



# Web Application Firewall

Илья Головацкий

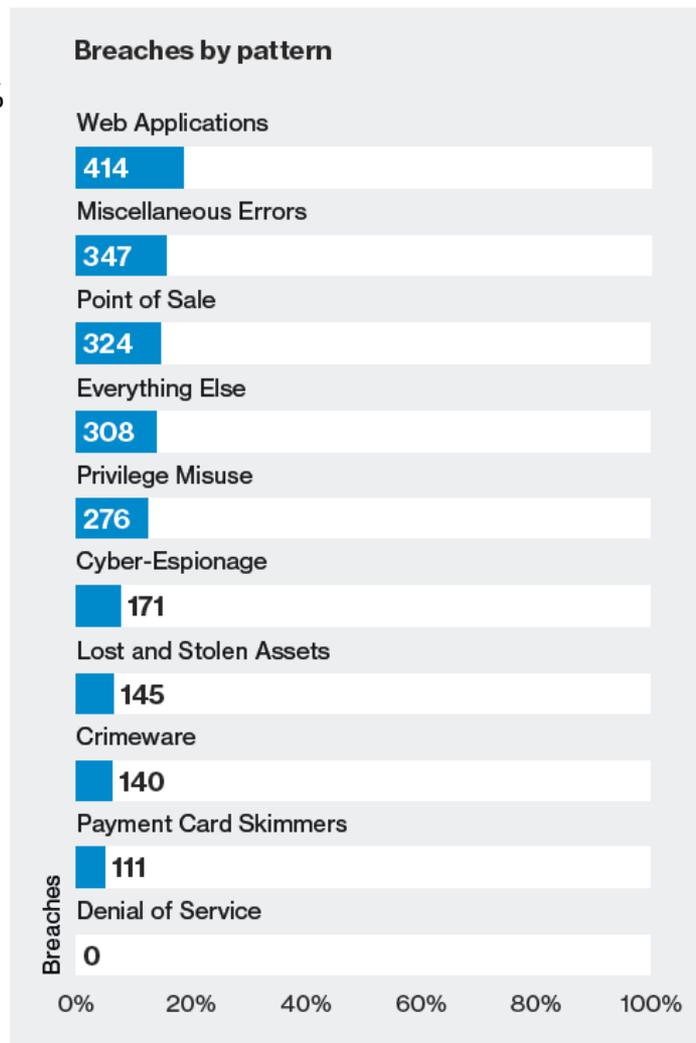
ilg@muk.ua

+380 63 569-52-41

# Отчет о расследовании нарушений данных

## Отчет о реальных нарушениях от Verizon

- Доля атак на веб-приложения составляет примерно 20% от общего числа зарегистрированных инцидентов
- Объем нарушений данных при атаках веб-приложений по-прежнему находится на вершине
- WAF может помочь предотвратить различные популярные атаки: XSS, SQL-инъекции, CSRF и другие атаки на веб-приложения
- Главный фокус:
  - Финансовая отрасль
  - Государственные службы
  - Информационные порталы



# Инциденты утечки данных

## Скомпрометированные организации

### Legacy Health(U.S)

- Non-profit health system with hospitals
- 38,000 patient records exposed



### UnityPoint Health(U.S)

- A network of hospitals, clinics and homecare service
- 1.4 million patient records exposed



### LifeBridge Healthcare(U.S)

- Non-profit healthcare cooperation, operates several medical institutions
- 500,000 patient records exposed



### Sing Health(Singapore)

- Singapore's largest group of healthcare institution
- Operates 4 general hospitals and 5 national specialty centers
- 1.5 million patient records exposed



### Norway(South-East Regional Health Authority, RHF)

- A state enterprise responsible for specialist healthcare in one of our regions of Norway
- More than half of the Norway population(2.9 million) healthcare data exposed



# Инциденты утечки данных

## Скомпрометированные организации

### Avid Life Media(U.S)

- Mother company of Ashley Madison
- A company to provide online date and social networking service
- 37 million private data exposed



### Adult Friend Finder (U.S)

- A company to primarily deal in adult entertainment, online dating and social networking service
- 412 million account exposed



### Yahoo(U.S)

- Portal, directory and, e-mail service provider
- 5 million user account data exposed



### Korea Telecom(South Korea)

- Telecommunication and internet service Provider
- 12 million user data exposed



**OWASP <https://www.owasp.org/>**

**Open Web Application Security Project (OWASP) —**



это открытый проект обеспечения безопасности веб-приложений

OWASP был основан 9 сентября 2001 года Марком Керфи и Дэннисом Гривзом.

Сообщество OWASP включает в себя корпорации, образовательные организации и частных лиц со всего мира. Сообщество работает над созданием статей, учебных пособий, документации, инструментов и технологий, находящихся в свободном доступе.

Фонд OWASP — это благотворительная организация по 501(c)(3) organization[en], которая оказывает поддержку и осуществляет управление проектами и инфраструктурой OWASP. Кроме того, Фонд зарегистрирован как некоммерческая организация в Европе с июня 2011 года.

# OWASP Testing Guide

## Руководство по тестированию веб приложений

- методы, способы и инструментарий этапа сбора информации о приложениях
- принципы проведения тестирования, объясняют смысл и общую концепцию управления процессами тестирования безопасности веб-приложений.
- технические аспекты тестирования на проникновение веб-приложений.
- Методы, способы и инструментарий тестирования

# OWASP TOP10 2017

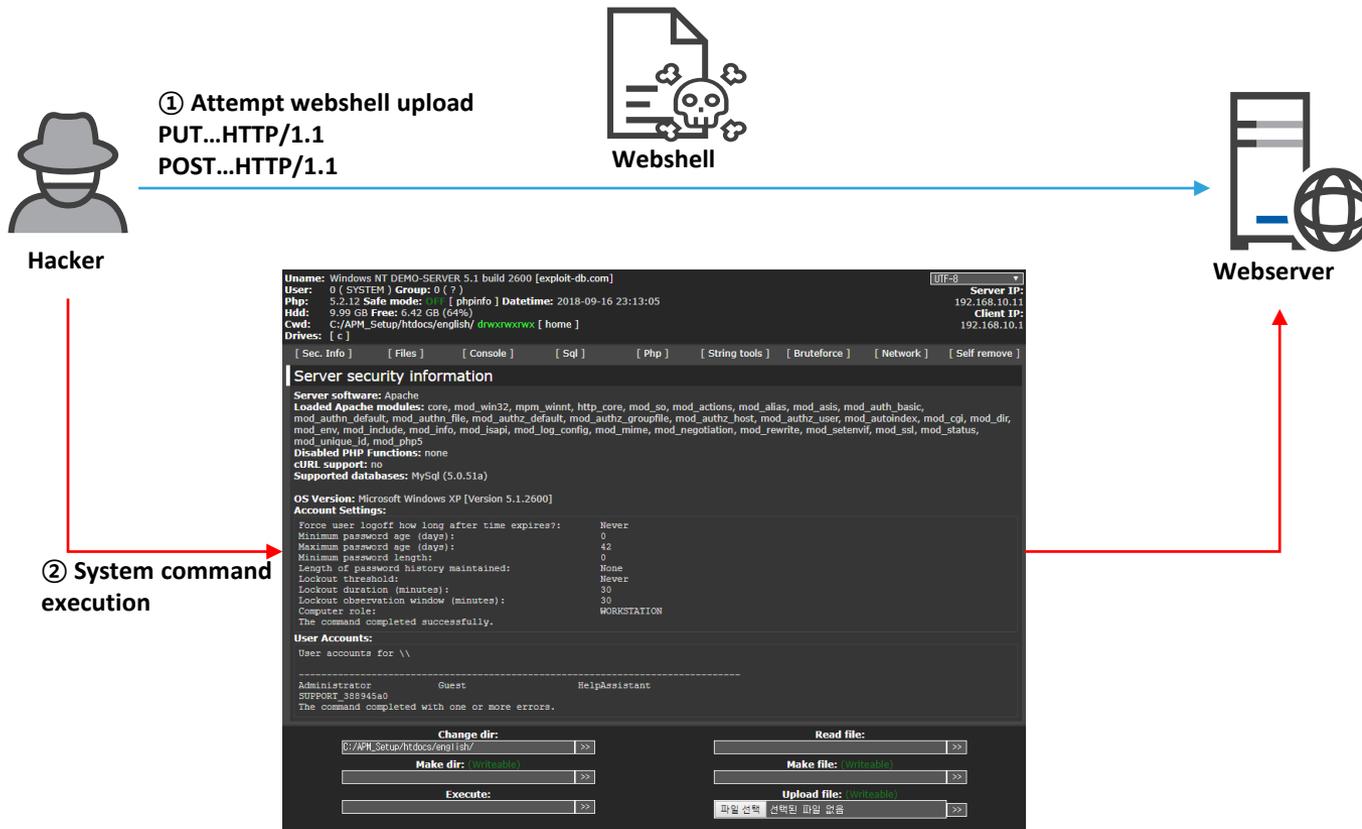
Список самых опасных рисков (уязвимостей) веб-приложений от 2017 года:

