ЗАЩИТА ОБЛАЧНЫХ И МУЛЬТИОБЛАЧНЫХ СРЕД

BELYAEV

Директор по КБ: Беляев Дмитрий Александрович

Обо мне

- Более 10 лет в ИБ
- Имею более 150 сертификатов/ дипломов и благодарностей по тематике ИБ
- Руководил пятью стартапами по ИБ и командой из более 100 человек.
- Успешный проект: **Айда Гулять**
- Имею 3 образования (ИБ, юриспруденция, безопасная разработка)
- 2хПобедитель в рейтинге ТОП-100 Лидеров ИТ (GlobalCIO)
- Член клуба 4CIO;
- Член клуба GlobaCIO;
- Основатель клуба [**RTCL**] |The Club of Russia's Top Cybersecurity Leaders|.
- Имею за плечами более 80 выступлений на публику суммарной численностью >6000 человек (PHDay Fest, TADVISER, ТБ Форум, Территория Безопасности, CISO Форум, CNews, ITsec, Security Summit, Код ИБ, ТБ, SmartGoPro и т.д)
- Амбассадор платформы «Цифровой прорыв» в 2021-2022

Дмитрий Александрович Беляев

Директор по Кибербезопасности (CISO)

ОСНОВНЫЕ УГРОЗЫ ДЛЯ ОБЛАЧНЫХ СРЕД

1. Потеря или утечка данных
2. Несанкционированный доступ к сервисам
3. Нарушения конфиденциальности и целостности информации
4. DDoS-атаки и угрозы со стороны вредоносного ПО
5. Ошибки конфигурации и уязвимости приложений

СТАТИСТИКА ИНЦИДЕНТОВ 2024 ГОДА

1. **Фишинг -33% всех инцидентов**
2. **Скомпрометированные УЗ — 28% случаев**
3. **Атаки на публичные приложения**

Цели:

1. Остановка бизнес-процессов

2. Доступ к базам данных и S3-хранилищам

3. Атаки на цепочки поставок для майнинга, DDoS и C2

***По данным IBM X-Force Cloud Threat Landscape Report 2024**

ПРАКТИЧЕСКИЕ КЕЙСЫ НАРУШЕНИЙ БЕЗОПАСНОСТИ

1. Amazon S3 (2018) =25% утечек
2. DIKIDI (2023) = 40 млн клиентов CRM
3. 90% утечек — человеческие ошибки
4. 11% утечек - действия провайдера
5. 99% облачных пользователей имеют избыточные права

amazon

DIKIDI

Доля заказных кибератак на российские компании к августу 2024 года значительно выросла, достигнув 44%

