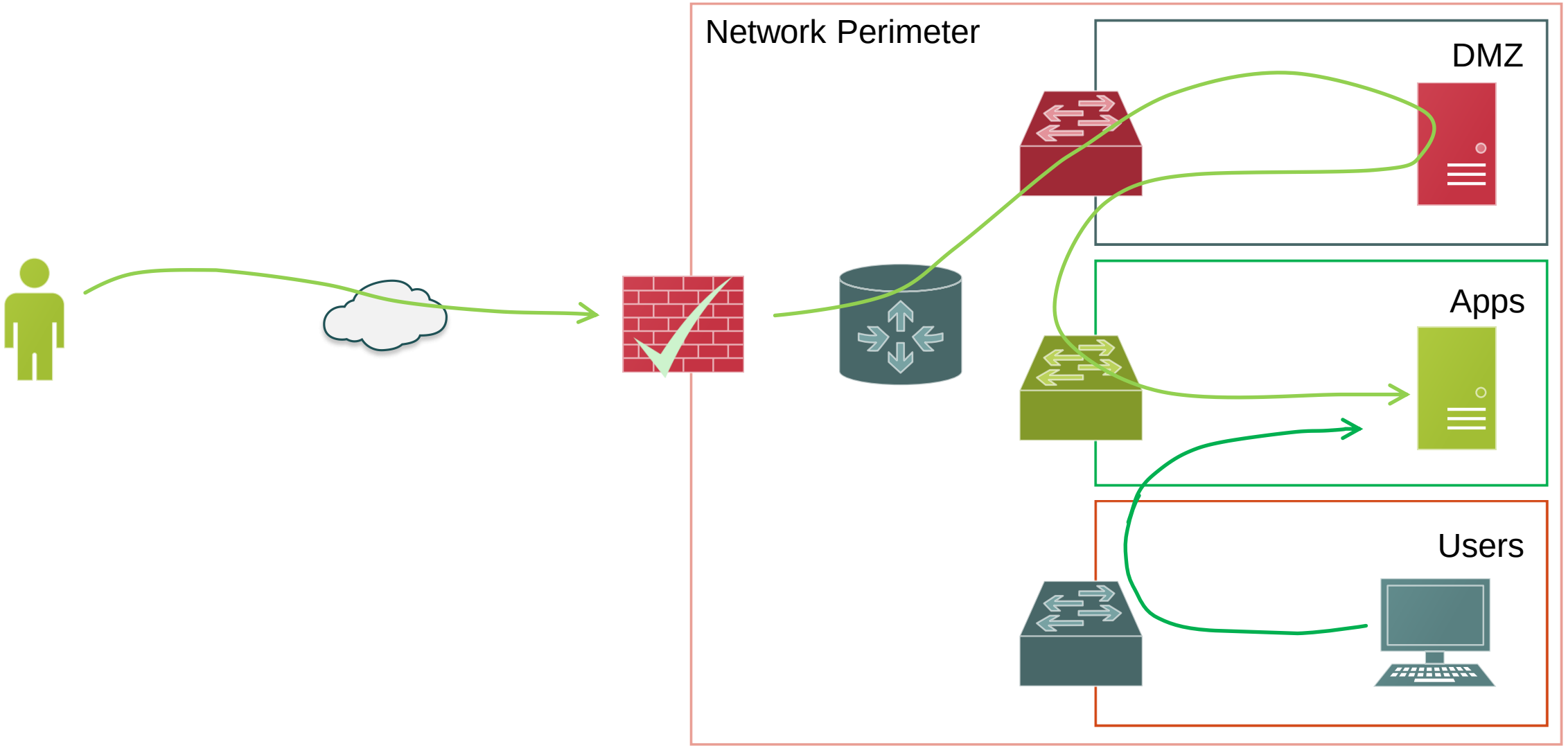
Эффективность применения WAF для защиты приложений