- A1 Внедрение кода
- A2 Некорректная аутентификация и управление сессией
- A3 Утечка чувствительных данных
- A4 Внедрение внешних XML- сущностей (XXE)
- A5 Нарушение контроля доступа
- A6 Небезопасная конфигурация
- A7 Межсайтовый скриптинг
- A8 Небезопасная десериализация
- A9 Использование компонентов с известными уязвимостями
- A10 Отсутствие журналирования и мониторинга

# Инциденты утечки данных: A1 Внедрение кода

## ▪ Webshell Upload

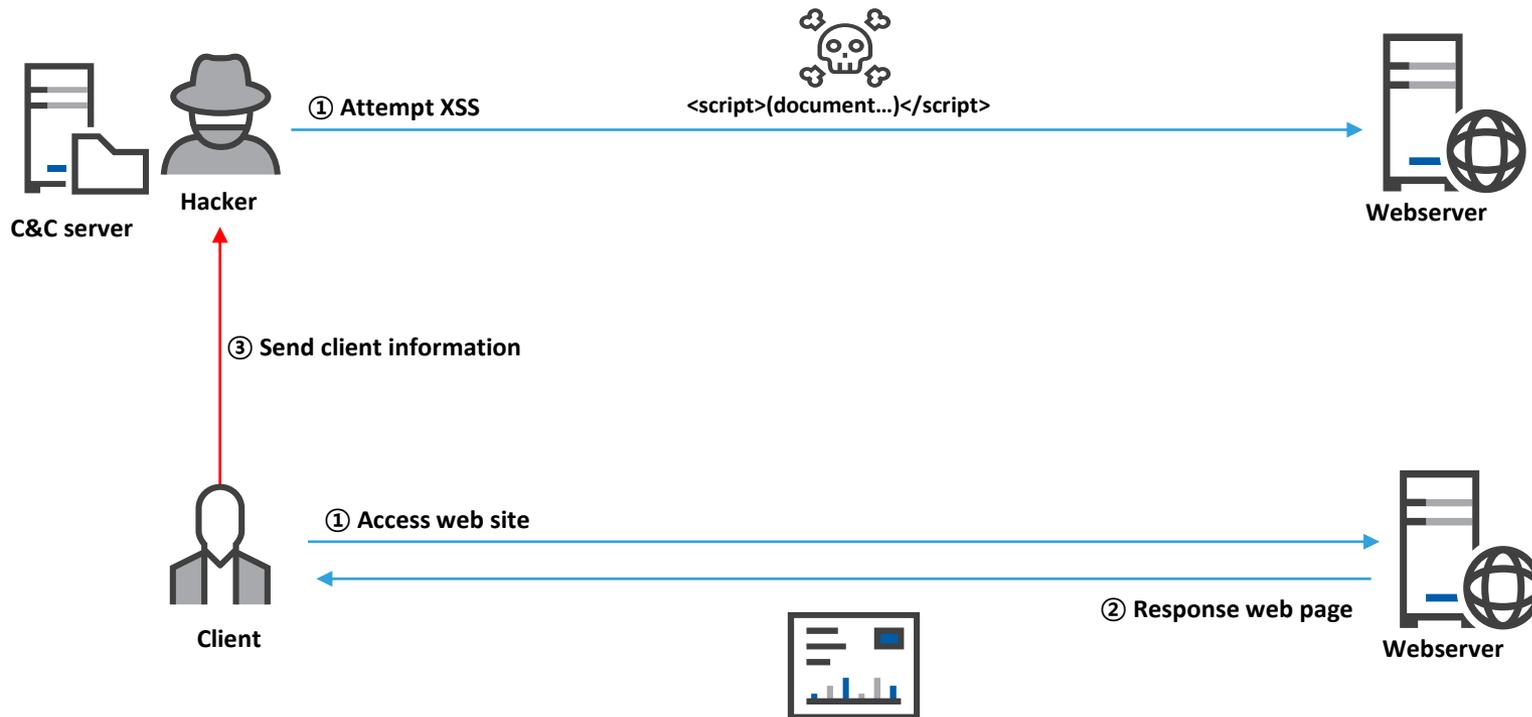
- Хакер пытается загрузить веб-страницу, чтобы отправить системную команду или ввести вредоносный код в уязвимую систему.
- Хакер доминирует над системой, принимая учетную запись системного администратора, внедряя вредоносный код из удаленного и веб-сайта с помощью веб-браузера



# Инциденты утечки данных: A7 Межсайтовый скриптинг

- Межсайтовый скриптинг

- Передает код вредоносного скрипта с помощью HTTP-запроса, чтобы вставить его на веб-страницу или веб-приложение.
- Переданный код позволяет выполнять скрипт на стороне клиента, когда клиент обращается к веб-сайту. Затем информация о клиенте будет передана хакерам через C&C сервер (Command and Control).



