

Воркшоп по настройке защиты веб-приложений в облаке



Во время воркшопа вы научитесь настраивать облачную защиту веб-приложений с помощью [Smart Web Security \(SWS\)](#):

- Настраивать [профили безопасности](#) SWS с использованием базовых правил и правил Smart Protection
- Настраивать правила [Web Application Firewall \(WAF\)](#) для защиты от эксплуатации уязвимостей приложения
- Настраивать правила [Advanced Rate Limiter \(ARL\)](#) для контроля и ограничения нагрузки на веб-приложение
- Проверять работоспособность настроенной защиты веб-приложений

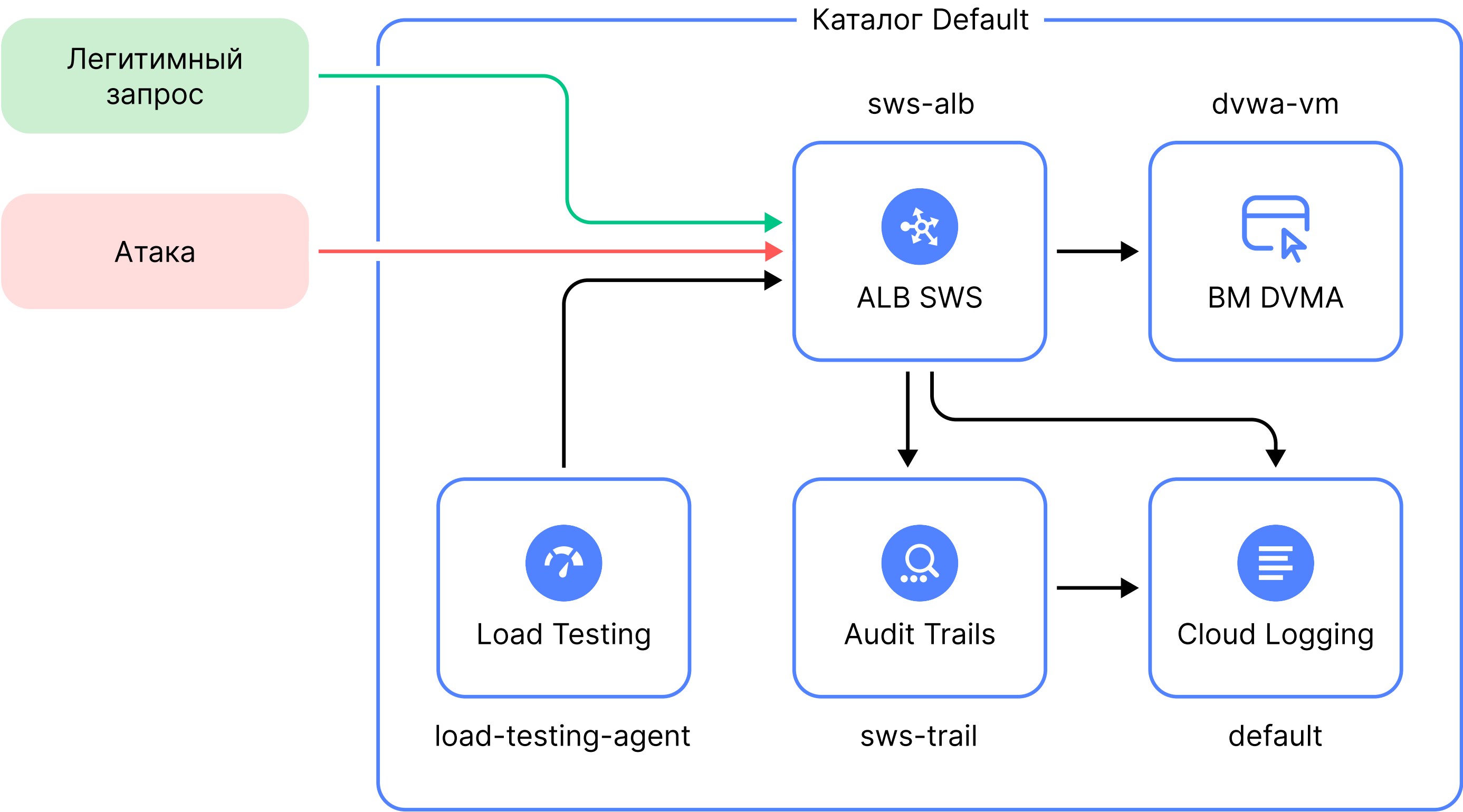
Схема лабораторного стенда и справочная информация