Всеволод Петров, vpetrov@ptsecurity.com

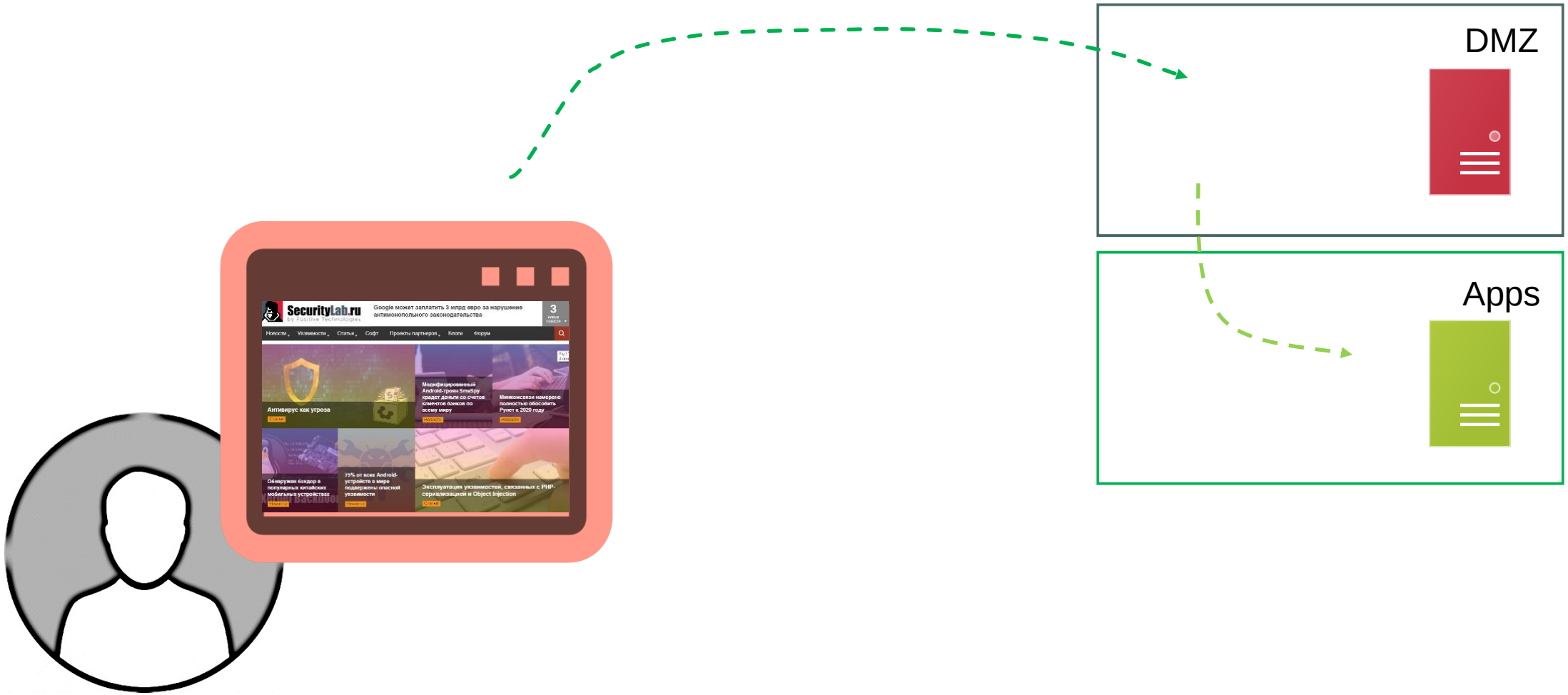
POSITIVE TECHNOLOGIES

На сегодняшний день, существует целый ряд техник вывода из строя приложений или сервисов. При этом, атаки на прикладном уровне требуют минимум ресурсов по сравнению с сетевыми атаками, а результат может быть достигнут гораздо быстрее. Способен ли Web Application Firewall обеспечить безопасность и доступность приложений? Существуют ли универсальные решения? Обсудим традиционные подходы к защите веб-приложений, их недостатки и современные тенденции.