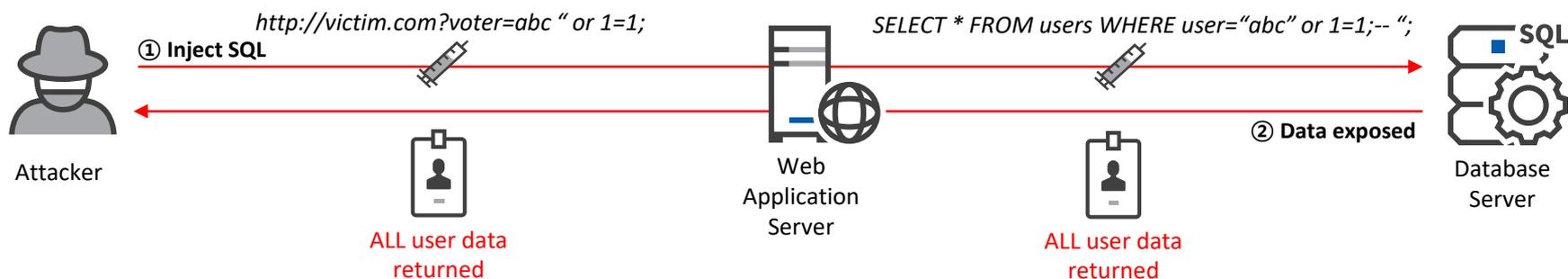
# Инциденты утечки данных

## Предполагаемый характер нападения

- SQL Injection

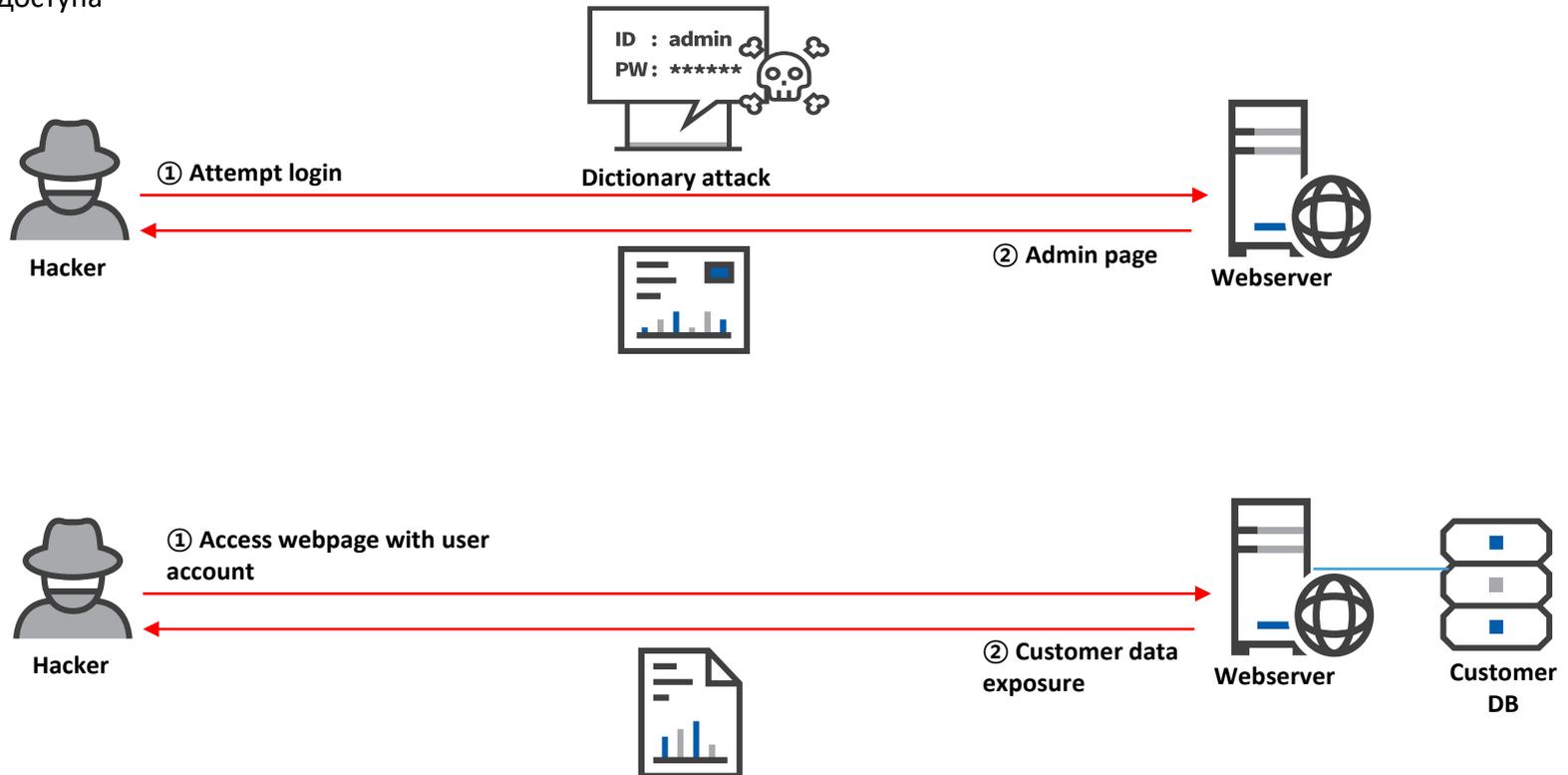
- Широко используемый вектор атаки для веб-сайтов, где злоумышленник вставляет SQL-запросы в поля ввода для непосредственного взаимодействия с внутренней базой данных для достижения любой из следующих целей:

- Обход аутентификации
- Дамп базы данных
- Подделка существующих данных
- И другие..



# Инциденты утечки данных

- Обход аутентификации и прав доступа
  - Внедрение случайных идентификаторов и паролей с использованием автоматизированной атаки по словарю для взлома учетной записи администратора и неправильного использования учетной записи
  - Перехват и неправомерное использование информации о клиентах путем доступа к конфиденциальным данным и информации с анонимной учетной записью пользователя из-за нарушения (слабого) контроля доступа



# Инциденты утечки данных

## Цель несанкционированного доступа

- Уязвимости правительственной системы используются по ряду причин:
  - **Хактивизм** - использование компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации[1].
  - **Правительственный кибер-шпионаж**



## Инциденты утечки данных

### Цель кражи данных

- Данные учетной записи пользователя имеют личную информацию, которая включает имя, дату рождения, электронную почту и платежную информацию
- Данные продаются на черном рынке, для возможности использовать для других атак
- Он использует для того, чтобы снизить репутацию взломанной компании



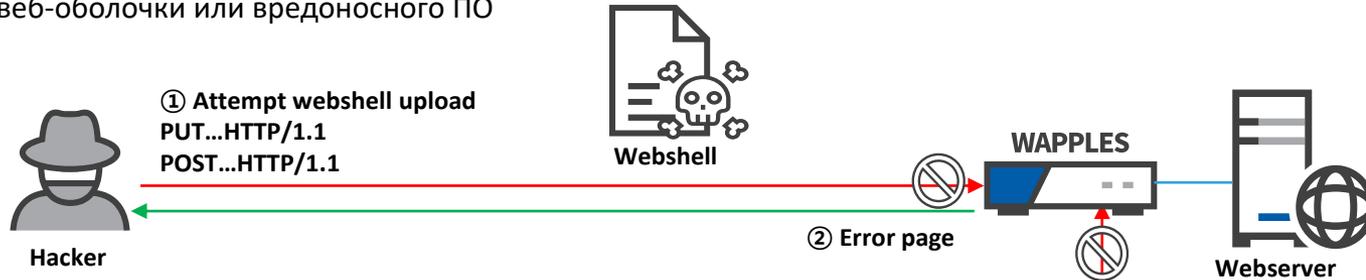
# Защищаемся с WAPPLES

*Предотвращаем атаки*

# Defense with WAPPLES

- Webshell Upload

- WAPPLES предотвращает попытку загрузки веб-страниц, проверяя содержимое файла. Используя механизм анализа типа данных, находит скрытые под веб-оболочкой изображения, и может быть обнаружена WAPPLES
- WAPPLES также обеспечивает предотвращение выполнения системных команд с помощью ранее загруженной веб-оболочки или вредоносного ПО



The screenshot shows a Windows command prompt window with the following content:

```
Uname: Windows NT DEMO-SERVER 5.1 build 2600 [exploit-db.com]
User: 0 (SYSTEM) Group: 0 (? )
Php: 5.2.12 Safe mode: [phpinfo] Datetime: 2018-09-16 23:13:05
Hdd: 9.99 GB Free: 6.42 GB (64%)
Cwd: C:/APM_Setup/htdocs/english/ drwxrwxrwx [ home ]
Drives: [ c ]
Server IP: 192.168.10.1
Client IP: 192.168.10.1
```

Below the system information, there is a section titled **Server security information** with the following details:

- Server software: Apache
- Loaded Apache modules: core, mod\_win32, mpm\_winnt, http\_core, mod\_so, mod\_actions, mod\_alias, mod\_asis, mod\_auth\_basic, mod\_authn\_default, mod\_authn\_file, mod\_authz\_default, mod\_authz\_groupfile, mod\_authz\_host, mod\_authz\_user, mod\_autoindex, mod\_cgi, mod\_dir, mod\_env, mod\_include, mod\_info, mod\_isapi, mod\_log\_config, mod\_mime, mod\_negotiation, mod\_rewrite, mod\_setenvif, mod\_ssi, mod\_status, mod\_unique\_id, mod\_php5
- Disabled PHP Functions: none
- cURL support: no
- Supported databases: MySQL (5.0.51a)

Next is the **OS Version** section:

```
OS Version: Microsoft Windows XP [Version 5.1.2600]
Account Settings:
Force user logoff how long after time expires?: Never
Minimum password age (days): 0
Maximum password age (days): 42
Minimum password length: 0
Length of password history maintained: None
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: WORKSTATION
The command completed successfully.
```

Finally, the **User Accounts** section is shown:

```
User accounts for \\
-----
Administrator Guest HelpAssistant
support_38944a0
The command completed with one or more errors.
```

At the bottom of the window, there are several input fields for file operations:

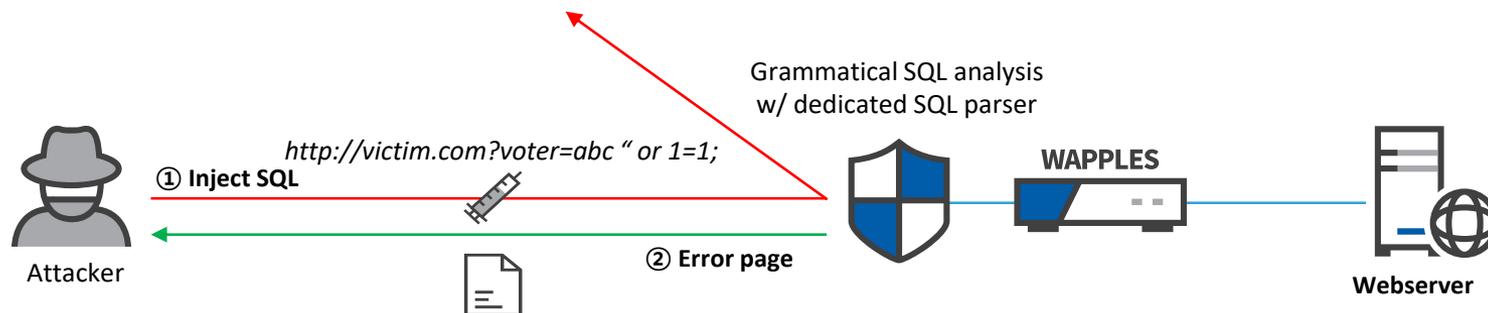
- Change dir: C:/APM\_Setup/htdocs/english/
- Read file: [empty]
- Make dir: [empty]
- Make file: [empty]
- Execute: [empty]
- Upload file: [empty]