В облаке Yandex Cloud в каталоге default для вас предварительно развёрнуты ресурсы:

- Балансировщик [Application Load Balancer \(ALB\)](#) с публичным IP-адресом, через который публикуется уязвимое веб-приложение [Damn Vulnerable Web Application \(DVWA\)](#). Целевым ресурсом для ALB является виртуальная машина (VM) с уязвимым приложением
- Трейл [Audit Trails](#) с настроенными событиями уровня сервиса SWS
- Лог-группа default в [Cloud Logging](#) для хранения и анализа логов ALB и событий Audit Trails
- Агент [Load Testing](#) для генерации тестовой нагрузки на приложение

Остались вопросы?

Свяжитесь с вашим менеджером в Yandex Cloud для получения подробной информации.



Название	Описание
Каталог default	Каталог с ресурсами демостенда
sws-alb	Балансировщик ALB, который используется для публикации приложения и его защиты с помощью SWS
dvwa-vm	ВМ с публикуемым уязвимым приложением DVWA. ВМ является целевым ресурсом для целевой группы ALB
sws-trail	Трейл Audit Trails, в который поступают события уровня сервиса SWS
Лог-группа default	Лог-группа Cloud Logging, в которую поступают логи ALB и события трейла Audit Trails. Используется для поиска и анализа угроз и атак на приложение
load-testing-agent	Агент Load Testing для генерации нагрузки на приложение

Остались вопросы?

Свяжитесь с вашим менеджером в Yandex Cloud для получения подробной информации.

Перед началом работы со стендом

- Не превышайте нагрузку в тестах Load Testing свыше рекомендованной в инструкции

Как подключиться к облаку для выполнения заданий

Название	Значение
Ссылка на страницу входа в консоль управления	console.yandex.cloud/federations

Если в консоли управления используется английский язык, то измените его на русский:

1. В консоли управления, на панели слева, выберите раздел **Settings**.
2. Перейдите в раздел **Language and region**.
3. Выберите русский язык для консоли управления.

Как подключиться к веб-приложению DVWA

Название	Значение
Порт	TCP 443
Username	admin
Password	password

Настройка приложения DVWA для первого использования

1. Откройте в браузере интерфейс веб-приложения DVWA и авторизуйтесь, используя информацию из таблицы выше.
2. Появится страница **Database Setup** для инициализации базы данных. Внизу страницы нажмите кнопку **Create Database / Reset Database**.

3. После инициализации базы данных произойдёт перенаправление на страницу логина. Введите логин/пароль: admin/password. Откроется страница **Welcome to Damn Vulnerable Web Application!**
4. В левом меню нажмите на **DVWA Security**, в выпадающем списке выберите низкий уровень безопасности **Low** и нажмите **Submit**.

Настройка профиля безопасности SWS

1. В консоли управления Yandex Cloud в списке сервисов выберите **Smart Web Security**. Перейдите в левом меню на вкладку **Профили безопасности**.
2. Нажмите кнопку **Создать профиль**, выберите **По преднастроенному шаблону** и заполните поля:
 - Имя профиля: **sws**
 - Действие для базового правила по умолчанию: **Запретить**
 - SmartCaptcha: **По умолчанию**
 - В разделе **Обучение ML-моделей** включите или отключите использование информации об HTTP-запросах для улучшения моделей машинного обучения
 - Анализировать тело запроса (макс. 8 КБ): **Включить**
 - При превышении макс. размера: **Не анализировать тело запроса**
 - Нажмите **Создать профиль**
3. Перейдите в левом меню на вкладку **Профили WAF** и нажмите **Создать профиль WAF**:
 - Имя профиля: **waf**
 - Нажмите **Создать**
4. После создания профиля нажмите **Настроить набор базовых правил**:
 - Порог аномальности: выберите **Своё значение**. Укажите **15**
 - Нажмите **Сохранить настройки**
5. Перейдите в левом меню на вкладку **Профили безопасности** и выберите созданный ранее профиль безопасности.
6. Нажмите кнопку **Добавить правило**:
 - Имя правила: **waf-rule**
 - Приоритет: **1000**

