

Нос Ивана Кузьмича

Зачем мы интегрировали наши фаерволы,
и что из этого получилось

POSITIVE TECHNOLOGIES

Алексей Гончаров
algoncharov@ptsecurity.com

15 ЛЕТ ОПЫТА

Обеспечиваем безопасность в масштабах
Сочи-2014, Универсиады-2013 в Казани,
электронных выборов

КАЖДЫЙ ГОД

200+

аудитов
безопасности

200+

обнаружений
уязвимостей
нулевого дня

ЭКСПЕРТИЗА

Находим уязвимости
в промышленности и телекомах

150+

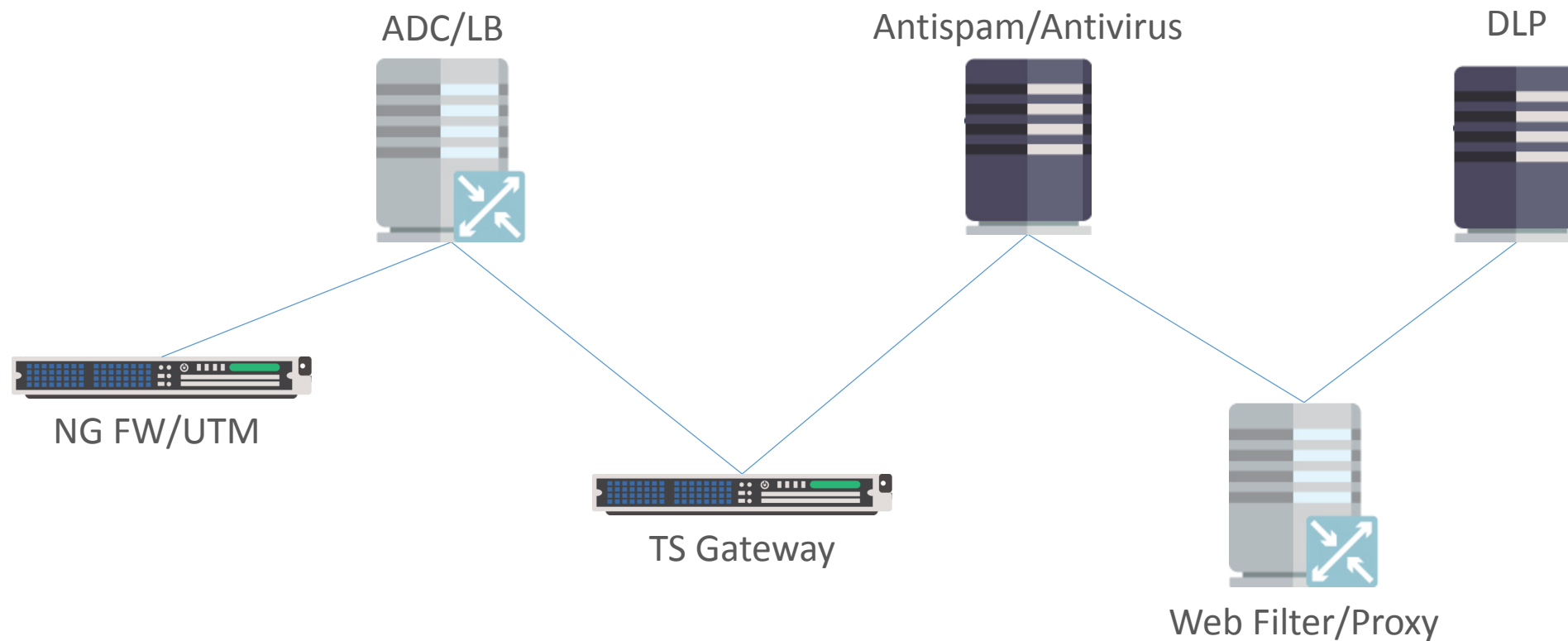
обнаружений
уязвимостей
нулевого дня
в АСУ ТП

