Нос Ивана Кузьмича

Зачем мы интегрировали наши файрволы, и что из этого получилось

Алексей Гончаров
algoncharov@ptsecurity.com

POSITIVE TECHNOLOGIES

Positive Technologies в цифрах

POSITIVE TECHNOLOGIES

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

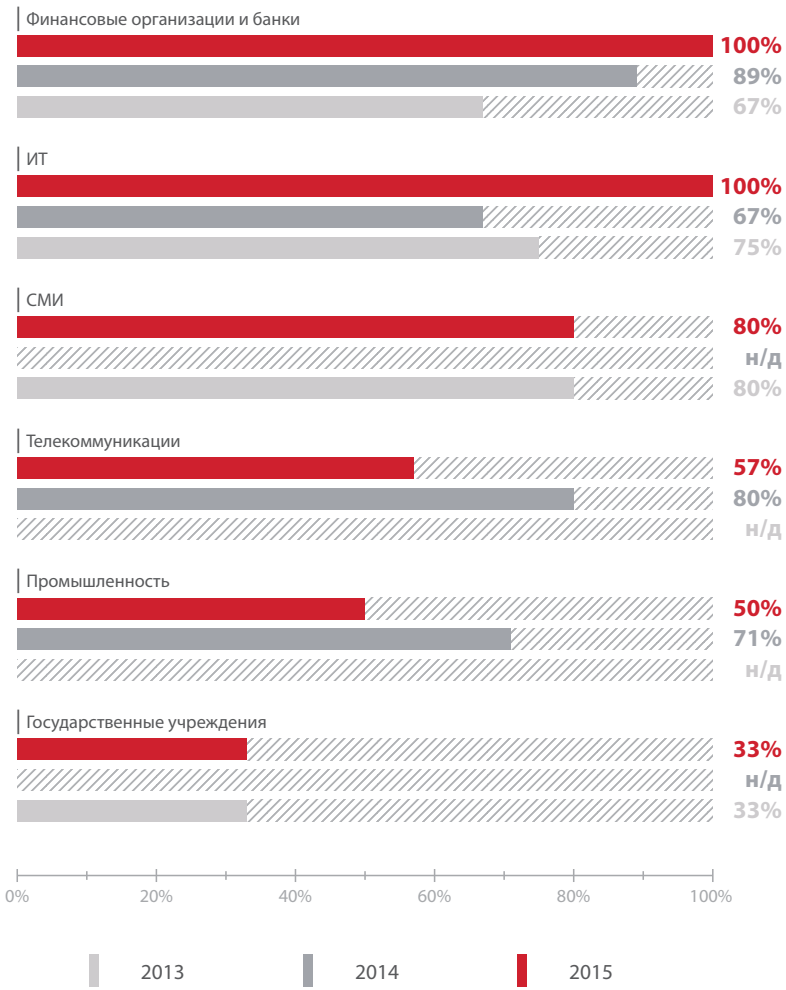
150+ обнаружений уязвимостей нулевого дня в АСУ ТП

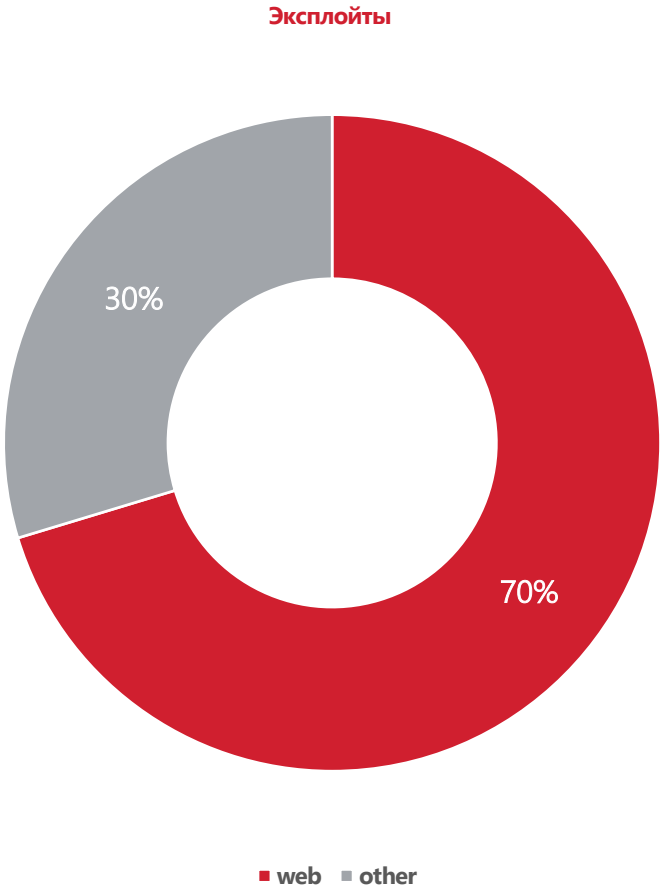
30+ обнаружений уязвимостей нулевого дня в телеком