- Тип правила: **Web Application Firewall**
- Профиль WAF: выберите созданный ранее профиль WAF
- Действие: **Полная защита**
- Трафик: **При условии**
- Условия: **Request URI**
- Request path: выберите **Начинается с** и укажите `/vulnerabilities`
- Нажмите **Добавить**

7. Для защиты веб-приложения от резкого увеличения нагрузки и сохранения работоспособности сервиса настройте функциональность [ARL](#). Перейдите в левом меню на вкладку **Профили ARL** и нажмите **Создать профиль ARL**:

- Имя профиля: **arl**
- Нажмите **Добавить правило**
- Имя правила: **rate-limit**
- Приоритет: **1000**
- Трафик: **Весь трафик**
- Группировать запросы: **Без группировки**
- Лимит запросов: **100 запросов за 1 с**
Все запросы сверх лимита будут блокироваться
- Действие: **Блокировать запросы свыше лимита**
- Нажмите **Сохранить правило**
- Нажмите **Создать**

8. Перейдите в левом меню на вкладку **Профили безопасности** и выберите созданный ранее профиль безопасности. Нажмите **Редактировать**. В поле **Профиль ARL** выберите созданный профиль ARL. Нажмите **Сохранить**.

9. Проверьте настройки правил безопасности в созданном профиле безопасности в соответствии с информацией в [Приложении](#). Если они отличаются, приведите их в соответствие.

Остались вопросы?

Свяжитесь с вашим менеджером в Yandex Cloud для получения подробной информации.

Подключите профиль безопасности SWS к виртуальному хосту HTTP-роутера ALB

1. Перейдите в левом меню на вкладку **Профили безопасности** и выберите созданный ранее профиль безопасности.
2. Во вкладке **Подключённые хосты** нажмите **Подключить к хосту**.
Выберите следующие ресурсы для подключения профиля безопасности SWS к виртуальному хосту HTTP-роутера ALB:
 - Балансировщик: **sws-alb**
 - HTTP-роутер: **alb-http-router**
 - Виртуальный хост: **dvwa-domain**
3. Нажмите **Подключить**.

Демонстрация WAF

Атака Reflected Cross Site Scripting (XSS)

1. Подключитесь к приложению, используя информацию в разделе [Как подключиться к приложению DVWA](#).
2. В левом меню выберите **XSS (Reflected)**.
3. В поле **What's your name?** укажите:
`<img ""><script>alert("XSS")</script>"\>`
4. Нажмите **Submit**.
5. WAF заблокирует запрос, и будет получен HTTP-ответ с кодом 403, в браузере отобразится страница **Access to our service has been temporarily blocked**.
6. В консоли управления Yandex Cloud зайдите в сервис **Cloud Logging**, выберите группу **default** и перейдите на вкладку **Логи**.
7. В поле **Запрос** укажите выражение для отображения запросов, заблокированных правилами WAF из профиля безопасности:
`json_payload.smartwebsecurity.matched_rule.rule_type = WAF and
json_payload.smartwebsecurity.matched_rule.verdict = DENY`
8. Раскройте запись в логах для просмотра детальной информации.

9. В поле **Запрос** укажите выражение для отображения событий Audit Trails при срабатывании правил из профиля WAF:

```
json_payload.event_type =  
"yandex.cloud.audit.smartwebsecurity.WafMatchedRule" and  
json_payload.details.verdict = DENY
```

10. Раскройте запись в логах для просмотра детальной информации.