② System command execution

# Защищаемся с WAPPLES

## Предотвращение атак

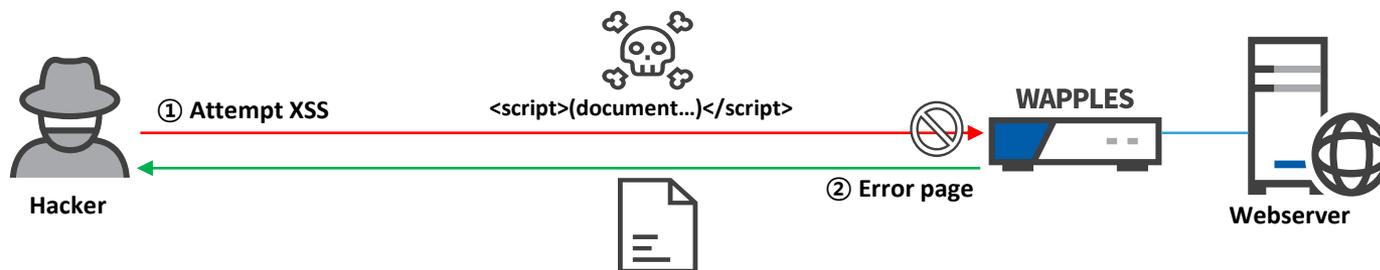
- SQL Injection
  - WAPPLES обнаруживает грамматику SQL в HTTP-запросе (предварительно расшифровывая при необходимости) с использованием выделенного синтаксического анализатора SQL и блокирует запрос, если найдены синтаксически допустимые и потенциально вредоносные SQL-выражения.



# Защищаемся с WAPPLES

- Cross Site Scripting

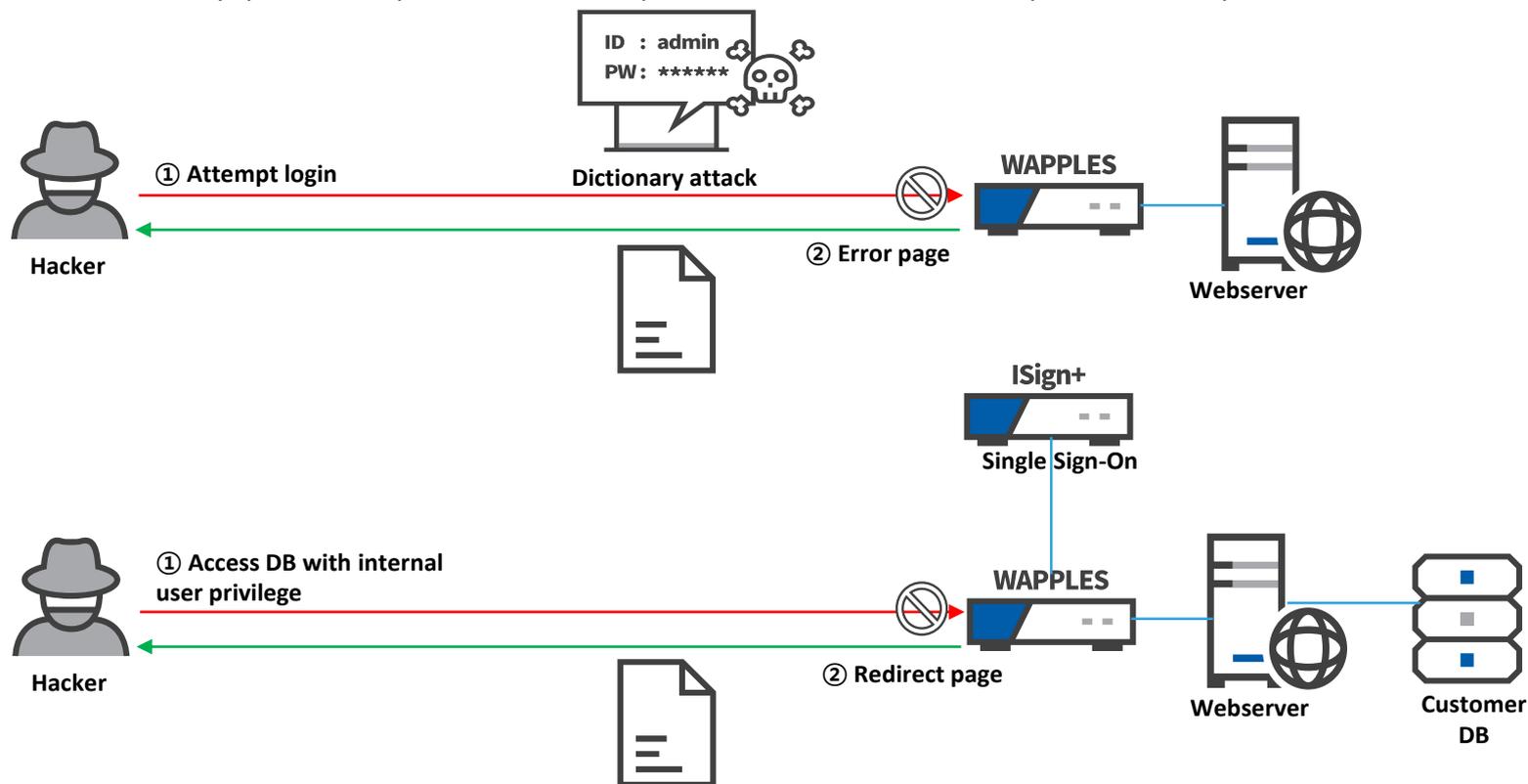
- WAPPLES запрещает использовать теги скрипов, которые могут быть выполнены в веб-приложении, путем проверки пакета HTTP-запроса
- WAPPLES блокирует не только основные теги HTML, но и различные типы исполняемых функций для приложений