СОВРЕМЕННЫЕ РЕШЕНИЯ И ЛУЧШИЕ ПРАКТИКИ

Приоритетные меры защиты

СОВРЕМЕННЫЕ ТЕХНОЛОГИЧЕСКИЕ РЕШЕНИЯ

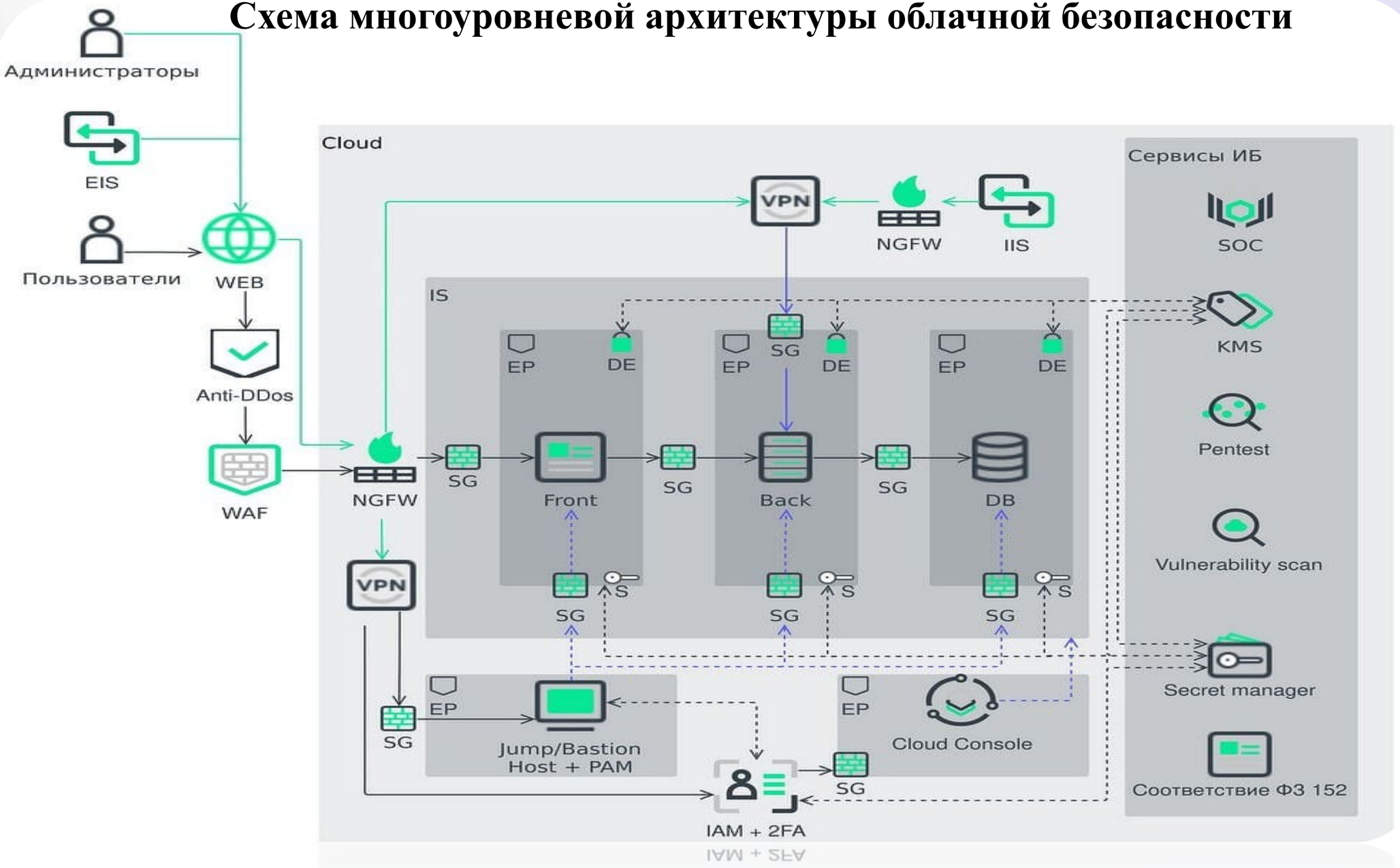
Cloud Security Posture Management (CSPM): Решения CSPM защищают рабочие нагрузки от угроз извне, оценивая плоскость управления облачной платформы

Cloud Workload Protection Platform (CWPP): CWPP унифицирует управление сервисами нескольких облачных провайдеров и помогает защитить согласованность рабочих нагрузок.

Zero Trust: Zero Trust — это модель ИТ-безопасности, которая требует строгой авторизации для каждого пользователя и устройства, пытающихся получить доступ к ресурсам в частной сети.

SASE (Secure Access Service Edge): SASE объединяет сетевое взаимодействие и безопасность в единый облачный сервис, который сопровождает пользователей и данные в разных средах