Атака SQL Injection

1. Подключитесь к приложению, используя информацию в разделе [Как подключиться к приложению DVWA](#).

2. В левом меню выберите **SQL Injection**.

3. В поле **User ID** укажите:

```
`%' and 1=0 union select null, concat(user,':',password) from users #`
```

4. Нажмите **Submit**.

5. WAF заблокирует запрос, и будет получен HTTP-ответ с кодом 403, в браузере отобразится страница **Access to our service has been temporarily blocked**.

6. В консоли управления Yandex Cloud зайдите в сервис **Cloud Logging**, выберите группу default и перейдите на вкладку **Логи**.

7. В поле **Запрос** укажите выражение для отображения запросов, заблокированных правилами WAF из профиля безопасности:

```
json_payload.smartwebsecurity.matched_rule.rule_type = WAF and  
json_payload.smartwebsecurity.matched_rule.verdict = DENY
```

8. Раскройте запись в логах для просмотра детальной информации.

9. В поле **Запрос** укажите выражение для отображения событий Audit Trails при срабатывании правил из профиля WAF:

```
json_payload.event_type =  
"yandex.cloud.audit.smartwebsecurity.WafMatchedRule" and  
json_payload.details.verdict = DENY
```

10. Раскройте запись в логах для просмотра детальной информации.

Демонстрация Smart Protection

1. В консоли управления Yandex Cloud зайдите в сервис **Load Testing / Агенты** и выберите load-testing-agent. Проверьте, что статус у агента **Ready for test**. Если статус агента отличается от **Ready for test**, перезапустите агента.
2. Зайдите в сервис **Load Testing / Тесты** и нажмите **Создать тест**.
3. В поле **Агенты** выберите агента **load-testing-agent**.
4. В поле **Способ настройки** выберите **Конфигурационный файл**, вставьте конфигурацию ниже или нажмите **Прикрепить файл**, предварительно скачав файл agent-test.yaml с конфигурацией теста по [ссылке](#). В конфигурации теста замените <домен_приложения> на значение в разделе [Как подключиться к приложению DVWA](#):

```
pandora:
  enabled: true
  package: yandextank.plugins.Pandora
  config_content:
    pools:
      - id: HTTP
    discard_overflow: true
    gun:
      type: http # Протокол
      target: <домен_приложения>:443 # см. раздел
        "Как подключиться к приложению DVWA"
      ssl: true
    ammo:
      type: uri
      uris:
        - /login.php # URI в запросах
    result:
      type: phout
      destination: ./phout.log
    rps:
      - duration: 120s # Время подачи нагрузки
      type: const # Тип нагрузки: постоянная
      ops: 150 # RPS нагрузки
    startup:
      type: once
      times: 1000 # Количество тестирующих потоков
core: {}
autostop:
  enabled: true
  package: yandextank.plugins.Autostop
```

autostop:

- limit (5m) # предельное время работы теста 5 мин
- instances(90%,60s) # Завершение теста, если в течение 60 секунд будет занято 90%
- # тестирующих потоков, что свидетельствует о возникновении
- # проблем тестирования.

5. Нажмите **Создать**.

6. После начала теста во вкладке **Результаты теста** на графике **HTTP-коды ответов** наблюдайте за количеством ответов в секунду со статус-кодом 302. Профиль безопасности SWS перенаправляет запросы от агента на капчу.

7. Зайдите в сервис **Cloud Logging**, выберите группу **default** и перейдите на вкладку **Логи**.

8. В поле **Запрос** укажите выражение для отображения запросов, для которых сработали правила с отправкой на капчу:

```
json_payload.smartwebsecurity.matched_rule.rule_type =  
SMART_PROTECTION and  
json_payload.smartwebsecurity.matched_rule.verdict = CAPTCHA
```

9. Раскройте запись в логах для просмотра детальной информации.

10. Зайдите в профиль безопасности sws и в левом меню перейдите на вкладку **Мониторинг**. На графике будет отображён **Redirected to SmartCaptcha RPS**.

