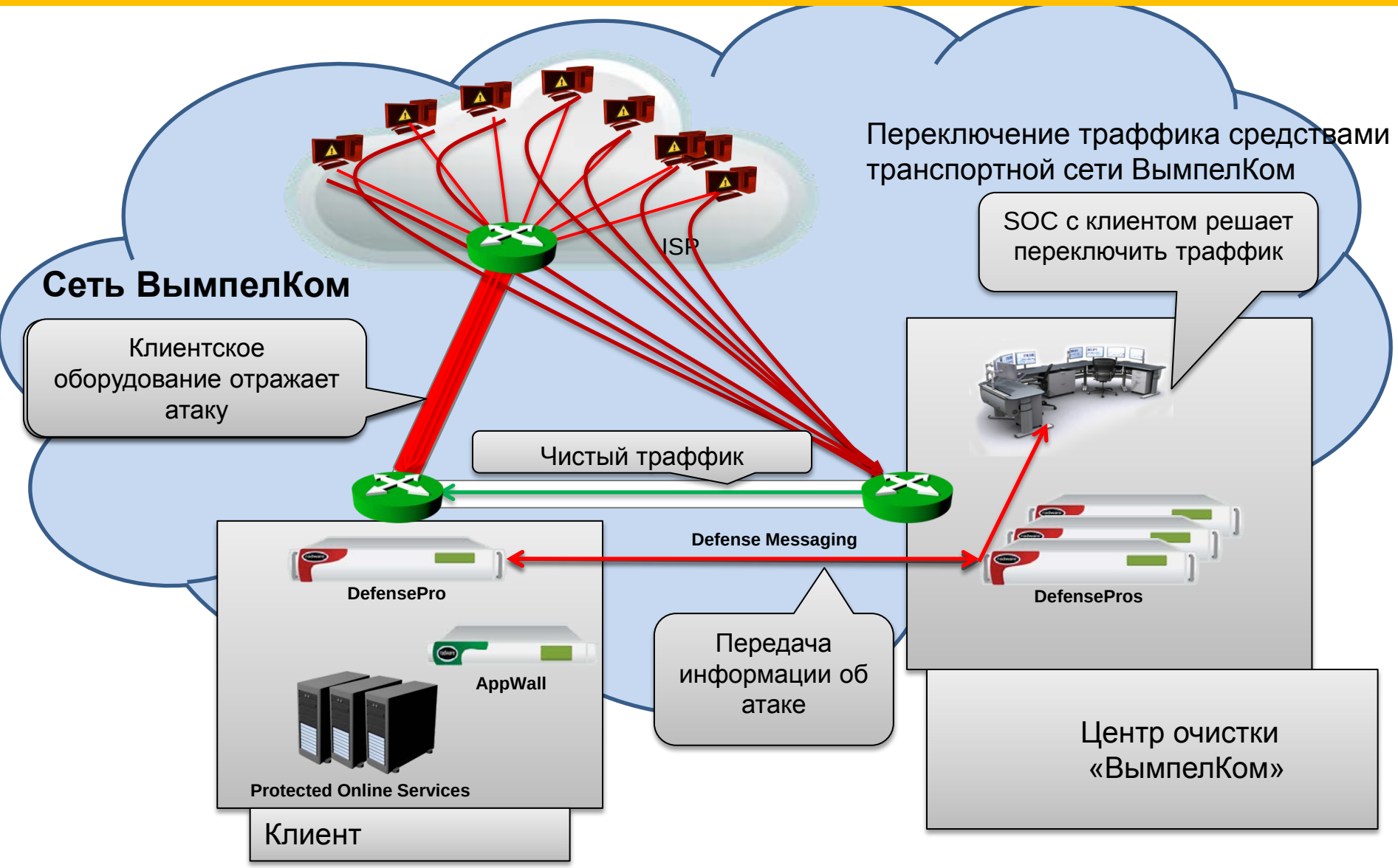


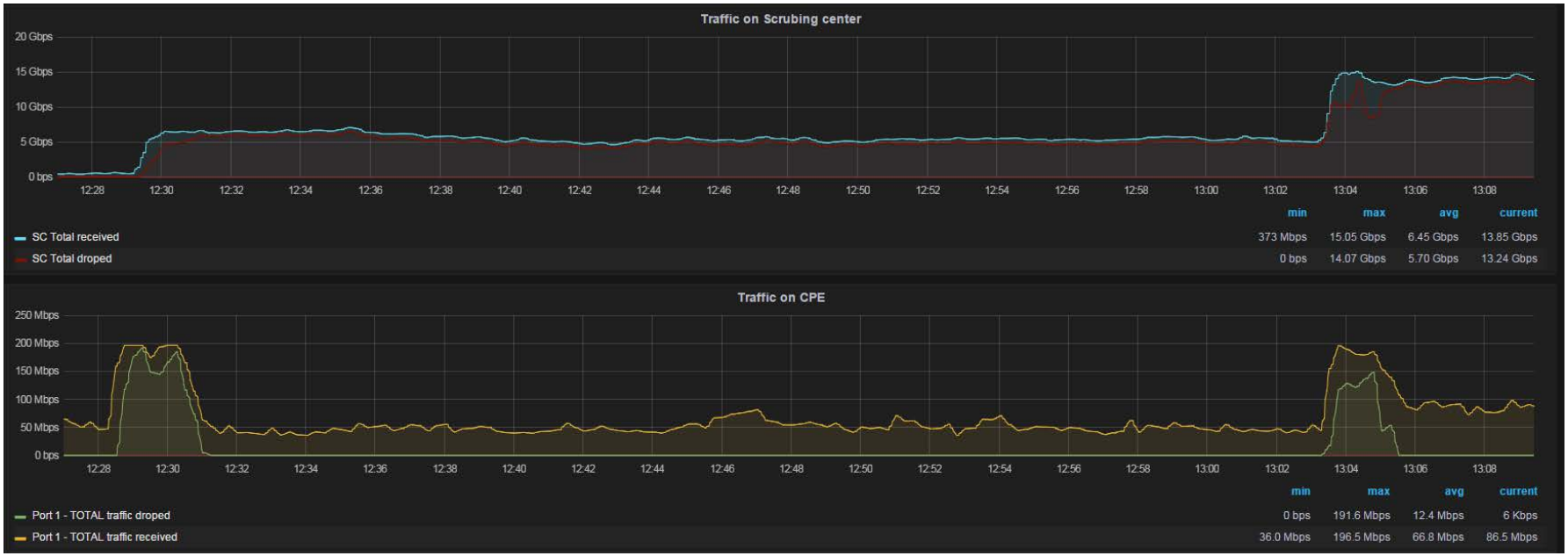
Схема работы программно–аппаратного комплекса



Характеристики решения

- Начало отражения атаки через 18 секунд (на порядки быстрее конкурентных предложений);
- Отсутствие влияния на легитимных пользователей
- Борьба с самым широким на рынке спектром атак (от Layer 4 до шифрованных атак и атак на уровне WEB)
- Автоматическое создание профиля интернет-трафика ресурса компании и правил фильтрации «вредоносного» трафика на его основе;
- Не требует участия персонала клиента в момент атаки
- Возможность отражения атак под SSL без выноса сертификатов за межсетевой экран
- Самостоятельное обучение оборудования;
- Автоматическое переключение траффика на Центр Очистки;

Характеристики решения на примере атаки



- Начало атаки - ~12:28:15
- Начало отражения на клиентском устройстве – ~12:28:30
- Начало переключения на ЦО - ~12:29:30
- Траффик полностью переключен на ЦО ~12:30:15
- Изменение вектора атаки, детектирование и отражение новой атаки - ~13:04

Директор по информационной безопасности
ПАО «ВымпелКом»

А. Голубев

avg@beeline.ru