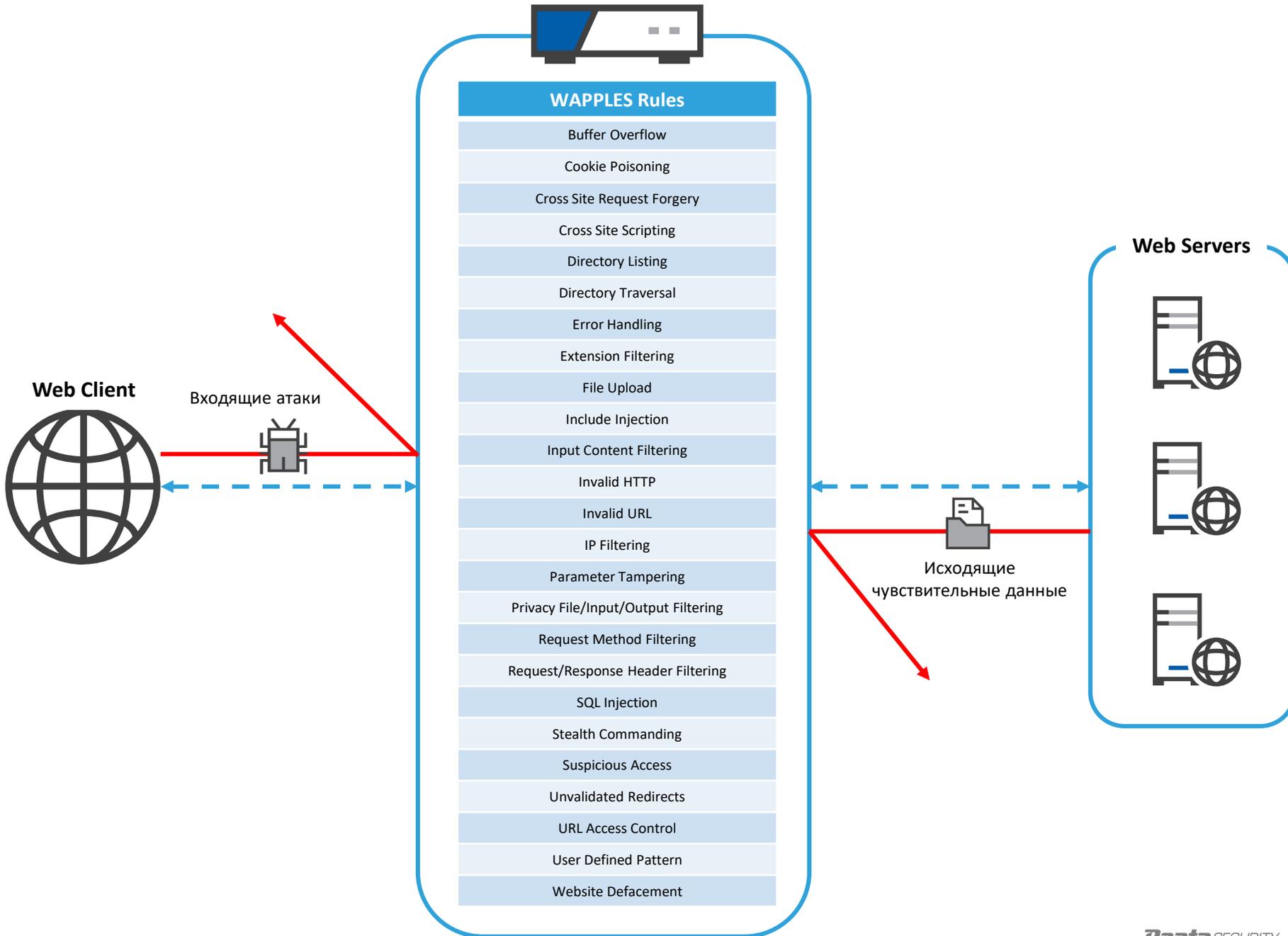
# Защищаемся с WAPPLES

## ▪ Broken Authentication and Access Control

- WAPPLES предотвращает автоматическую атаку по словарю через функцию предотвращения атак с использованием грубой силы
- WAPPLES поддерживает интеграцию SSO для идентификации авторизованного пользователя для проверки подлинности и управления привилегиями авторизованного пользователя с различными протоколами



# WAPPLES





## Соответствие PCI-DSS

- PCI-DSS определяет набор требований для обеспечения безопасности данных держателей карт
- WAPPLES обеспечивает покрытие значительного подмножества требований безопасности, установленных PCI-DSS, включая следующие:
  - ✓ Маскирование карточных данных
  - ✓ Предотвращение атак на веб приложения таких как buffer overflow, XSS, CSRF, и других.
  - ✓ Непрерывный контроль трафика
  - ✓ Управление доступом к Web-приложениям, разделам сайтов
  - ✓ Подробный журнал доступа, учет изменений

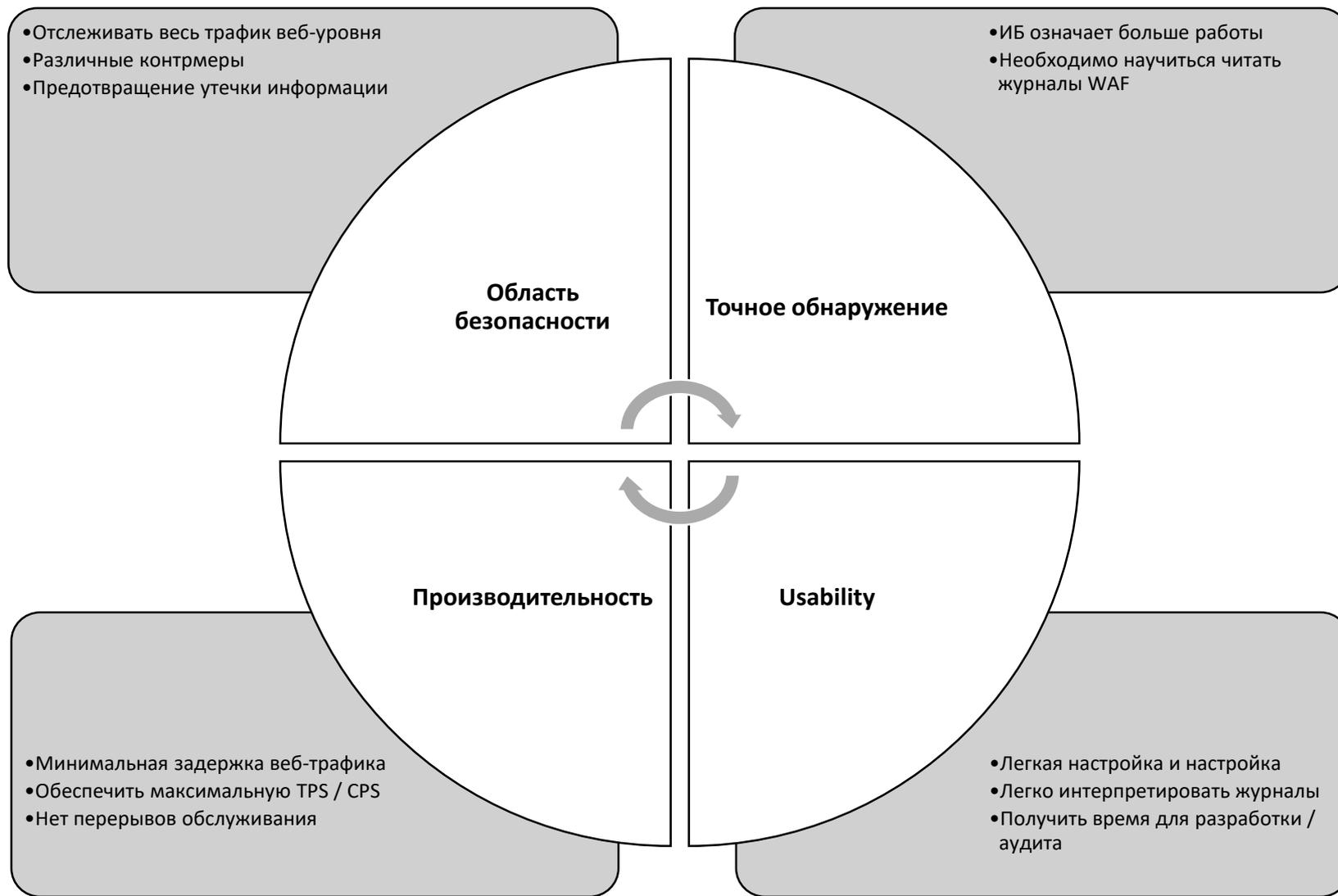
\*Детальная информация о соответствии PCI-DSS и покрытии требований по запросу.

## Преимущества WAPPLES

## WAF's advantage for OWASP Top 10 vulnerability

OWASP Top 10 (2017)	Network Firewall	IDS / IPS	WAF
A1: Injection	X	△	○
A2: Broken Authentication	X	△	○
A3: Sensitive Data Exposure	X	△	○
A4: XML External(XXE) Entities	X	X	○
A5: Broken Access Control	X	X	○
A6: Security Misconfiguration	X	X	○
A7: Cross Site Scripting(XSS)	X	X	○
A8: Insecure Deserialization	X	X	○
A9: Using Components with Known Vulnerabilities	X	○	○
A10: Insufficient Logging & Monitoring	X	X	○

# Что должен делать хороший WAF?



## Проблемы с WAF на основе сигнатур (1-е и 2-е поколение)



### Технические нюансы

- Невозможно предотвратить атаки нулевого дня или модифицированные атаки
- Больше сигнатур подразумевает увеличение числа ложных срабатываний
- Увеличение числа сигнатур приводит к ухудшению производительности

### Операционные нюансы

- Оборона всегда будет отставать от преступной деятельности
- Сигнатуры накладывают административную нагрузку на администратора
- Сигнатуры могут быть к конкретным приложениям и не иметь отношения к другим пользователям