Демонстрация ARL

Правила ARL применяются к трафику, который уже прошёл проверку правил из профиля безопасности. Поэтому необходимо добавить правило, которое «обелит» трафик генератора нагрузки Load Testing, чтобы продемонстрировать работу ARL.

1. В консоли управления Yandex Cloud зайдите в сервис **Virtual Private Cloud / IP-адреса** и скопируйте публичный IP-адрес с именем public-ip-load-testing, который принадлежит агенту Load Testing.

2. Зайдите в сервис **Smart Web Security / Профили безопасности** и выберите профиль безопасности **sws**.

3. Нажмите **Добавить правило** и заполните поля:

- Имя: **allow-load-testing**
- Приоритет: **90**
- Тип правила: **Базовое**
- Действие: **Разрешить**

- Действие: **Разрешить**
 - Трафик: **При условии**
 - Условия: **IP → Совпадает или принадлежит диапазону**
 - **Совпадает или принадлежит диапазону**: укажите публичный IP-адрес агента Load Testing, полученный в шаге 1
 - Нажмите **Добавить**
4. Зайдите в сервис **Load Testing / Агенты**. Проверьте, что агент load-testing-agent имеет статус **Ready for test**. Если статус агента отличается от **Ready for test**, перезапустите агента.
 5. Зайдите в сервис **Load Testing / Тесты**, у созданного ранее теста нажмите ... и выберите **Перезапустить** для повторения нагрузки, настроенной в тесте во время [демонстрации Smart Protection](#).
 6. После начала теста во вкладке **Результаты теста** на графике **HTTP-коды ответов** наблюдайте за количеством ответов в секунду со статус-кодами 200 и 429. Все запросы свыше лимита, установленного в правилах профиля ARL, будут блокироваться (будет возвращена ошибка 429).
 7. Зайдите в сервис **Cloud Logging**, выберите группу **default** и перейдите на вкладку **Логи**.
 8. В поле **Запрос** укажите выражение для отображения запросов, заблокированных правилами профиля ARL:
`json_payload.smartwebsecurity.advanced_rate_limiter.verdict = DENY`
 9. Раскройте запись в логах для просмотра детальной информации.
 10. Зайдите в профиль безопасности sws и в левом меню перейдите на вкладку **Мониторинг**. На графиках **Denied by ARL Profile RPS** и **Allowed by ARL Profile RPS** будет отображён rate запросов, заблокированных и разрешённых профилем ARL.

Лучшие практики по настройке защиты SWS

Приводим примеры дополнительных настроек профиля безопасности SWS для наиболее часто встречающихся сценариев защиты веб-приложений.

Для выполнения настроек в [консоли управления](#) Yandex Cloud в списке сервисов выберите **Smart Web Security**. Предварительно должен быть [создан профиль безопасности SWS](#) по преднастроенному шаблону. К профилю безопасности должен быть подключён профиль ARL.

Правила в профиле безопасности и профиле ARL выполняются на основе приоритета. Чем меньше значение параметра приоритета, тем больший приоритет у правила. Приоритеты преднастроенных правил в профиле безопасности:

- Правило Smart Protection с полной защитой: 999900
- Базовое правило по умолчанию: 1000000



«Обеление» трафика бизнес-партнёров

При соблюдении правила Smart Protection в режиме полной защиты API-вызовы ваших бизнес-партнёров будут отправляться на капчу и блокироваться, поэтому необходимо для таких эндпойнтов сделать более щадящий режим SWS — защиту API.

В этом режиме работают наиболее достоверные и проверенные правила, которые блокируют нелегитимный трафик. Остальные запросы будут проходить без отправки в капчу.

Добавьте базовые правила, разрешающие трафик бизнес-партнёров к вашему веб-приложению с IP-адресов бизнес-партнёров и с определёнными HTTP header.