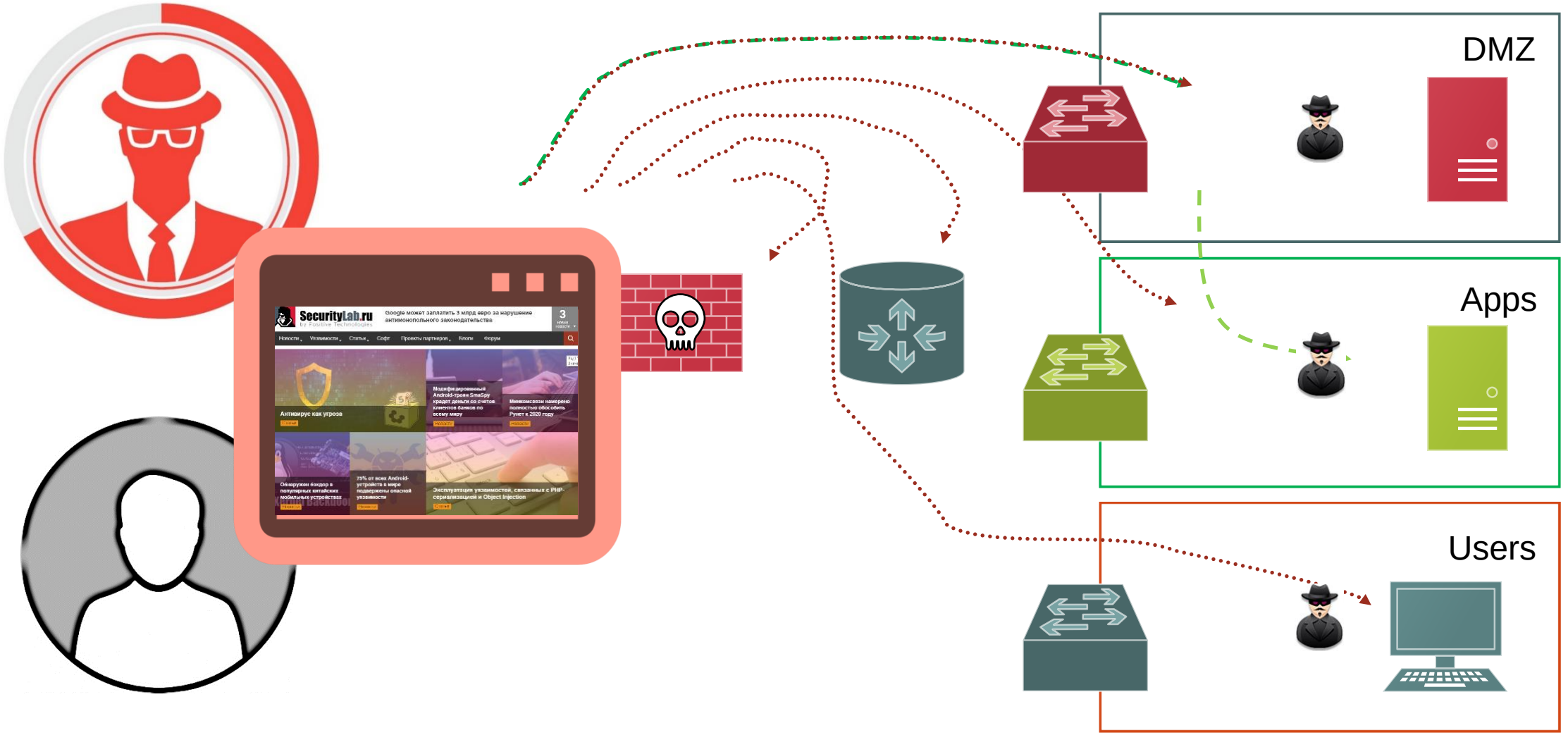
Что мы знаем о периметре сети?