400+ исследований безопасности веб

Веб – стартовая площадка для атаки

POSITIVE TECHNOLOGIES





На основе данных сайта exploit-db.com

Модель OSI

POSITIVE TECHNOLOGIES

PT Application Firewall

Check Point
SOFTWARE TECHNOLOGIES LTD.

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Remote Code Exec
OS Commanding
Evasion
Tampering
RFI/LFI/SSI
Clickjacking
XSS
Bots
CSRF
WebSpam
Pollution
SlowDOS

Атаки на приложения

L7 DDoS
ShellShock
XXE
SQL Injection
Path Traversal

BEAST
POODLE

SSL/TLS атаки

SSL Stripping
OpenSSL Heartbleed

SYN Flood
UDP Flood
L3/L4 DoS
Smurf

Сетевые атаки

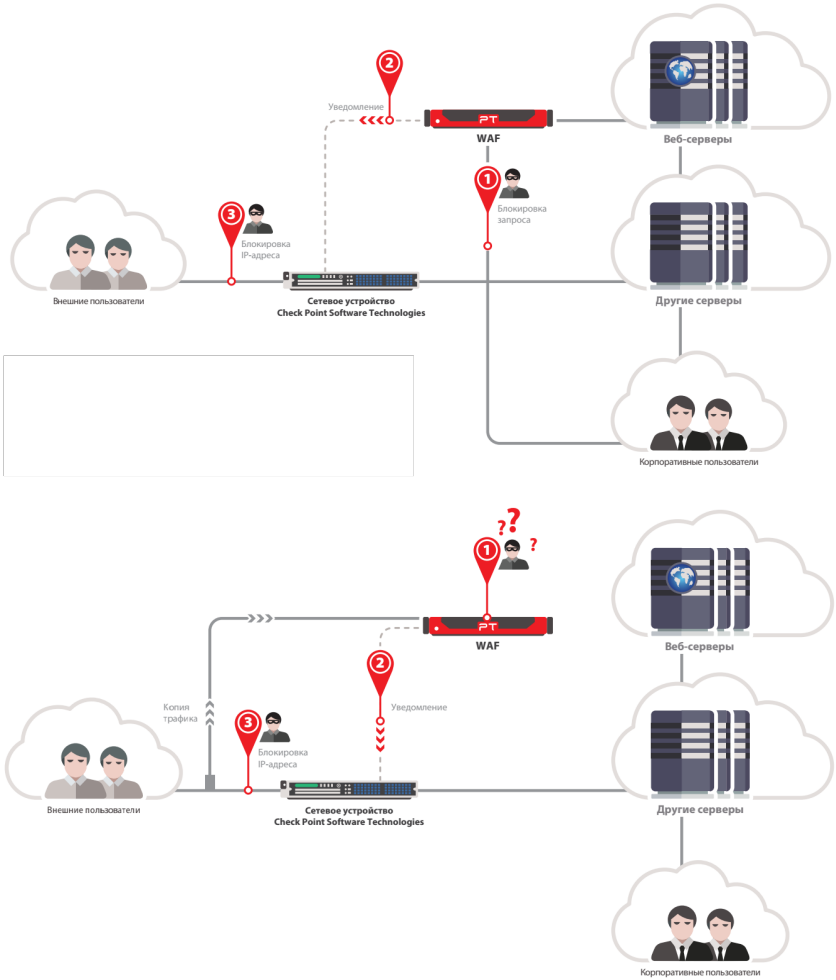
ICMP Flood
ARP Spoofing
MAC Flood

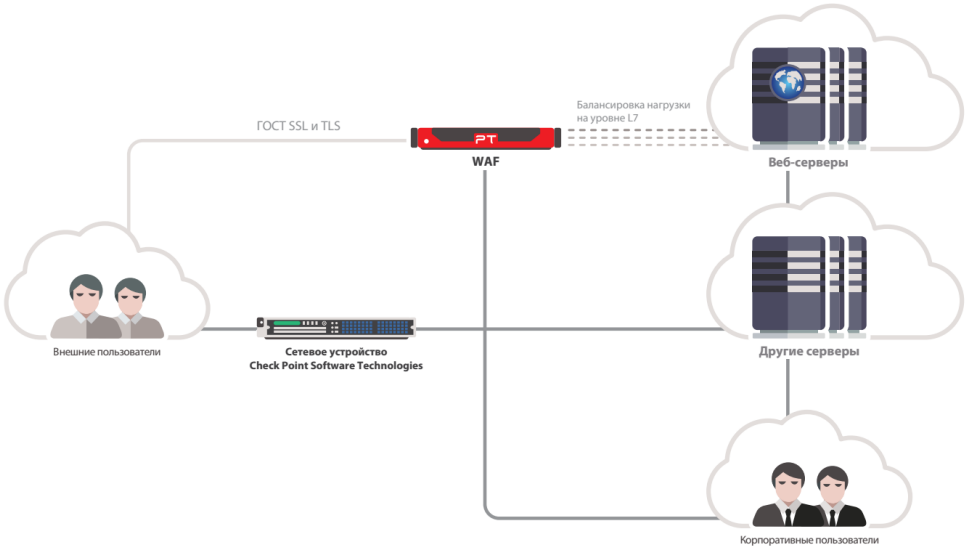
«Вот если бы губы Никанора Ивановича да приставить к носу Ивана Кузьмича ...»

Н. В. Гоголь, "Женитьба"