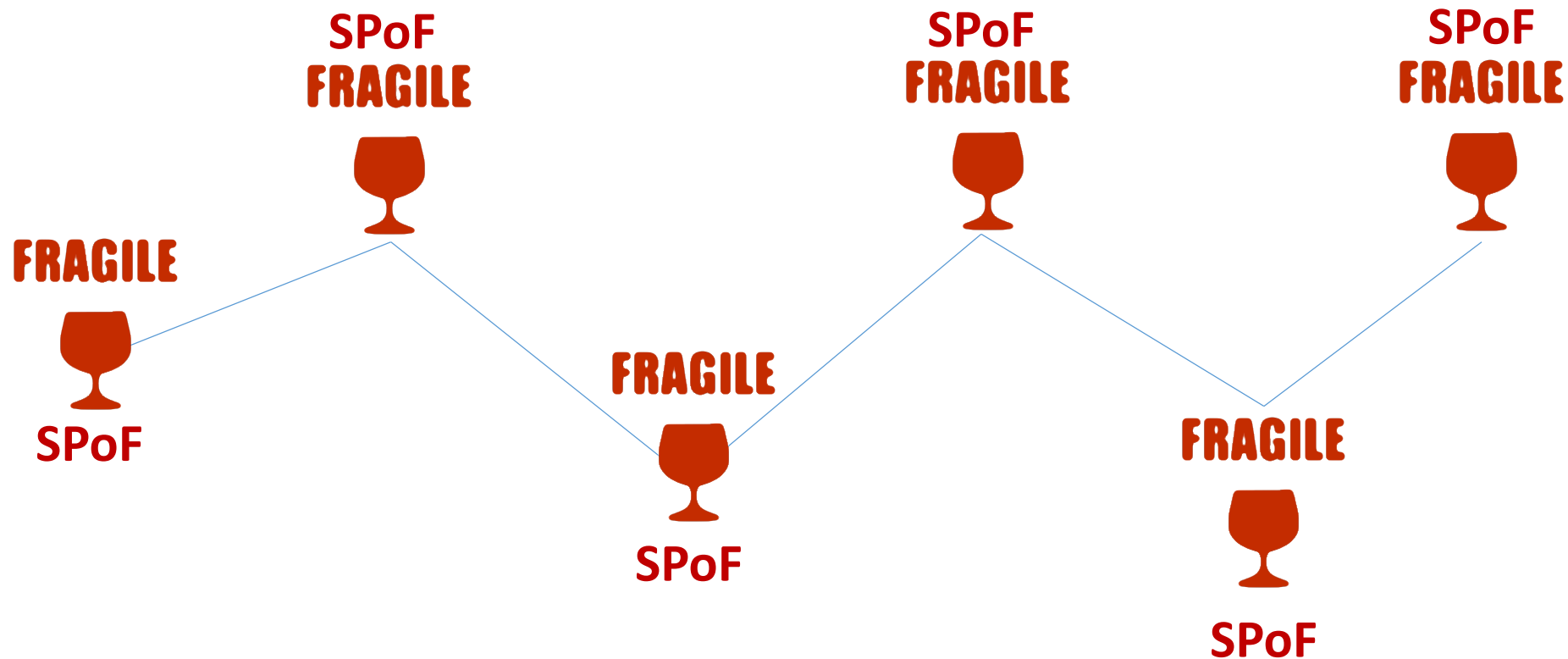
30+

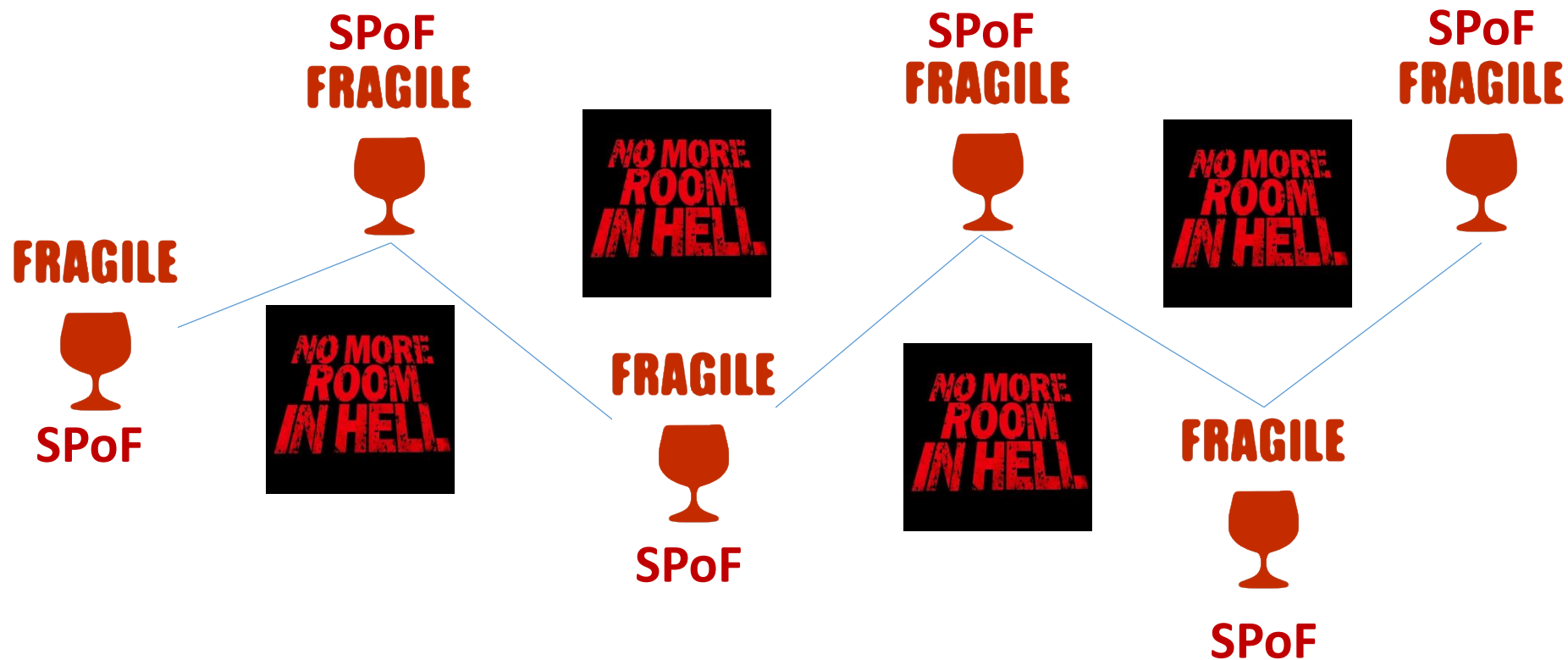
обнаружений
уязвимостей
нулевого дня
в телеком

400+

исследований
безопасности
веб

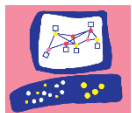




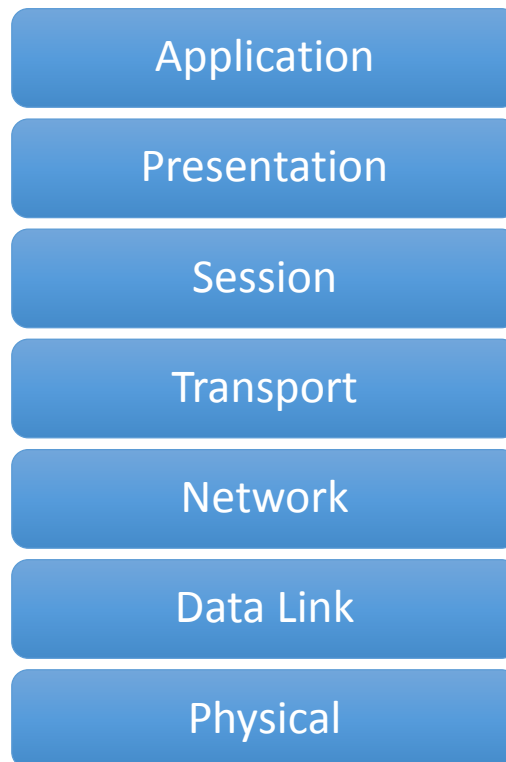




PT Application Firewall



Check Point®
SOFTWARE TECHNOLOGIES LTD.



Remote Code Exec
Bots
Tampering
CSRF
OS Commanding
RFI/LFI/SSI
WebSpam
Pollution
Clickjacking
Evasion
XSS
SlowDOS
L7 DDoS
ShellShock
XXE
SQL Injection
Path Traversal

Атаки на приложения

BEAST
POODLE
SSL Stripping
OpenSSL Heartbleed
UDP Flood
SYN Flood
Smurf
L3/L4 DoS