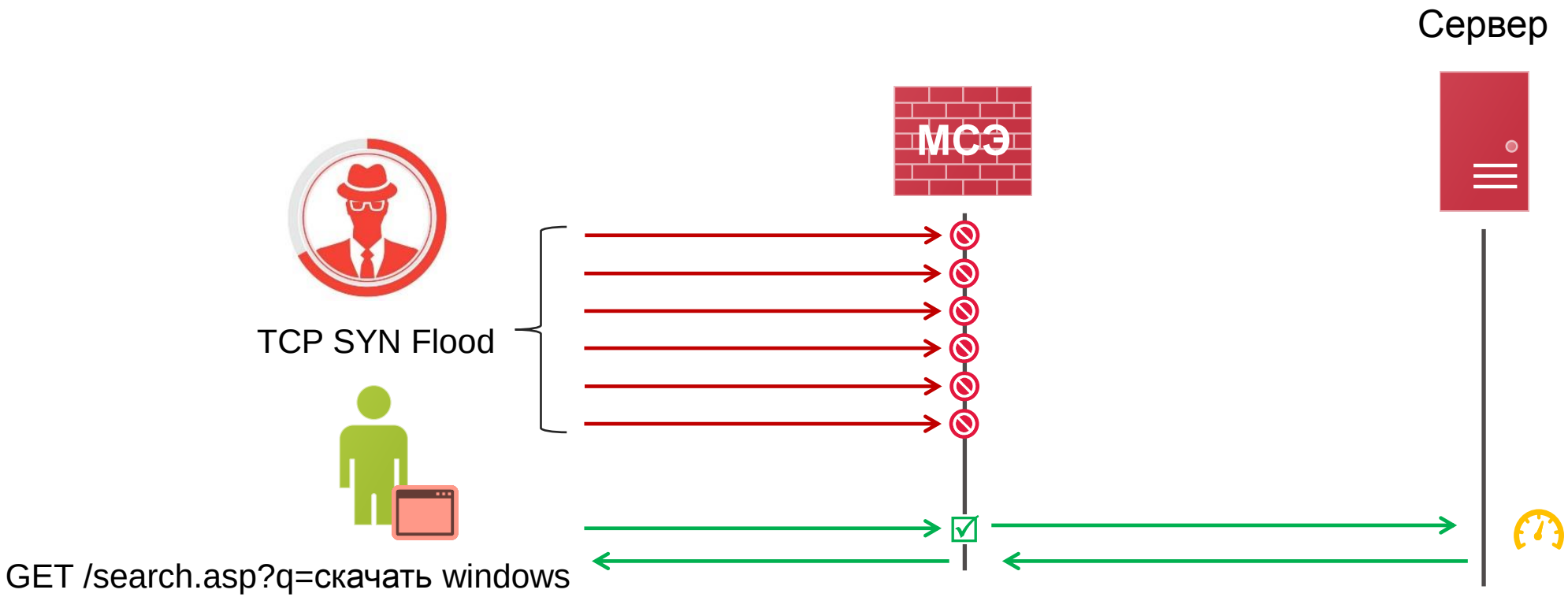
Приложения ломают периметр



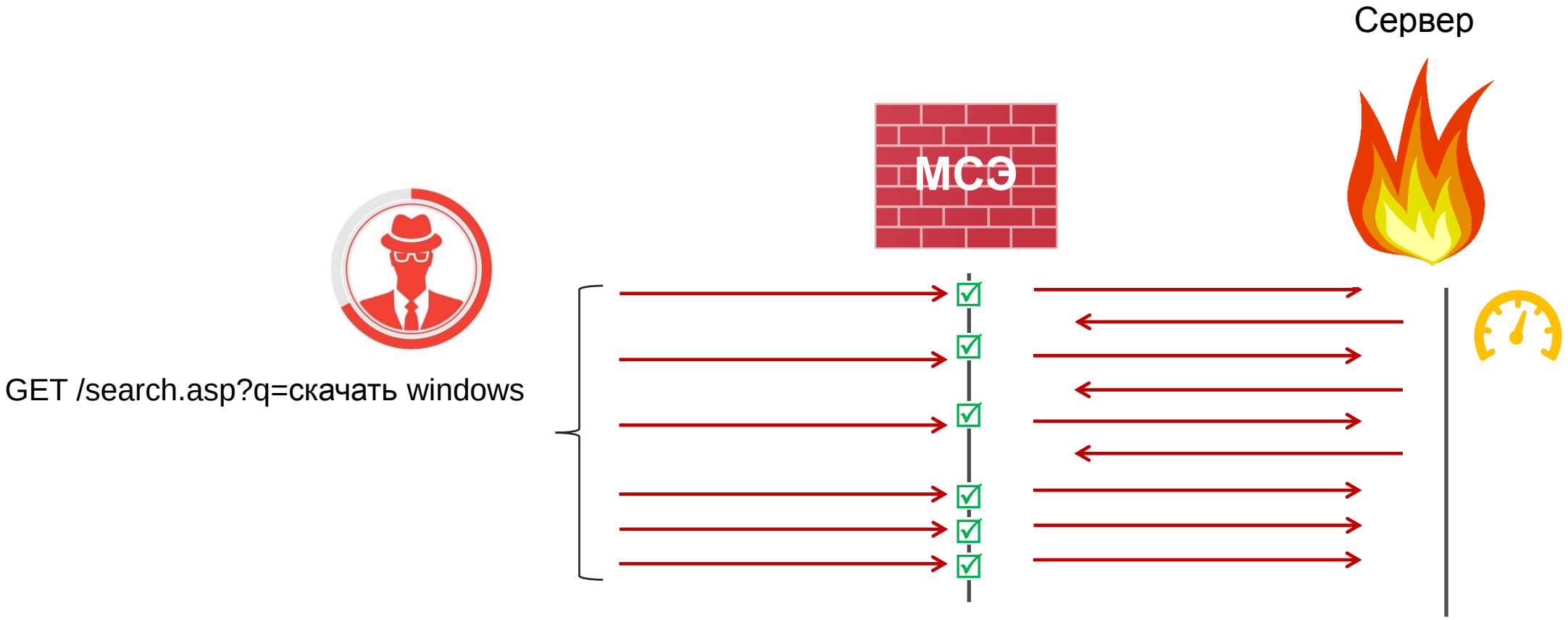