1. Перейдите в левом меню на вкладку **Профили безопасности** и выберите профиль безопасности.
2. Нажмите **Добавить правило**:
 - Имя правила: **business-partner-ip-rule**
 - Приоритет: укажите приоритет
 - Тип правила: **Базовое**
 - Действие: **Разрешить**
 - Трафик: **При условии**
 - Условия: **IP → Совпадает или принадлежит диапазону**
 - **Совпадает или принадлежит диапазону**: укажите диапазон IP-адресов бизнес-партнёра. Допустимые значения: IP-адрес, префикс, диапазон адресов. Например, 1.2.33.44, 1.2.3.0/24, 1.2.0.0–1.2.1.1.
 - Для добавления дополнительных IP-диапазонов бизнес-партнёра нажмите + или **Добавить**
 - Также мы рекомендуем использовать функциональность [Списки](#). В этом случае одним правилом можно добавить в исключения все IP-адреса из пользовательского списка.

3. Нажмите **Добавить правило**:

- Имя правила: **business-partner-header-rule**
 - Приоритет: укажите приоритет
 - Тип правила: **Базовое**
 - Действие: **Разрешить**
 - Трафик: **При условии**
 - Условия: **HTTP header**
 - **HTTP header**: укажите HTTP header, согласованный для использования с бизнес-партнёром. Например, partner.
 - Выберите условие соответствия для HTTP header и укажите его значение. Например, **Совпадает с** и значение partner-abc.
 - Для добавления дополнительных значений HTTP header для бизнес-партнёра нажмите + или **Добавить**
4. Рекомендуется дополнительно «обелить» трафик бизнес-партнёра в профиле ARL. Решение применимо в случае, если вы исключаете возможность абыюза ручек API со стороны партнёров.

Перейдите в левом меню на вкладку **Профили ARL** и выберите профиль ARL. Далее в каждом из ранее созданных правил необходимо отредактировать условие на матчинг трафика:

- Трафик: **При условии**
- Условия: **IP → Совпадает или принадлежит диапазону**
- **Совпадает или принадлежит диапазону**: укажите диапазон IP-адресов бизнес-партнёра. Допустимые значения: IP-адрес, префикс, диапазон адресов. Например, 1.2.33.44, 1.2.3.0/24, 1.2.0.0–1.2.1.1.
- Альтернативно можно выбрать условие: **IP не принадлежит списку**
- **IP не принадлежит списку**: выбрать пользовательский список с IP-адресами бизнес-партнёров (при наличии)
- Нажмите **Сохранить правило**



Блокировка запросов из списков is_ddoser, is_tor, is_anonymous

[Списки Yandex Cloud](#) — это предустановленные наборы IP-адресов, собранные по определённому признаку. Эти списки регулярно обновляются и предоставляются как часть функционала SWS. Цель таких списков — составить индивидуальную стратегию безопасности и автоматически блокировать потенциально опасный трафик.

Добавьте базовое правило, запрещающее запросы с IP-адресами из [списков](#) is_ddoser (список IP-адресов, которые участвовали в DDoS-атаках), is_tor (IP-адреса сети TOR, которая используется для анонимизации трафика), is_anonymous (IP-адреса анонимных сетей, которые часто используются для сокрытия личности).

1. Перейдите в левом меню на вкладку **Профили безопасности** и выберите профиль безопасности.
2. Нажмите **Добавить правило**:
 - Приоритет: укажите приоритет
 - Тип правила: **Базовое**
 - Действие: **Запретить**
 - Трафик: **При условии**
 - Условия: **IP → IP не принадлежит списку → is_ddoser**
 - Нажмите + для добавления ещё одного списка и выберите **is_tor**
 - Нажмите + для добавления ещё одного списка и выберите **is_anonymous**
 - Нажмите **Добавить**

В качестве более щадящей меры безопасности возможно создать правило с действием **Показать капчу** для запросов с IP-адресов, принадлежащих этим спискам.

Остались вопросы?

Свяжитесь с вашим менеджером в Yandex Cloud для получения подробной информации.

Защита API от резкого увеличения нагрузки

Для защиты API от резкого увеличения нагрузки и сохранения работоспособности приложения рекомендуется настроить подключённый ARL-профиль на число запросов с уникального IP-адреса.