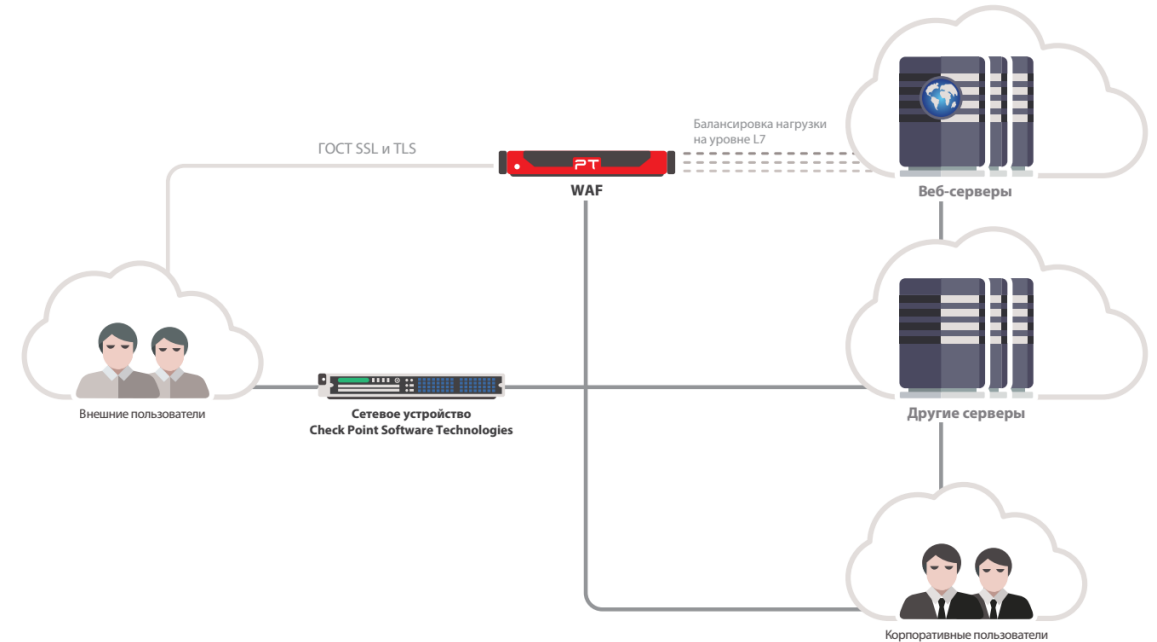
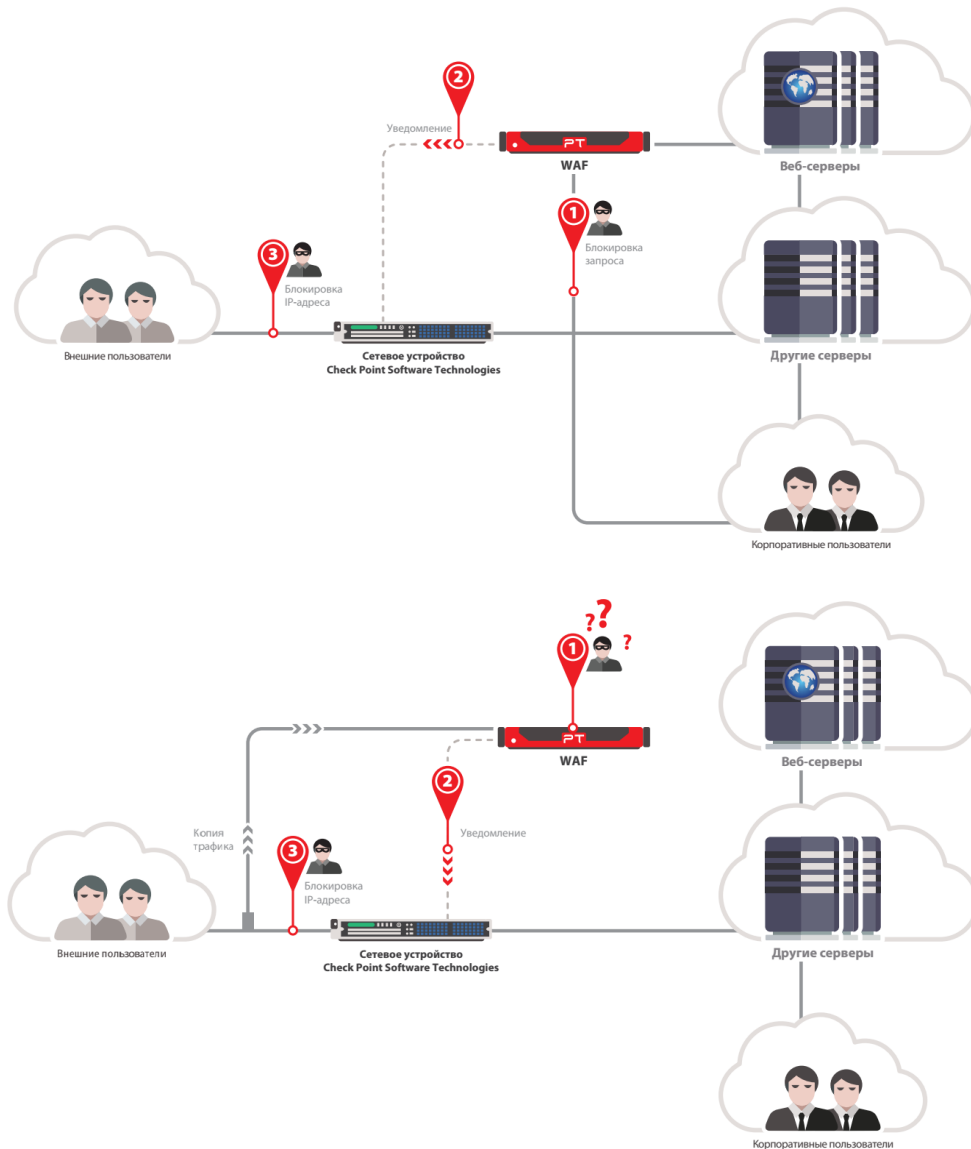
SSL/TLS атаки