Приложения – доступ к инфраструктуре



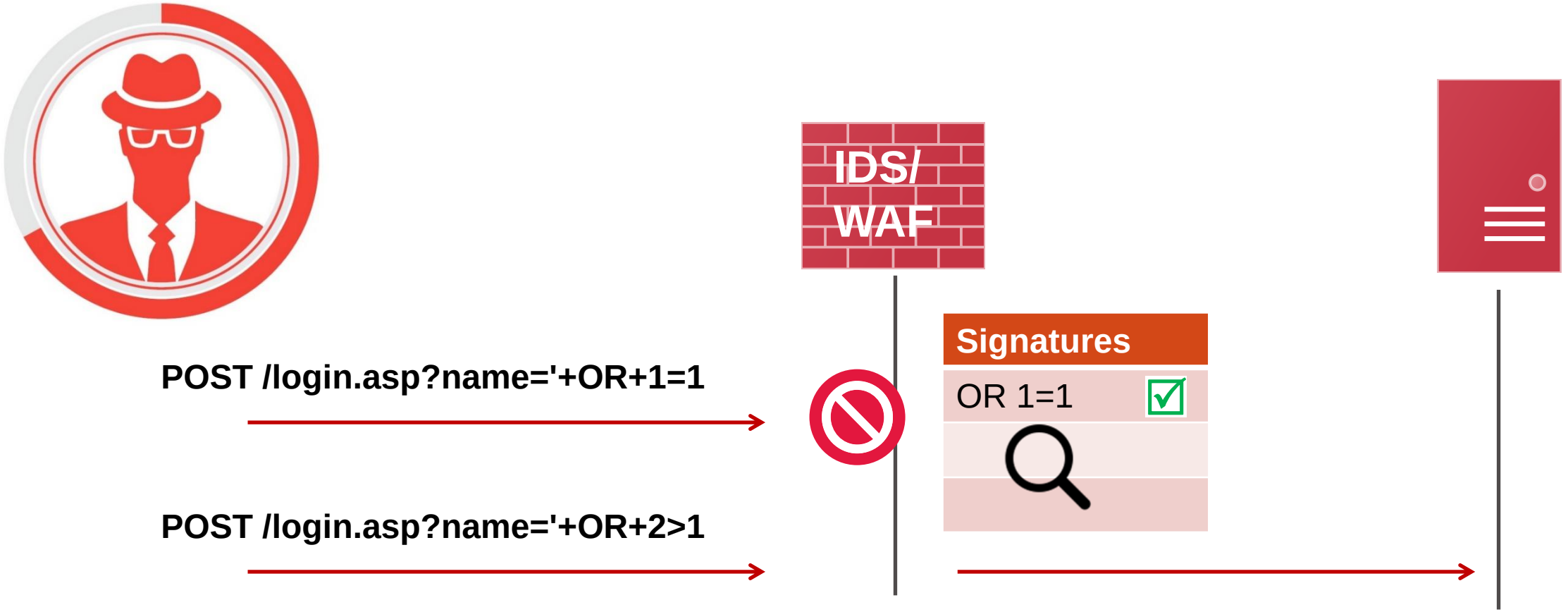
Сетевой DoS



Прикладной DoS



Сигнатуры?