Схема многоуровневой архитектуры облачной безопасности

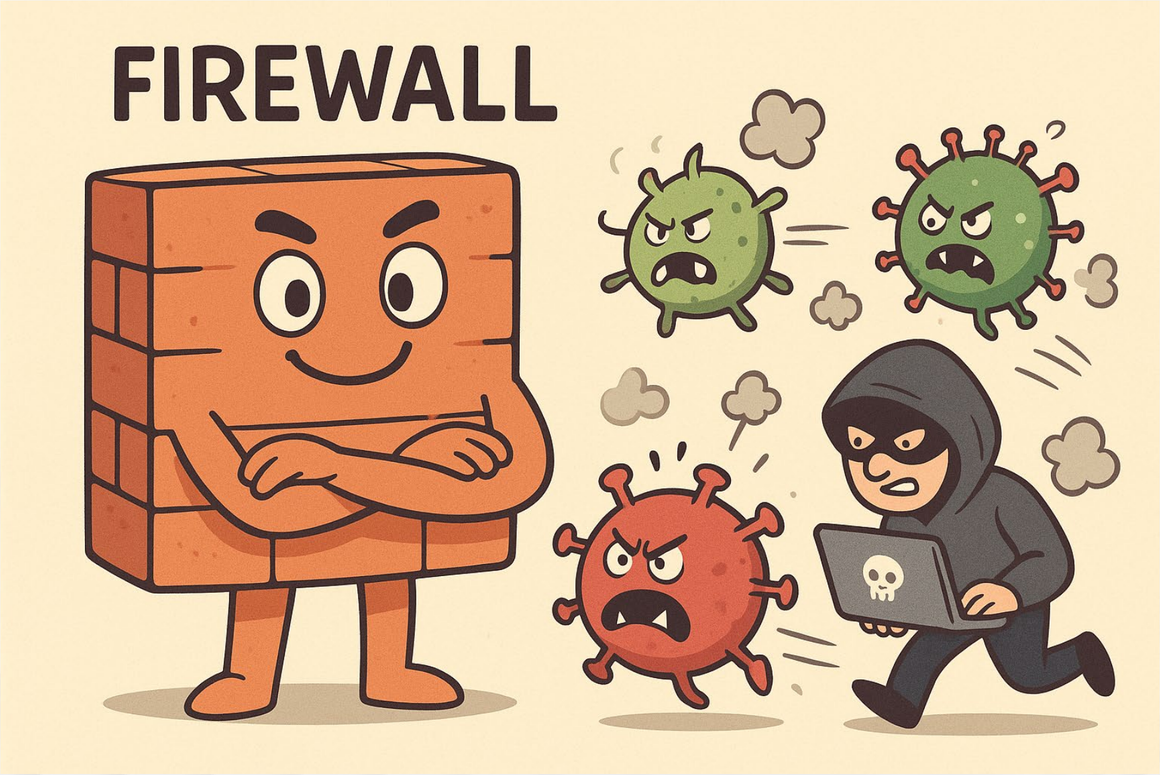


ОСОБЕННОСТИ ЗАЩИТЫ МУЛЬТИОБЛАЧНЫХ СРЕД

- Централизованный контроль и единая политика безопасности для всех провайдеров
- Интеграция средств защиты (NGFW, SDN, SD-WAN) и мониторинги между облаками
- Защита виртуализации: контроль над жизненным циклом виртуальных машин, обнаружение аномалий
- Применение концепций Zero Trust Network Access и анти-DDoS решений
- Внедрение автоматизированных систем управления идентификацией пользователей и контролем доступа

А КАК НА СЧЕТ ЗАЩИТЫ ПЕРИМЕТРА?

КАК ВЫБРАТЬ ПЕРИМЕТРОВЫЙ NGFW?