ICMP Flood
ARP Spoofing
MAC Flood

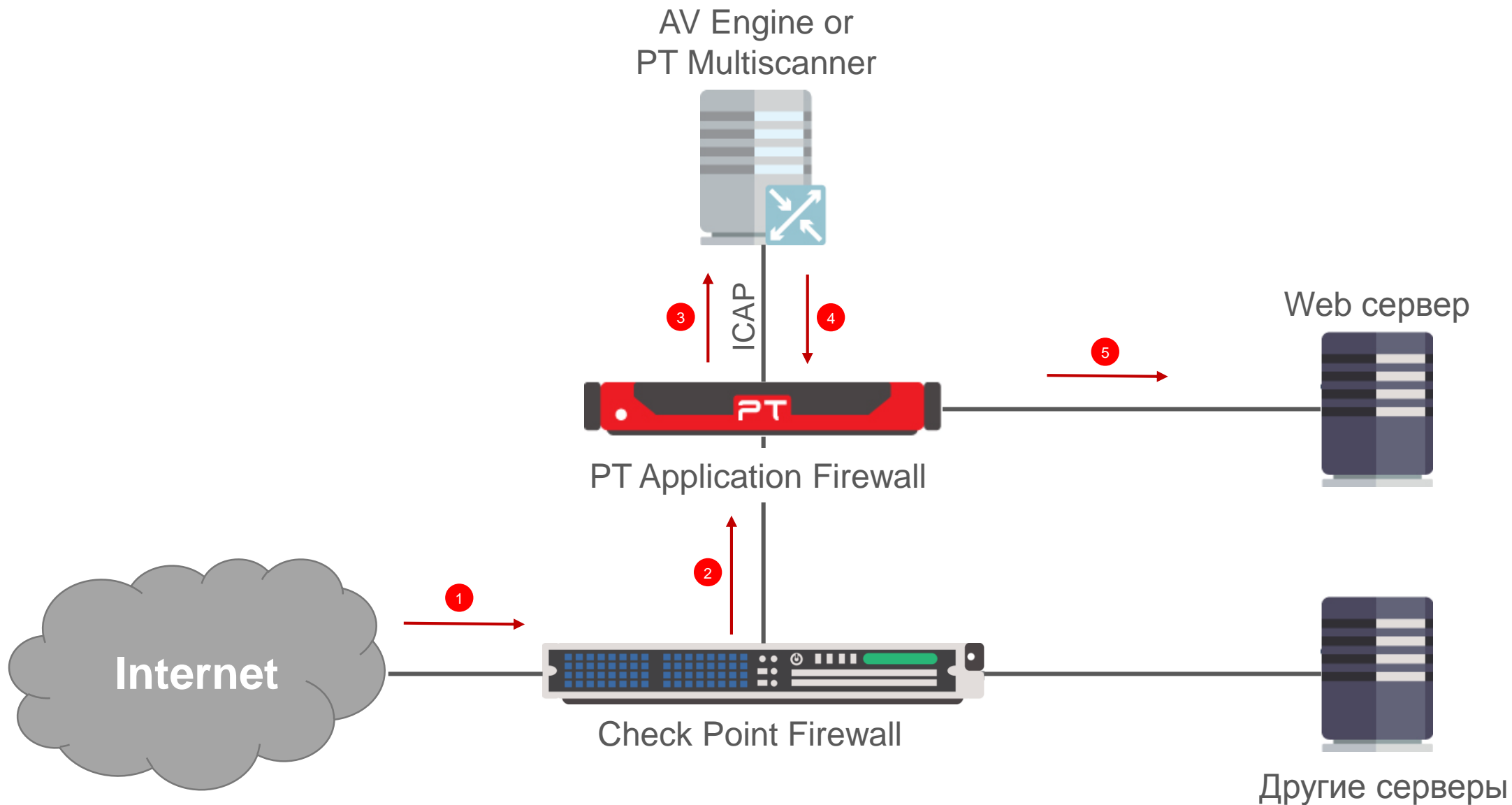
Сетевые атаки