IDS/
WAF
Signatures
OR 1=1
POST /login.asp?name='+OR+1=1
POST /login.asp?name='+OR+2>1

Сигнатуры? Можно обойти!

- Использование HTTP Parameter Fragmentation (HPF)
  - Пример уязвимого кода
    - Query("select * from table where a=".$_GET['a']." and b=".$_GET['b']);
    - Query("select * from table where a=".$_GET['a']." and b=".$_GET['b']." limit ".$_GET['c']);
  - Следующий запрос не позволяет провести атаку
    - /?a=1+union+select+1,2/*
  - Используя HPF, такие запросы могут успешно отработать
    - /?a=1+union/*&b=*/select+1,2
    - /?a=1+union/*&b=*/select+1,pass/*&c=*/from+users--
  - SQL запросы принимают вид
    - select * from table where a=1 union/* and b=*/select 1,2
    - select * from table where a=1 union/* and b=*/select 1,pass/* limit */from users--

Мистер Union Select

+500

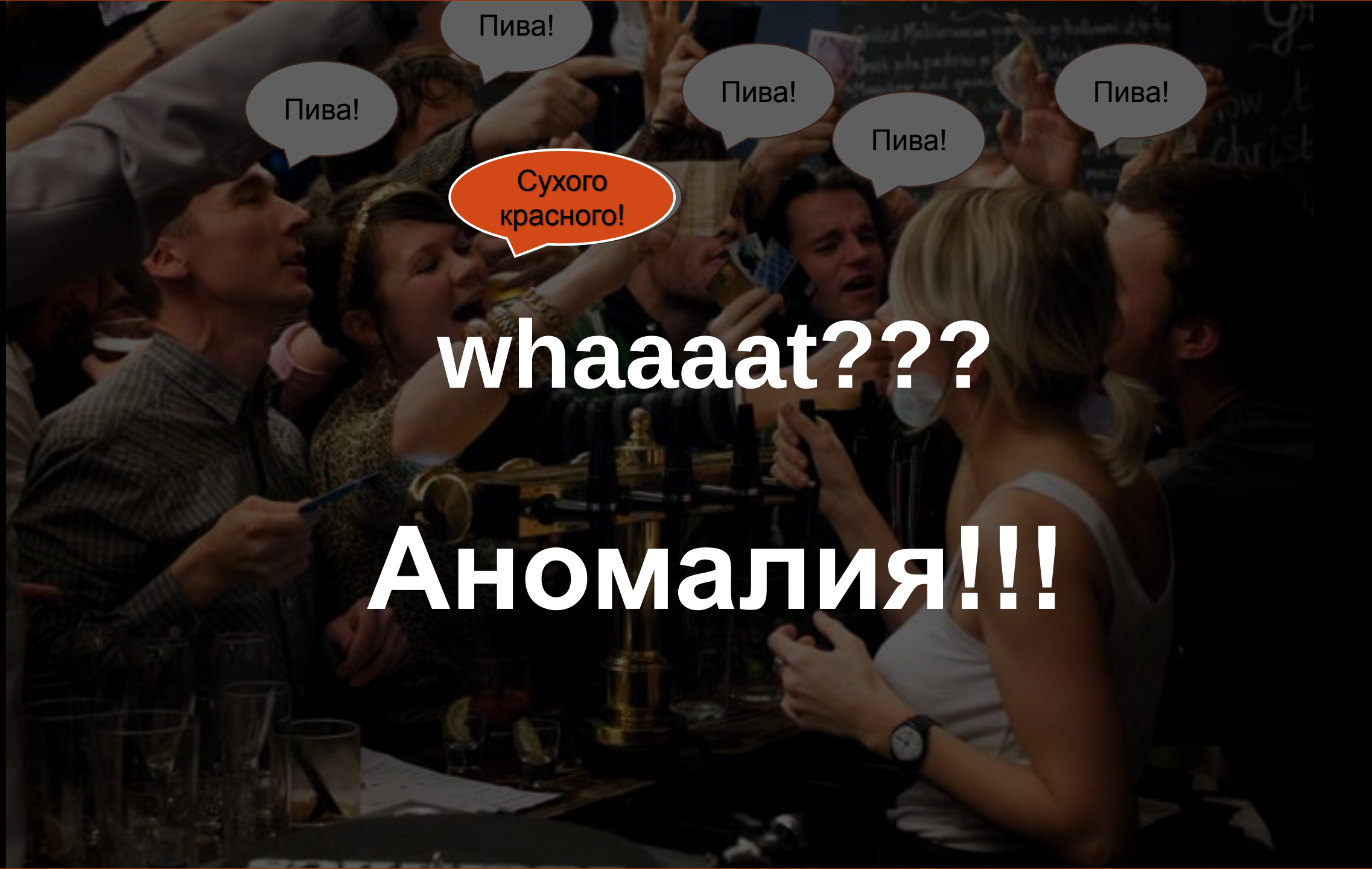
Users: Вова
Дима
Лёша
Оля
Саша
POST /login?id= Миша &action=submit
Вика