## 3<sup>rd</sup> Поколение WAF: Обнаружение на основе логического анализа

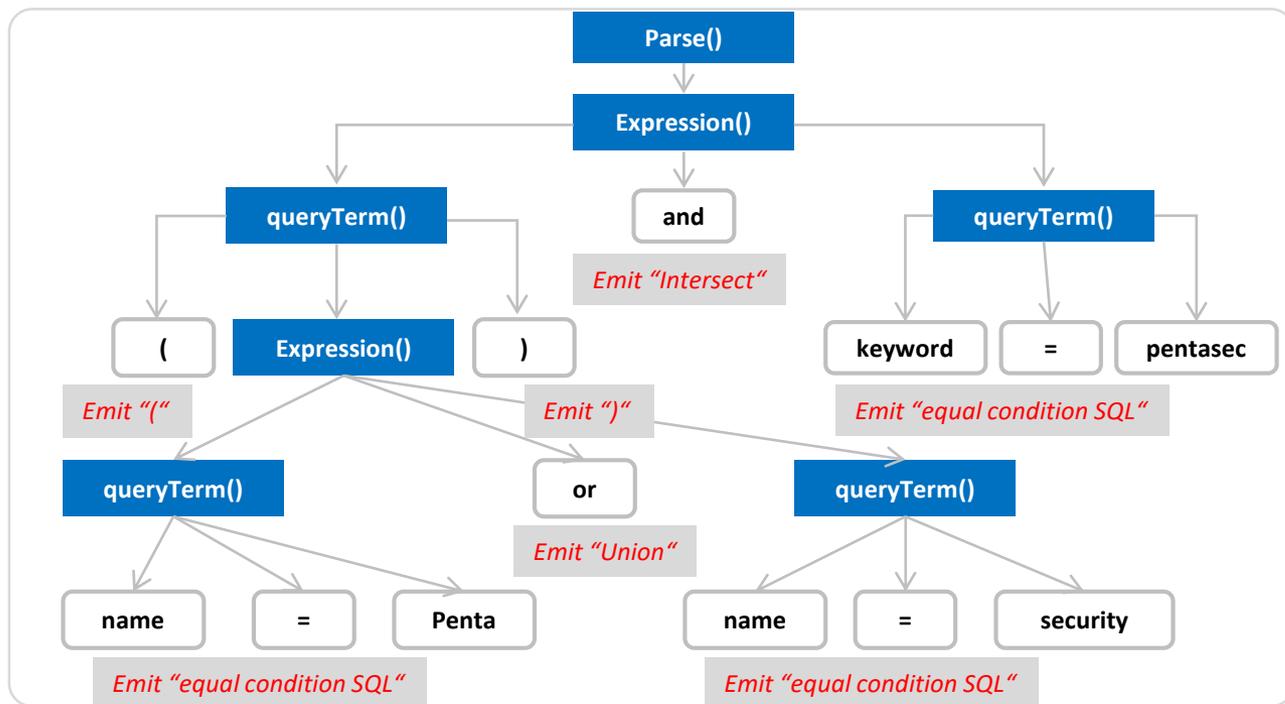


- ✓ **WAPPLES COCEP\***: Механизм обнаружения на основе запатентованного протокола логического анализа
- ✓ **Минимальные ошибочные сработки**: Он проверяет содержимое веб-трафика и анализирует каждую транзакцию по существу.
- ✓ **Обнаружение и Блокирование ранее не известных атак** потому что его метод обнаружения основан на анализе логики атаки, а не сигнатуры
- ✓ **Минимальная потеря производительности**: 27 predetermined правил в отличие от тысяч сигнатур. WAPPLES проверяет трафик за менее чем 1/1000 секунды
- ✓ **Уменьшите административную нагрузку на администраторов** по сравнению с сигнатурным анализом

\*COCEP: COntents Classification and Evaluation Processing)

# Как работает ядро обнаружения WAPPLES

Пример: Обработка SQL-инъекций посредством разбора грамматики SQL



- Первый этап - проверить, является ли это действительной фразой SQL.

- Если исходная строка не является фразой SQL, строка не может использоваться для атаки; в противном случае WAPPLES проверяет, может ли SQL-фраза иметь доступ к уязвимым процедурам или функциям.

## WAPPLES управление и сетевые сервисы

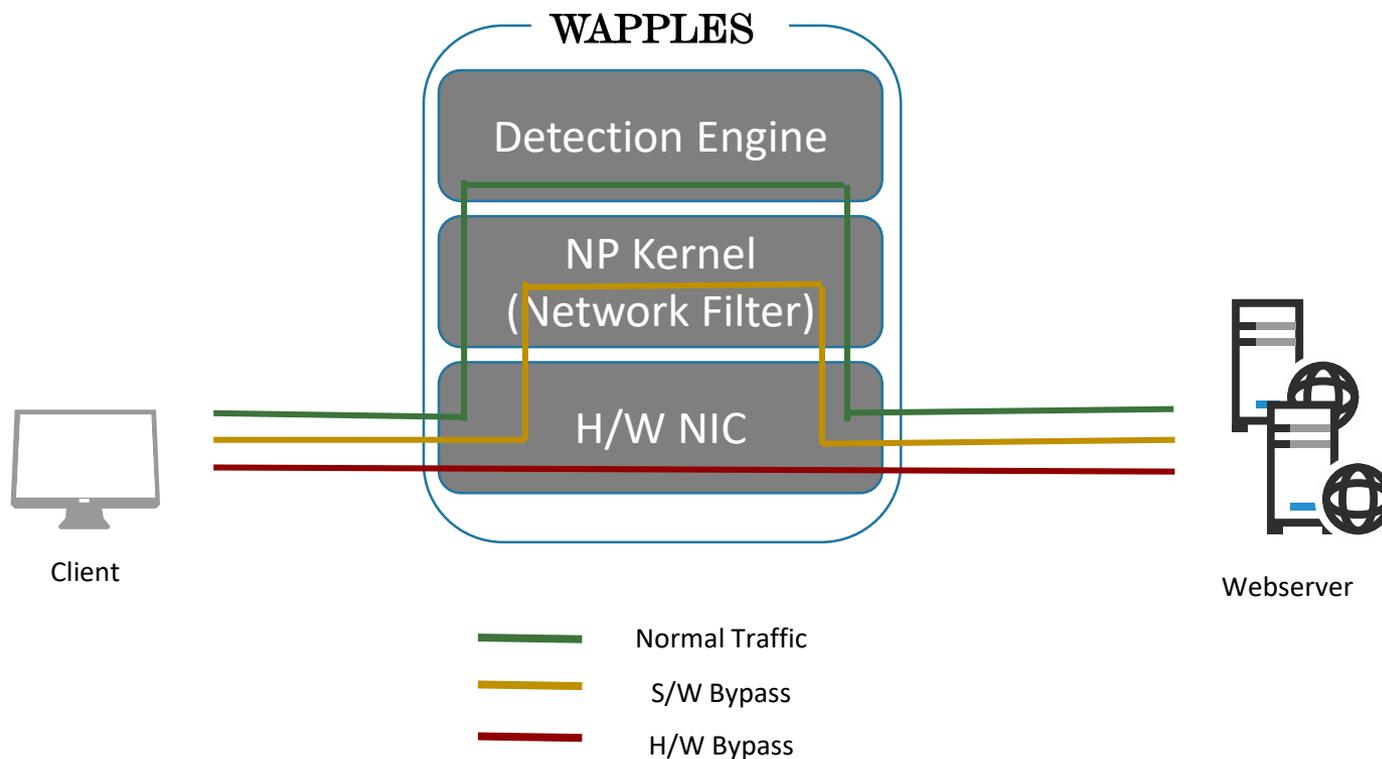
# Поддержка обхода аппаратного и программного обеспечения

What is Bypass?

The WAPPLES H/W and S/W bypass options enable web access even in the case of H/W or S/W problems respectively.

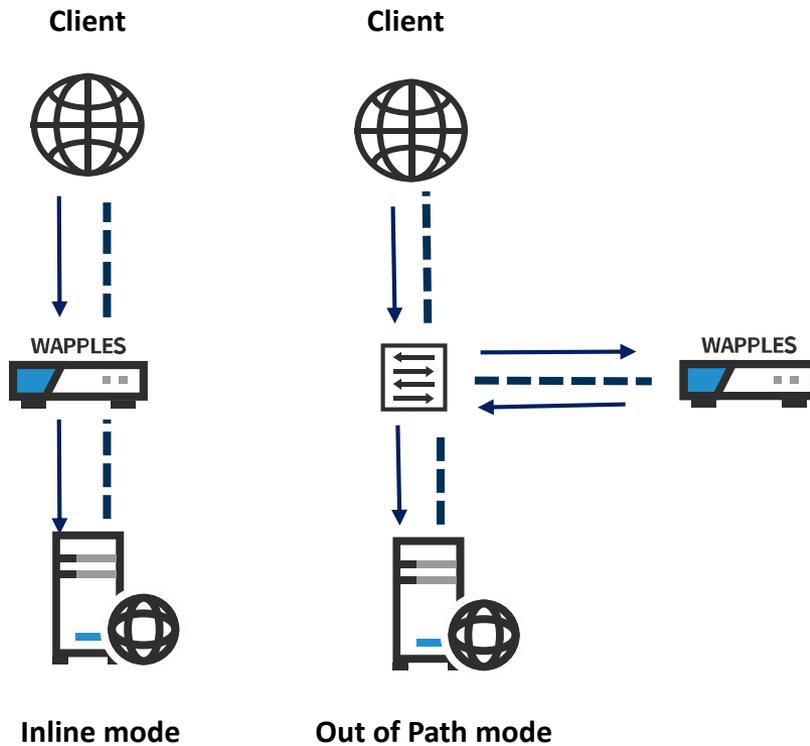
**Software (S/W) Bypass** : The network traffic will be bypassed at the Kernel (S/W) level without being touched by the Detection Engine.