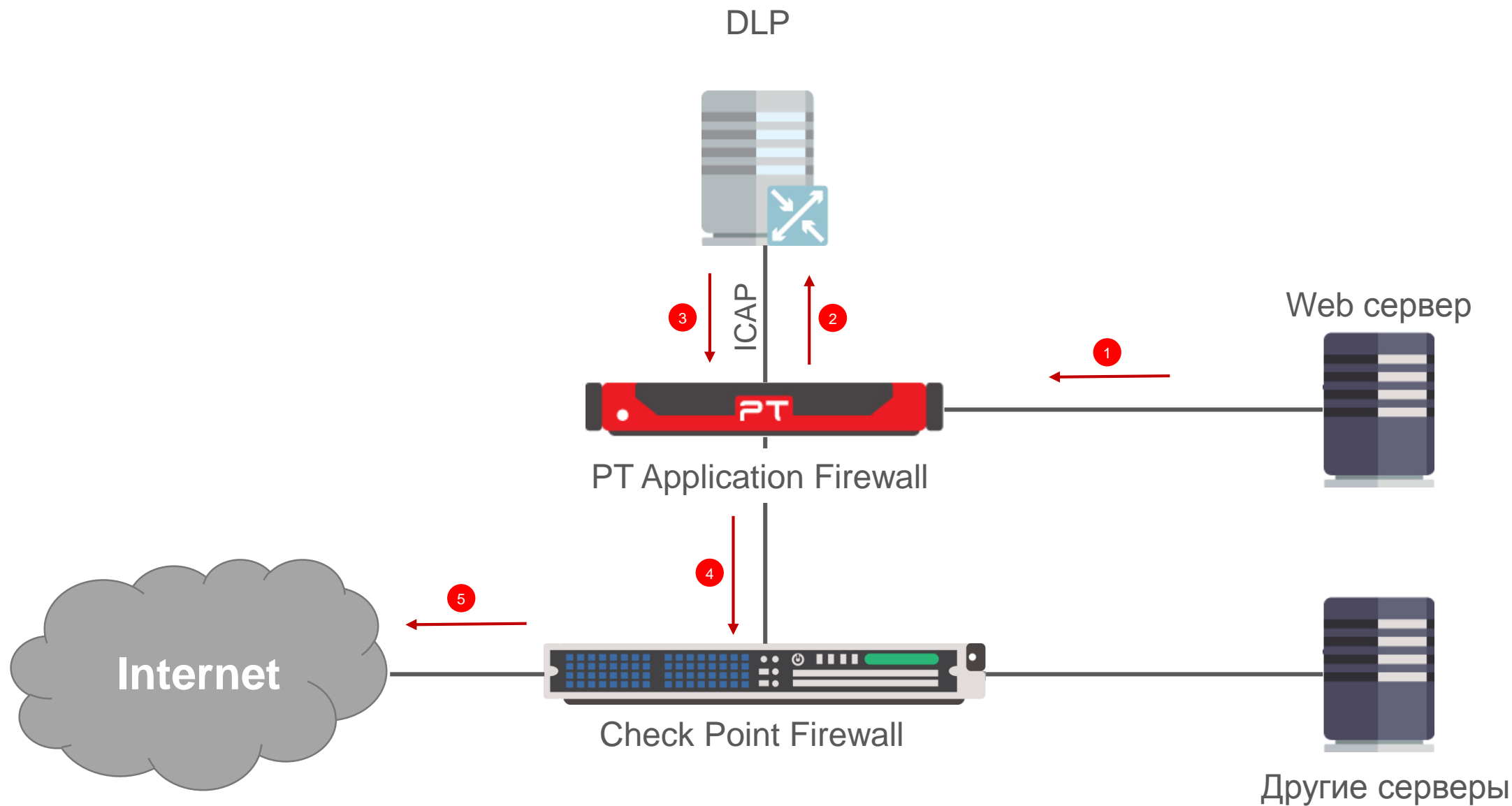
«Вот если бы губы Никанора Ивановича да приставить к носу
Ивана Кузьмича ...»