Перейдите в левом меню на вкладку **Профили ARL** и выберите профиль ARL. Нажмите **Добавить правило**:

- Приоритет: укажите приоритет
- Трафик: **При условии**
- Условия: **Request URI**
- Request path: выберите **Начинается с** и укажите путь ручки API, например /public-api/
- Группировать запросы: **По характеристикам**
- Характеристика: **IP адрес**
- Лимит запросов на группу: задайте лимит запросов с уникального IP-адреса, а также временной интервал, за который рассчитывать лимит. Ко всем запросам сверх лимита будет применяться действие
- Действие: **Блокировать все запросы в группе свыше лимита**
- Нажмите **Сохранить правило**

В дополнении к ARL-правилу на ограничение числа запросов с уникального IP-адреса хорошей практикой будет настройка общего лимита запросов на ручку API (смотрите пример настройки правила ARL в шаге 7 раздела [Настройки профиля безопасности SWS](#)). При создании правила можно задать условие трафика на основе Request URI, соответствующее URI защищаемой ручки API.

Остались вопросы?

Свяжитесь с вашим менеджером в Yandex Cloud для получения подробной информации.



Защита от brute-force-атак

Для защиты веб-приложения от brute-force-атаки (перебора паролей) рекомендуется настроить подключённый ARL-профиль на ограничение количества запросов с уникального IP-адреса. Все запросы сверх установленного лимита будут блокироваться.

Перейдите в левом меню на вкладку **Профили ARL** и выберите профиль ARL.

Нажмите **Добавить правило:**

- Приоритет: укажите приоритет
- Трафик: **При условии**
- Условия: **Request URI**
- Request path: выберите **Начинается с** и укажите путь страницы для ввода паролей, например /login/
- Группировать запросы: **По характеристикам**
- Характеристика: **IP-адрес**
- Лимит запросов на группу: задайте лимит запросов с уникального IP-адреса, а также временной интервал, за который рассчитывать лимит. Например, 15 запросов в час. Ко всем запросам сверх лимита будет применяться действие.
- Действие: **Блокировать все запросы в группе выше лимита**
- Нажмите **Сохранить правило**



Правила для трафика из регионов, от которых ваше веб-приложение не ожидает трафика

Вы можете добавить базовое правило в профиль безопасности для отправки на капчу или блокировку запросов из регионов, от которых ваш сервис не ожидает трафика. Альтернативным и менее жёстким вариантом может быть добавление правила в подключённый ARL-профиль для ограничения количества запросов из этих регионов.

Вариант с базовым правилом для отправки на капчу или блокировки запросов:

1. Перейдите в левом меню на вкладку **Профили безопасности** и выберите профиль безопасности.
2. Нажмите **Добавить правило:**
 - Приоритет: укажите приоритет
 - Тип правила: **Базовое**

- Действие: выберите **Показать капчу** или **Запретить** в зависимости от требований к действиям с запросами
- Трафик: **При условии**
- Условия: **IP → IP принадлежит региону** → укажите регион
- Характеристика: **IP адрес**
- Для добавления дополнительных регионов нажмите + или **Добавить**

Вариант с правилом ARL-профиля для ограничения числа запросов:

1. Перейдите в левом меню на вкладку **Профили ARL** и выберите профиль ARL.
2. Нажмите **Добавить правило**:
 - Приоритет: укажите приоритет
 - Трафик: **При условии**
 - Условия: **IP → IP принадлежит региону** → укажите регион
 - Для добавления дополнительных регионов нажмите + или выберите группировку запросов **По характеристикам**
 - Характеристика: **IP-адрес**
 - Лимит запросов на группу: задайте лимит запросов с уникального IP-адреса, а также временной интервал, за который рассчитывать лимит. Ко всем запросам сверх лимита будет применяться действие.
 - Действие: **Блокировать все запросы в группе свыше лимита**
 - Нажмите **Сохранить правило**

Остались вопросы?

Свяжитесь с вашим менеджером в Yandex Cloud для получения подробной информации.