**Hardware (H/W) Bypass** : The physical Network Interface Card(NIC) link downtime occurs. The network traffic



# Support for Inline & Proxy Deployment

WAPPLES provides both inline (bridged) and proxy deployment



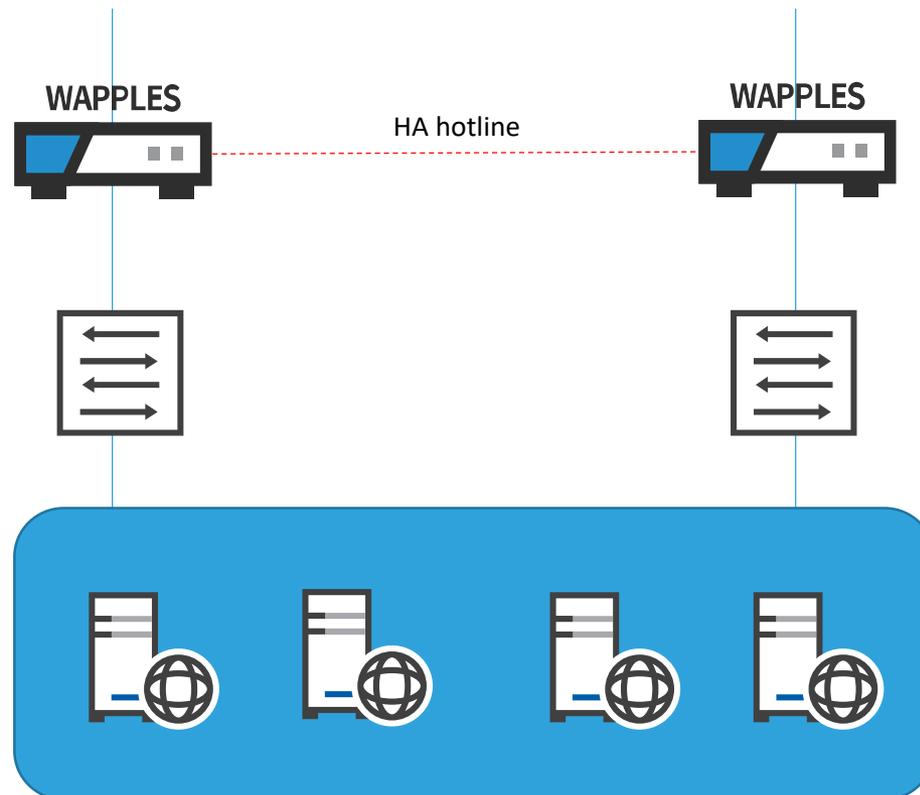
The screenshot shows the configuration interface for WAPPLES. The following fields are visible:

- Web Server IP: 192.168.20.103
- Web Server Port: 80
- Server Mode: Inline (selected in the dropdown menu, highlighted with a red box)
- Proxy IP: (empty field)
- Proxy Port: (empty field)
- Source IP Conservation:
- Certificate Settings: SSL Disable (selected in the dropdown menu)
- VLAN ID: (empty field)
- Certificate File: (empty field with a file selection icon)
- Private Key File: (empty field with a file selection icon)
- Mediation Certificate: (empty field with a file selection icon)
- Client Authentication: (empty field with a file selection icon)

Buttons for Update and Cancel are located at the bottom right of the configuration window.

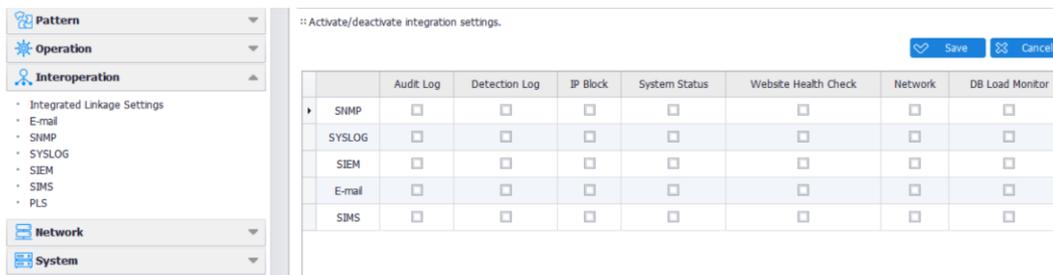
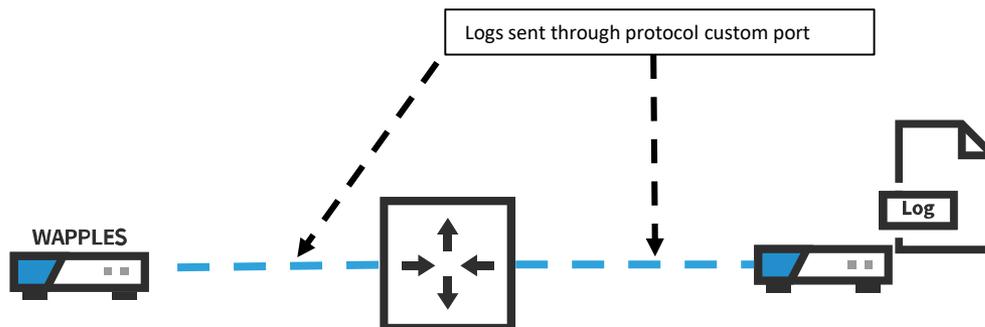
## Support for High Availability deployment with cross-failover

- Two appliances are protecting different network legs, and sharing TCP session information via “HA hotline”.
- The deployment can be “active-active” (both appliances detecting traffic) or “active-standby” (only one appliance is working, the other waiting for the other one to have an issue.)



# Support for External Logging

- Most modern network and security products support remote logging protocols which enable them to send logs to remote event management solutions such as SIEM.
- WAPPLES supports a number of standard and proprietary protocols to send detection logs, audit logs, system information, etc.
- Standard protocols supported by WAPPLES:
  - Syslog
  - SNMP
  - Email
- Proprietary integration:
  - Archsight (HPE)
  - Splunk



WAPPLES external logging can be configured on the GUI

# WAPPLES Графический интерфейс управления

- Предопределенные политики делают WAPPLES по существу решением plug-and-play
- Ежедневное управление осуществляется с помощью подробных журналов и редактируемой системы управленческой отчетности

The screenshot displays the WAPPLES Management interface with several overlapping windows and panels:

- Main Dashboard:** Shows the WAPPLES logo, navigation tabs (New Tab, Wizard, Dashboard, Detection Log, Audit Log, Graph, Report, Policy, Settings), and a "Detection Status" section with a note: "The controls on this tab enables you to set policies and websites to be used in WAPPLES."
- Policy and Websites List:** A tree view on the left shows various security policies, including "6.Unconditional Block", "5.PCI-DSS Security Level", "4.Advanced Security Level", "3.Standard Security Level", "2.Basic Security Level", "1.Detection Only, No-block", and "0.All-pass without detection".
- Policy Name:test:** A table showing detection rules and countermeasures:
 

Rule Name	Detection	Countermeasure
Buffer Overflow	Custom settings	Detection Only
Cookie Poisoning	Do not detect	Detection Only
Cross Site Scripting	Custom settings	Detection Only
Directory Listing	Detect suspicious page	Detection Only
- Log Details:** A table showing log entry details:
 

Field	Value
Policy	test
Rule	SQL Injection
Source Addr...	192.168.10.1:11381
- Data Stream:** Shows raw data for a request:
 

```
Raw Data: /webshelltest/dxshell_hk.php?%3D&hfile=C%3A%2FAPM_Setup%2Fhtdocs%2Fwebshelltest%2Findex.htm%22%20and%201%3D%40%40version&dxmode=F_DWN
```
- WAPPLES Summary Report:** A central dashboard with multiple charts and tables:
  - Summary of Detection Log per WAPPLES Rule:** A table with columns: Rule, No., Incidents, Percentage.
  - Top 10 Detection Rules:** A list of rules with their respective counts.
  - Global Hosts Distribution:** A world map showing incident locations.
  - WAPPLES Summary Report (Top 10 Detections per WAPPLES Rule):** A bar chart showing detection rates for various rules like Buffer Overflow (1%), Cookie Poisoning (2%), Error Handling (12%), etc.
  - WAPPLES Summary Report (Detections per OWASP 2015):** A bar chart showing detection rates for OWASP categories like Broken Access Control (20%), Broken Authentication (15%), etc.
  - LES Summary Report:** A pie chart showing the distribution of detected attacks across categories like WAF Bypass (3.1%), Missing Server Operation (4.0%), etc.
- Detection Events:** A table showing a list of detected incidents with columns for Date, Source, and Rule.
- Top 5 Countries:** A table showing the top countries for detected incidents, with "Unknown" having 371590 incidents.
- Top 5 Policies:** A table showing the top policies, with "test" having 371590 incidents.
- Top 5 Attacker IPs:** A table showing the top attacker IP addresses, with "192.168.10.1" having 371590 incidents.