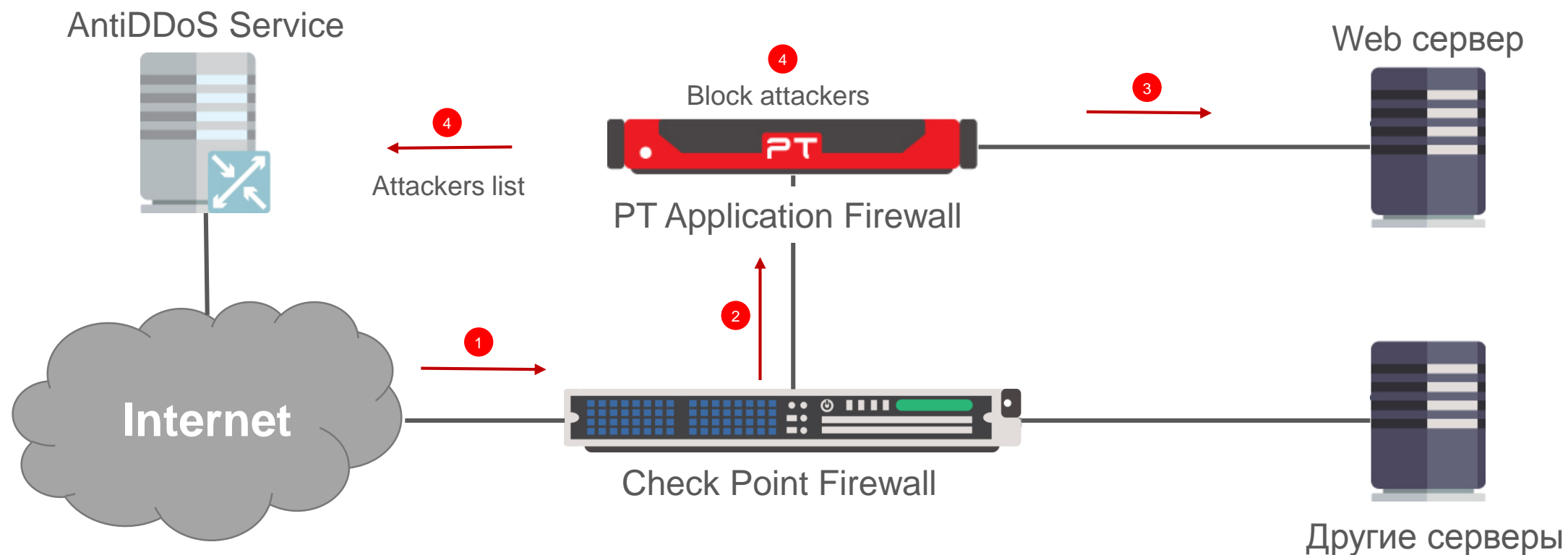
Н. В. Гоголь, "Женитьба"



- + PT AF выявляет атаку на веб-сайт и блокирует ее / уведомляет Check Point об источнике атаки
- + Check Point блокирует запросы от злоумышленника к остальным ресурсам
- + Может использоваться и для защиты от атак на веб-приложения под **GOST SSL/TLS**







Машинное обучение

- Доступ по модели белых списков
- Защита от неизвестных уязвимостей
- Определение скрытых попыток взлома

Минимум False Positive

- Встроенный сканер для поиска уязвимостей
- Инструменты для формирования корреляций
- Визард для исключений прямо на дэшборде



Виртуальные обновления

- Гарантированная защита от уязвимостей
- Идеально для уже работающих сайтов
- Наиболее правильный подход к ИБ

Поведенческий анализ и поиск аномалий

- Определение ботов
- Защита от DDoS атак 7-го уровня
- Контроль аномальной активности (crawlers, scrapping, scanning, etc)