Для защиты от СМС-бомбинга при вызове метода API, отвечающего за отправку СМС пользователям веб-приложения, добавьте в профиль ARL правило, ограничивающее количество запросов с определёнными параметрами в строке запроса.

Перейдите в левом меню на вкладку **Профили ARL** и выберите профиль ARL.

Нажмите **Добавить правило**:

- Приоритет: укажите приоритет правила (например, высокий, чтобы оно применялось перед другими правилами)
- Трафик: **При условии**
- Условия: **Request URI**
- Request path: выберите **Начинается с** и укажите путь метода API для отправки СМС пользователям, например `/send-sms/`. Убедитесь, что путь указан корректно, включая возможные параметры, если они являются частью URI
- Группировать запросы: выберите **Query params**
- Группировать по: укажите значение параметра, в котором передаётся номер телефона пользователя (например, `phone`)
- Лимит запросов на группу: задайте лимит запросов с уникального IP-адреса, а также временной интервал, за который рассчитывать лимит. Например, 15 запросов в час. Ко всем запросам сверх лимита будет применяться действие.
- Действие: **Блокировать все запросы в группе свыше лимита**
- Нажмите **Сохранить правило**

Остались вопросы?

Свяжитесь с вашим менеджером в Yandex Cloud для получения подробной информации.

Приложение

 Правила безопасности в профиле безопасности SWS

Имя	Тип	Действие	Условия	Приоритет	Только логирование	Профиль WAF
waf-rule	Web Application Firewall	Полная защита	Request URI: начинается с /vulnerabilities/	1000	—	ID профиля WAF
sp-rule-1	Smart Protection	Полная защита	Весь трафик	999900	—	—
—	Базовое	Запретить	Весь трафик	1000000	—	—

Параметр	Значение
SmartCaptcha	По умолчанию
Профиль ARL	ID профиля ARL

 Скриншот из консоли управления

Обзор

Имя arl

Идентификатор fev92ea0

Описание —

Подключенные профили безопасности [sws](#)

Правила

Группировка

▼

+

Добавить правило

Имя / Описание	Условия на трафик	Группировать запросы по	Лимит запросов	Действие при превышении	Приоритет ↑	Только логирование	
rate-limit	Весь трафик	Без группировки	100 за 1 сек	 Блокировать только запросы свыше лимита	1000	—	...

Профиль WAF

 Набор базовых правил

Параметр	Значение
Набор	OWASP® Core Ruleset 4.0.0
Активных правил	149
Порог аномальности	15
Уровень паранойи	1

 Скриншот из консоли управления

Обзор

Имя SWS

Идентификатор few

Описание SWS demo

Метки

created_by : terraform-yc-module

Подключённые профили безопасности

Имя	Правила
sws	waf-protection

Набор базовых правил

Набор OWASP Core Ruleset 4.0.0

Активных правил 264

Порог аномальности 15

Уровень паранойи

1

Настроить набор базовых правил

Профиль ARL

Имя	Условия на трафик	Группировать запросы по	Лимит запросов	Действие при превышении	Приоритет	Только логирование
rate-limit	Весь трафик	Без группировки	100 за 1 с	Блокировать только запросы свыше лимита	1000	—

 Скриншот из консоли управления

Обзор

Имя sws

Описание SWS demo

Идентификатор few

Метки created_by : terraform-yc-module

SmartCaptcha По умолчанию

Профиль ARL [few](#)

Правила безопасности

Подключенные хосты

Фильтр по имени или описанию

Тип правила: Все (2) ▼

Действие: Все (1) ▼

+ Добавить правило

Имя ↑↓	Описание	Тип	Действие	Условия	Приоритет	
waf-protection	—	Web Application Firewall	 Полная защита	Request URL : начинается с /vulnerabilities	100	...
smart-protection	—	Smart Protection	 Полная защита	Весь трафик	200	...
—	Базовое правило по умолчанию ?	Базовое	 Запретить	Весь трафик	1000000	

Остались вопросы?

Свяжитесь с вашим менеджером в Yandex Cloud для получения подробной информации.