**Кто уже использует?**

## Используется

### National Tax Service (S. Korea)

- One of the tax organizations in S. Korea
- Deployed to protect main web service from web attacks



### Ministry of Health (Malaysia)

- Responsible for health system: medical research and patient safety
- Deployed to protect web service and medical information



### Maritime Port Authority

- Regulates and manages port and marine services, facilities and activities
- Deployed to protect web service and related vulnerabilities



## Используется

### Samsung group(South Korea)

- Conglomerate company
- As a part of standardization of IT and security infrastructure, WAPPLES deployed to all subsidiary company by policy of Samsung IT subsidiary co Samsung SDS in South Korea



### LG Electronics(South Korea)

- A subsidiary company of LG group, manufacturer for home appliar IT device and mobile
- Deployed to protect customer and internal webservice against from external attack



### ASTRA International Tbk.(Indonesia)

- Holding company to deal in automotive, financial services, heavy equipment, agribusiness, information technology
- Deployed to protect internal webservice against from external attack



# Appendix

# Подбор оборудования WAPPLES

## Основные вопросы выбора модели оборудования

1. Сколько хитов на страницах сайта в пиковые нагрузки?

**Выберите модель, максимальная пропускная способность которой достаточна для покрытия входящего / исходящего трафика.**

**Общее количество запросов и ответов HTTP в пиковое время не должно превышать TPS WAPPLES.**

2. Необходимо ли использовать оптические байпасы в сетевой инфраструктуре?

**Выберите модель WAPPLES-700 или выше для поддержки сетевого интерфейса оптического байпаса.**

3. Нужны ли интерфейсы 10G (SFP+)?

**Выберите модель WAPPLES-2400 или выше с поддержкой байпас интерфейсов 10G**

## Reference Table

Class	Value	Performance			High-End	
Model	WAPPLES-700	WAPPLES-1400	WAPPLES-2400	WAPPLES-4000	WAPPLES-5200	WAPPLES-10000
Maximum Throughput	500 Mbps	1Gbps	2 Gbps	4 Gbps	5 Gbps	8 Gbps
HTTP TPS	35,000	70,000	100,000	150,000	200,000	250,000
HTTPS TPS	15,000	27,000	35,000	45,000	60,000	80,000
Specification	<ul style="list-style-type: none"> <li>HA Support</li> <li>1G Copper bypass</li> <li>1G Optical bypass</li> <li>VLAN Tagging</li> </ul>	<ul style="list-style-type: none"> <li>HA Support</li> <li>1G Optical bypass</li> <li>1G Copper bypass</li> <li>VLAN Tagging</li> <li>Redundant RSU</li> </ul>	<ul style="list-style-type: none"> <li>HA Support</li> <li>1G Copper bypass</li> <li>1G Optical bypass</li> <li>10G Optical bypass</li> <li>VLAN Tagging</li> <li>Redundant RSU</li> </ul>	<ul style="list-style-type: none"> <li>HA Support</li> <li>1G Copper bypass</li> <li>1G Optical bypass</li> <li>10G Optical bypass</li> <li>VLAN Tagging</li> <li>Redundant RSU</li> </ul>	<ul style="list-style-type: none"> <li>HA Support</li> <li>1G Copper bypass</li> <li>1G Optical bypass</li> <li>10G Optical bypass</li> <li>VLAN Tagging</li> <li>Redundant RSU</li> </ul>	<ul style="list-style-type: none"> <li>HA Support</li> <li>1G Copper bypass</li> <li>1G Optical bypass</li> <li>10G Optical bypass</li> <li>VLAN Tagging</li> <li>Redundant RSU</li> </ul>

# WAPPLES Виртуальные устройства для Публичных и Приватных облаков

## Cloud platform



**SOFTLAYER®**

## Hypervisor



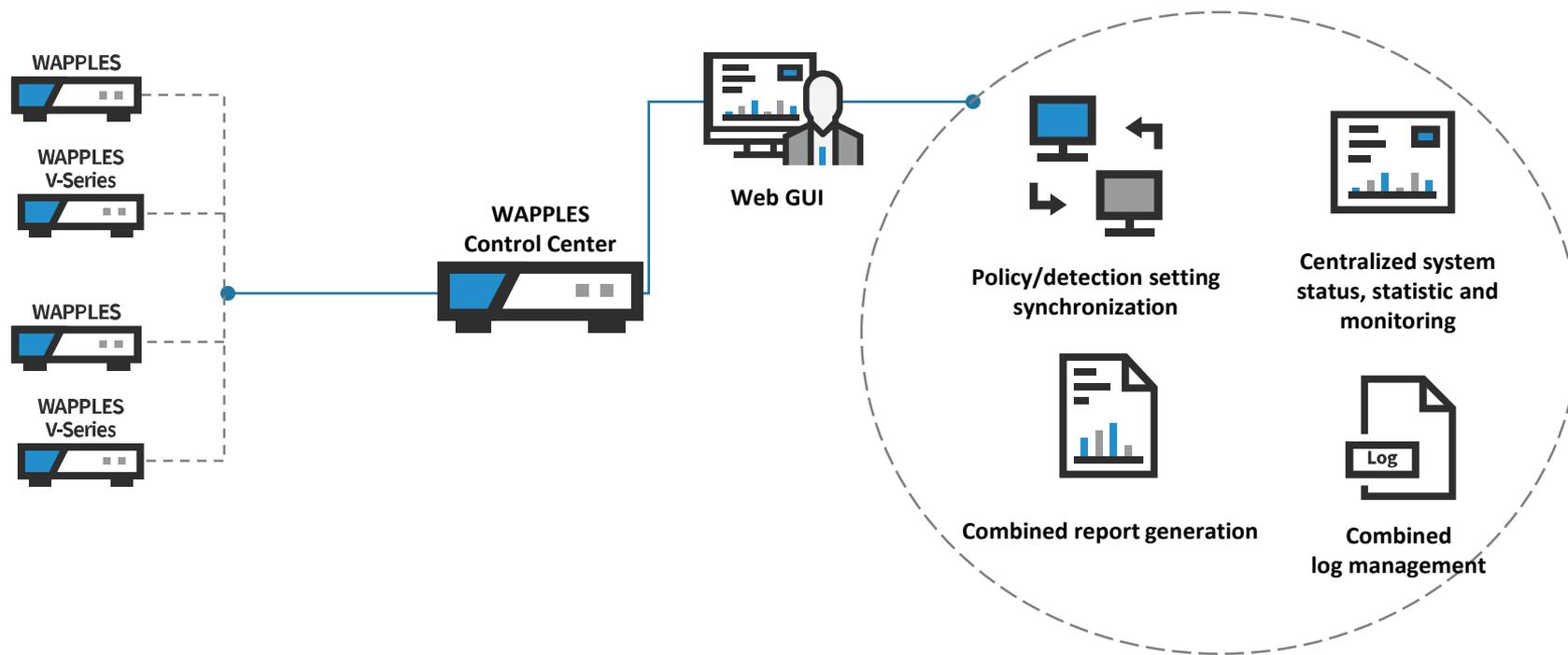
Windows Server  
Hyper-V™



# WAPPLES Control Center

Центр управления WAPPLES - это интегрированная система управления для нескольких WAPPLES.

- ✓ Когда в одной сети существуют различные типы развертывания, управление каждой из них по отдельности может быть большой проблемой
- ✓ Центр управления WAPPLES позволяет вам управлять несколькими WAPPLES (Appliance & Virtual Machine)





t h a n k   y o u

**Penta**SECURITY

Инженер по Информационной Безопасности  
Илья Головацкий  
email: ilg@muk.ua