Схема интеграции

POSITIVE TECHNOLOGIES





+ 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

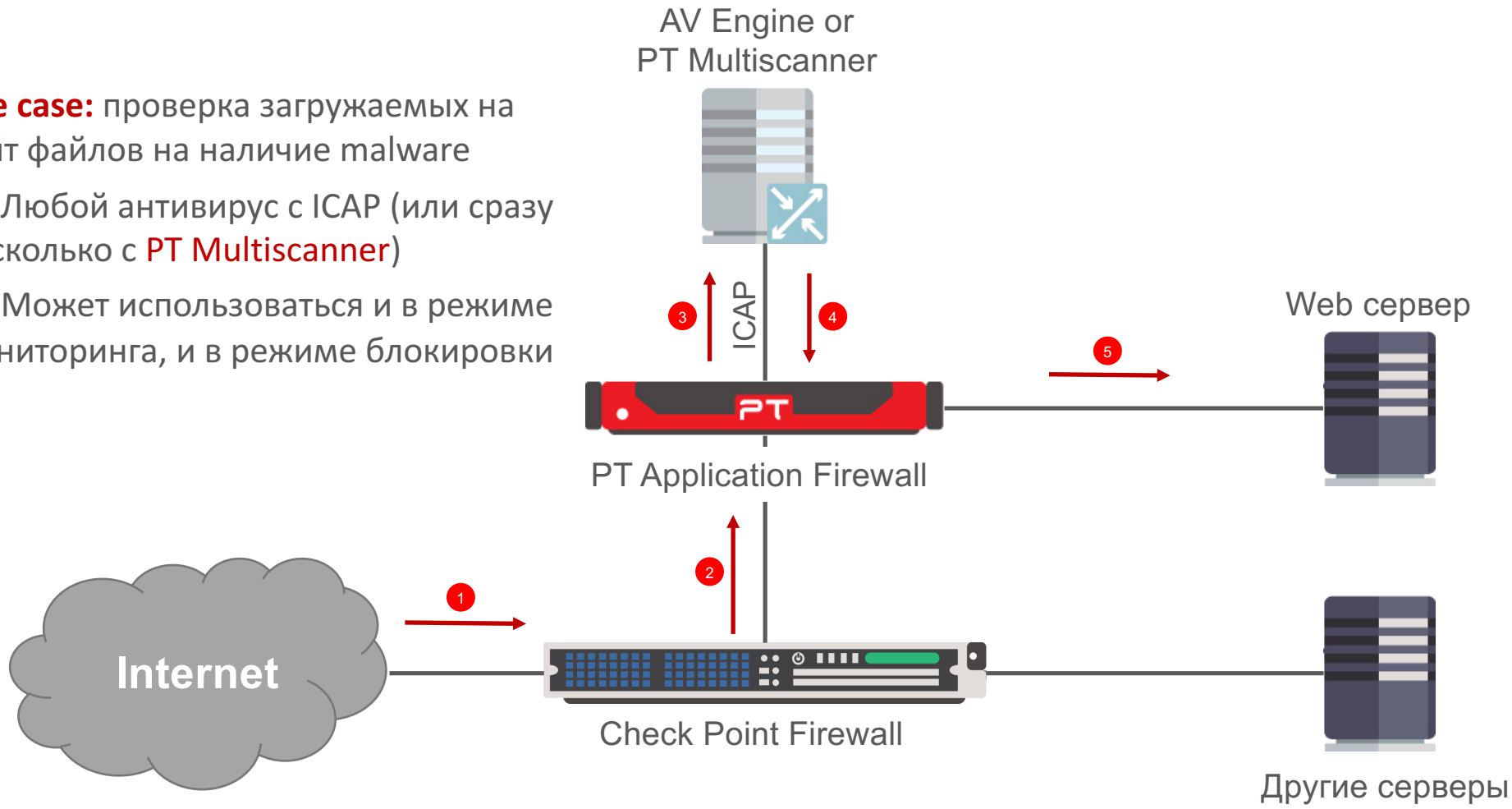
Сценарии использования: AV

POSITIVE TECHNOLOGIES

Use case: проверка загружаемых на сайт файлов на наличие malware

\+ Любой антивирус с ICAP (или сразу несколько с PT Multiscanner)