Сервер

1+union+select+1,2/*

POST /login?id= &action=submit


Пива!
Пива!
Пива!
Пива!
Пива!
Сухого красного!



whaaaat???

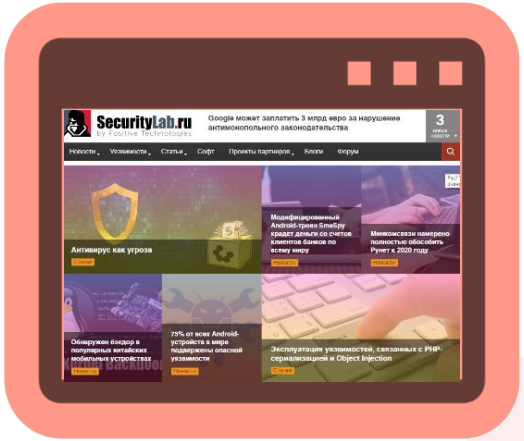
Аномалия!!!

Поиск аномалий на простом примере

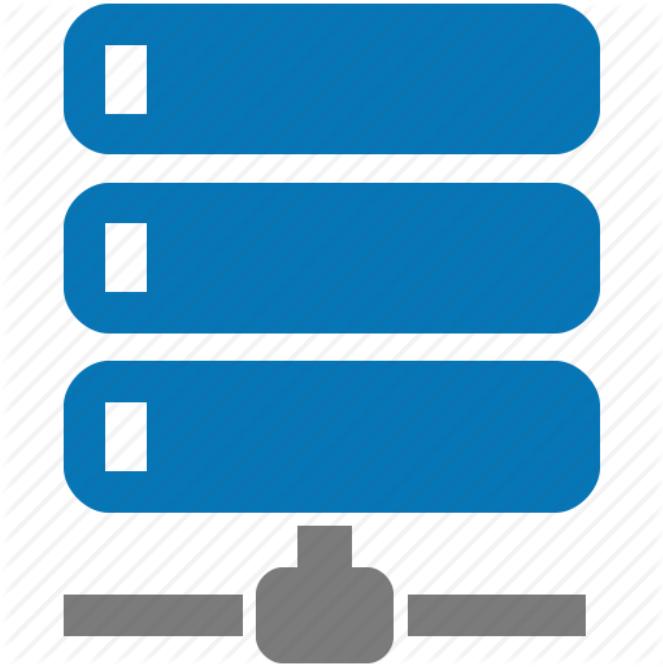
GET /search.asp?q=

Туры в Египет	1111010111111	2000
Рецепты рагу	111111101111	600
Купить шубку	111111011111	1100
Аптеки рядом	111111011111	
95 или 98	220111022	100500
Смотреть онлайн в HD	11111111011111101011	9999999999
1' or 1=1 -- -	23011023203303	7

Безопасное приложение – что это?