Чек-лист пилота NGFW

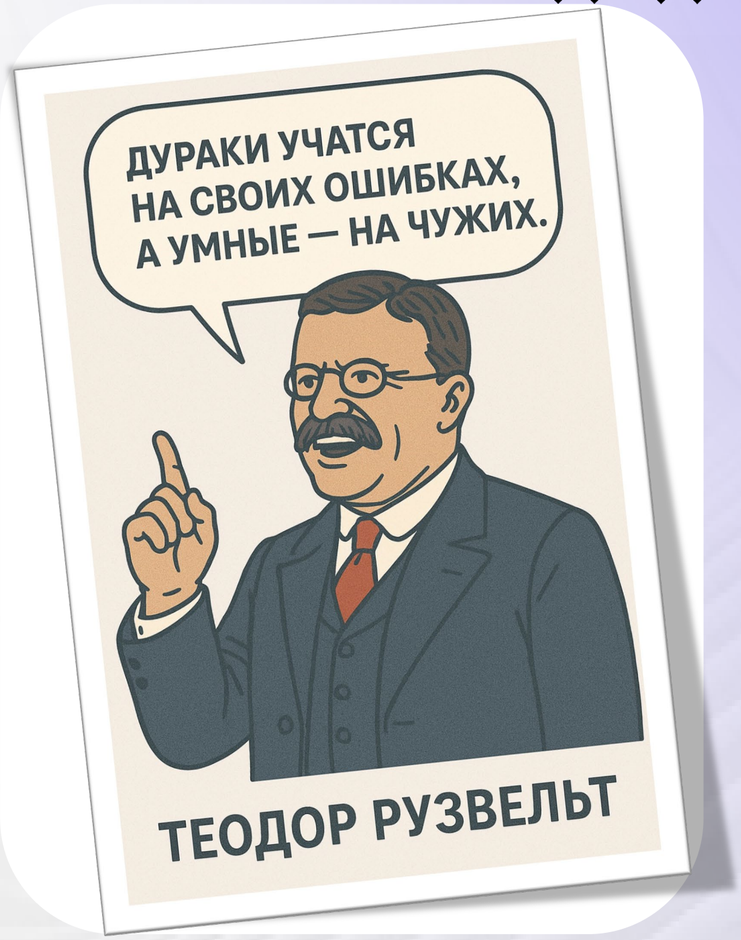
- [ ] Обнаружение старых типов атак
- [ ] Работа кластера — переключение между Active/Standby без потери сеансов и пауз
- [ ] Возможность Работы в облаке на виртуализации от Huawei
- [ ] Синхронизация NGFW (IPS) и EDR
- [ ] Работа фильтрации трафика по группам AD
- [ ] Наличие онлайн обновления сигнатур AV
- [ ] Наличие онлайн обновления сигнатур IPS
- [ ] Наличие поддержки ICAP
- [ ] Наличие блокировки файлов по расширениям
- [ ] Имеется ли падение в производительности свыше 40%?
- [ ] Обнаруживаются ли сетевые сканирования?
- [ ] Имеется ли поддержка IPv6 фильтрация и проверка трафика в IPv6-сетях (6to4, Teredo)
- [ ] Стабильна ли динамическая маршрутизация (BGP, OSPF), при изменении топологии?
- [ ] Работает ли изоляция трафика В VLAN?
- [ ] Работает ли ограничение сеансов по расписанию?
- [ ] Работает ли HTTPS инспекция?
- [ ] Обнаруживает ли потоковый AV сканер ВПО в виде архивов и скриптов?
- [ ] Обнаруживает ли IPS/IDS трендовые CVE?
- [ ] Корректность работы модуля «Контроль приложений»
- [ ] Проверка работоспособности модуля «Защита от DDoS-атак
- [ ] Нагрузочное тестирование — пропускная способность при 100% загрузке ЦП
- [ ] Есть ли снижение производительности при включении SSL-инспекции?
- [ ] Адекватное ли поведение при достижении максимального количества подключений?
- [ ] Адекватное ли время простоя при установке патчей?
- [ ] Имеется ли интеграция с SIEM?
- [ ] Есть ли журнал работы потокового AV?
- [ ] Ведется ли журнал DNS-запросов для анализа доменов для обнаружения C2-серверов
- [ ] Имеется ли интеграция с Ansible/Terraform через API?
- [ ] Работает ли блокировка трафика из запрещенных регионов (GeoIP)?
- [ ] Функция резервного копирования конфигураций
- [ ] Соответствие информации, описанной в формуляре и по факту?
- [ ] Наличие аппаратной фильтрации?

Тесты NGFW

*в 2023 году компания CloudScape пропустила тестирование IPv6-туннелей, что позволило злоумышленникам обойти блокировки через Teredo.

«Дураки учатся на своих ошибках, а умные — на чужих»

Теодор Рузвельт



ЧЕК-ЛИСТ ПО ЗАЩИТЕ ОБЛАЧНЫХ И МУЛЬТИОБЛАЧНЫХ СРЕД

Чек-лист

Контакты

Беляев Дмитрий Александрович

E-mail: for_belyaev_suggestions@mail.ru

Сайт: https://belyaev.expert/

Канал: @BELYAEV_SECURITY_bot

Отсканируй

↗ Канал «**BELYAEV_SECURITY**»: Твой проводник в мир защищенной информации (новости, статьи, экспертиза, юмор)

Вступи в канал