\+ Может использоваться и в режиме мониторинга, и в режиме блокировки

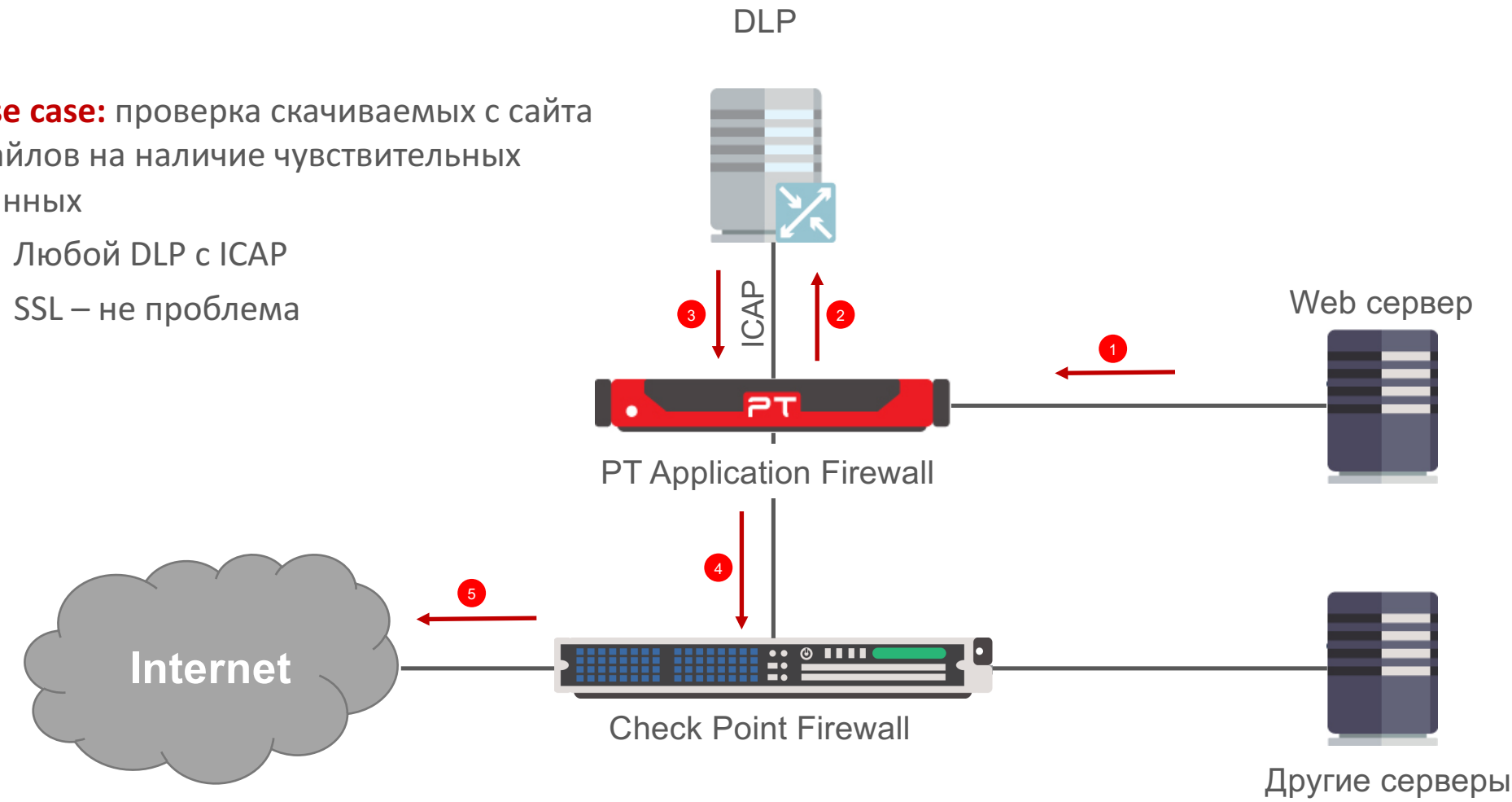


Сценарии использования: DLP

POSITIVE TECHNOLOGIES

Use case: проверка скачиваемых с сайта файлов на наличие чувствительных данных

+ Любой DLP с ICAP
+ SSL – не проблема

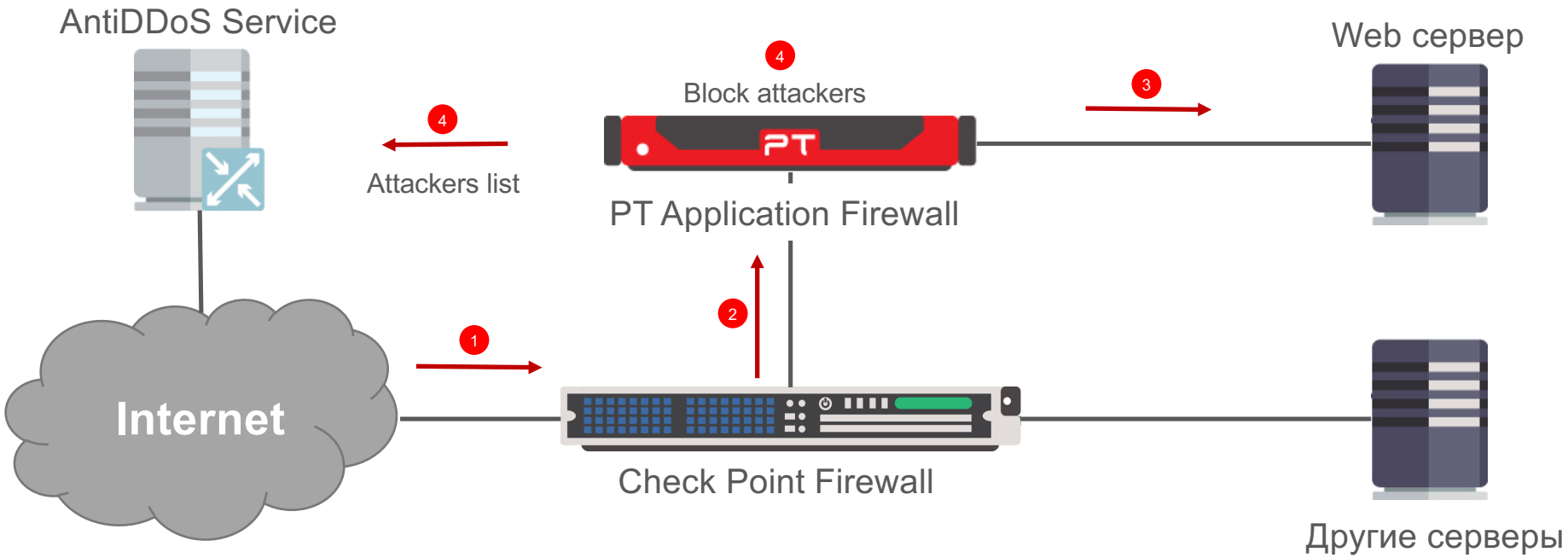


Сценарии использования: Application-layer AntiDDoS

POSITIVE TECHNOLOGIES

Use case: защита от Application-layer DDoS

+ Определяет атак по состоянию приложения (время ответа, 5XX errors)
+ Чистит трафик самостоятельно
+ Может передавать информацию об атакующих центрам очистки у провайдера



PT Application Firewall

POSITIVE TECHNOLOGIES

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)


POSITIVE TECHNOLOGIES
ptsecurity.ru