- Operating System
- HTTP Server Configuration
- Environment Configuration
- Framework
- Source Code
- External Components
- …



Продуктовый слайд №1

Web Application or Source Code

Repository | USB stick | E-mail | Website

Web address of the application, source code or application build on any media

PT Application Inspector

Abstract Interpretation | Pattern Matching | Configuration Checker | Fingerprint | DAST Engine

Combination of static (SAST), dynamic (DAST), and interactive (IAST) analysis approaches

PT Application Firewall

Virtual patches protect web application during vulnerabilities remediation

Automatic vulnerabilities validation

Exploit

Test case for vulnerability validation

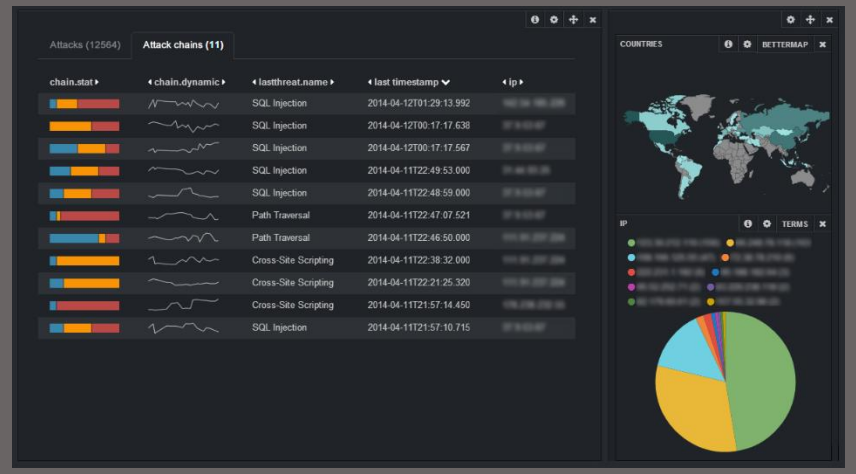
Report

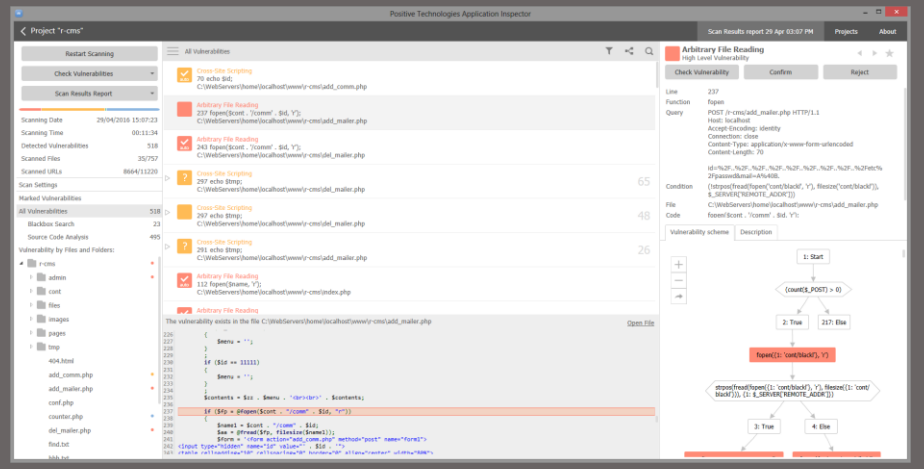
Customized and conformant with PCI DSS, OWASP and other compliance standards

Современный подход к безопасности приложений

+ Анализ кода => Виртуальные патчи
+ Анализ среды работы приложения
+ Подтверждение уязвимостей
+ Полное понимание контекста со стороны WAF
+ Адаптация под приложение и трафик
+ Сигнатуры – не таблетка от всех болезней
+ Машинное обучение и выявление аномалий
+ WAF должен быть удобным инструментом для защиты

PT Application Security Suite





Application Firewall

- Встроенный сканер уязвимостей (DAST)
- Защита от DDoS
- Выявлении аномалий
- Машинное обучение
- Продвинутые корреляции
- Прост в настройке и обслуживании

Application Inspector

- Анализ кода и среды
- Фокус на реальных уязвимостях
- Встраивание в процесс разработки (SSDL)
- Генерация эксплоитов
- Комбинация лучших свойств SAST и DAST
- Виртуальные патчи для PT AF
- Поиск закладок в коде

Приложения в безопасности

PT Application Security Suite

POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES

Спасибо!

vpetrov@ptsecurity.com