Защита внешнего периметра от КиберУгроз

ПроБизнес

МегаФон | ПроБизнес

Станислав Погоржельский

Руководитель технологической поддержки

Какие темы мы с вами обсудим?

- Инструментарии Защиты
- Что даёт нам применение этих инструментов
- Какие риски могут быть, если не применять защиту
- Примеры

ПроБизнес

Что такое внешний периметр безопасности?

- это область, которая ограничивает и защищает внешние границы организации или системы от несанкционированного доступа, вторжений и других угроз.

- Защищает от хакерских атак
- Защищает от киберпреступлений
- Защищает от физического вторжения
- Использует методологии защиты
- Исполняет требования регуляторов
- Обеспечивает конфиденциальность

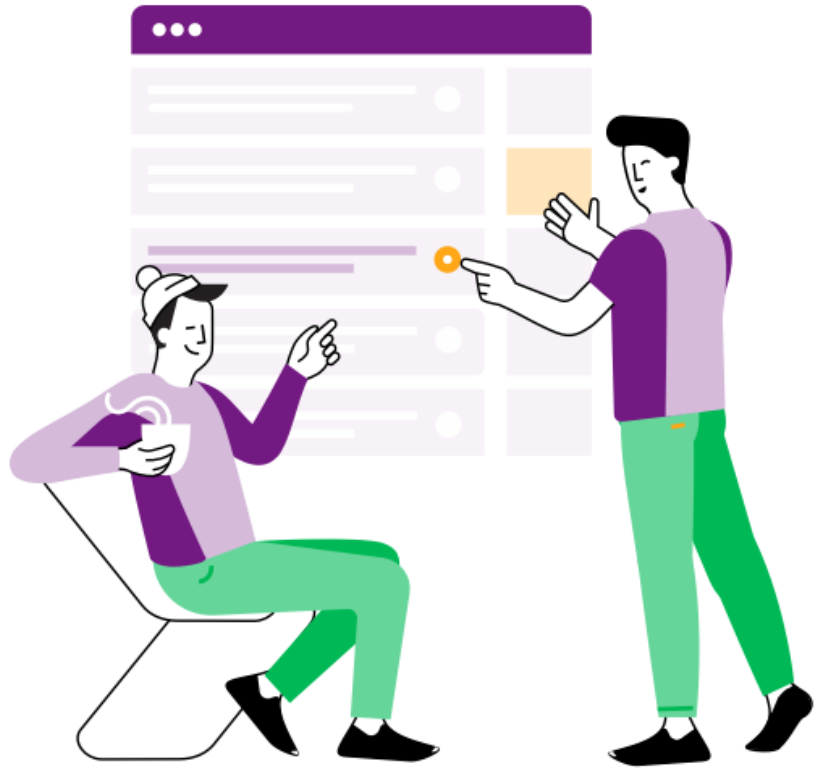
ПроБизнес

Какова цель КиберАтаки?

- Вывести из строя доступность WEB ресурса или IPv4 адреса Компании
- Вывести из строя оборудование
- Кража данных. Например, снятие копии дампа СУБД, где хранится информация об пользователях
- Испортить репутацию. Например, подмена текста на главной WEB странице сайта
- И прочее

ПроБизнес

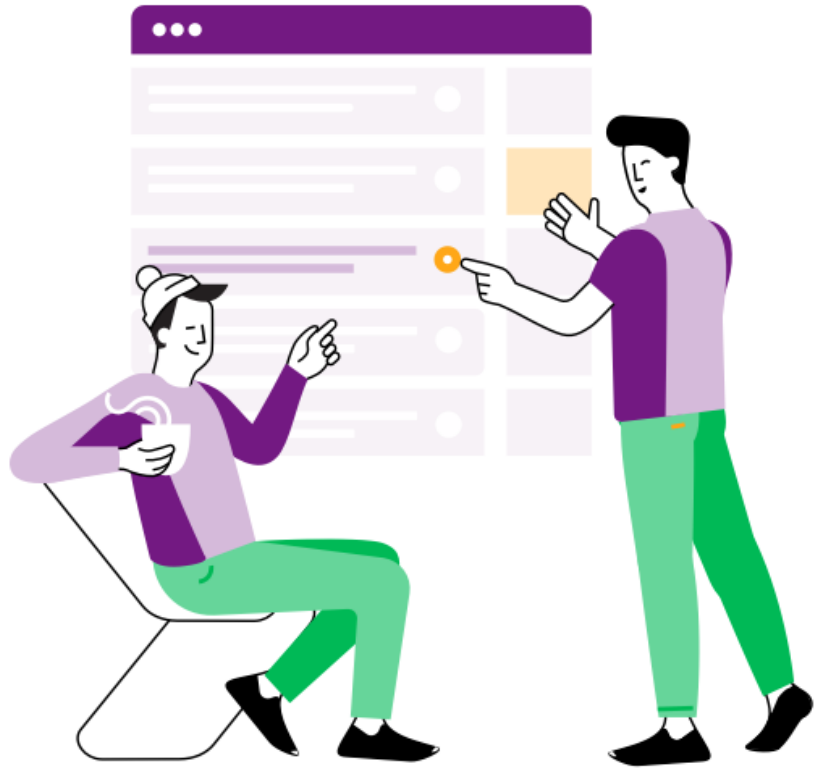
Инструменты безопасности внешнего периметра



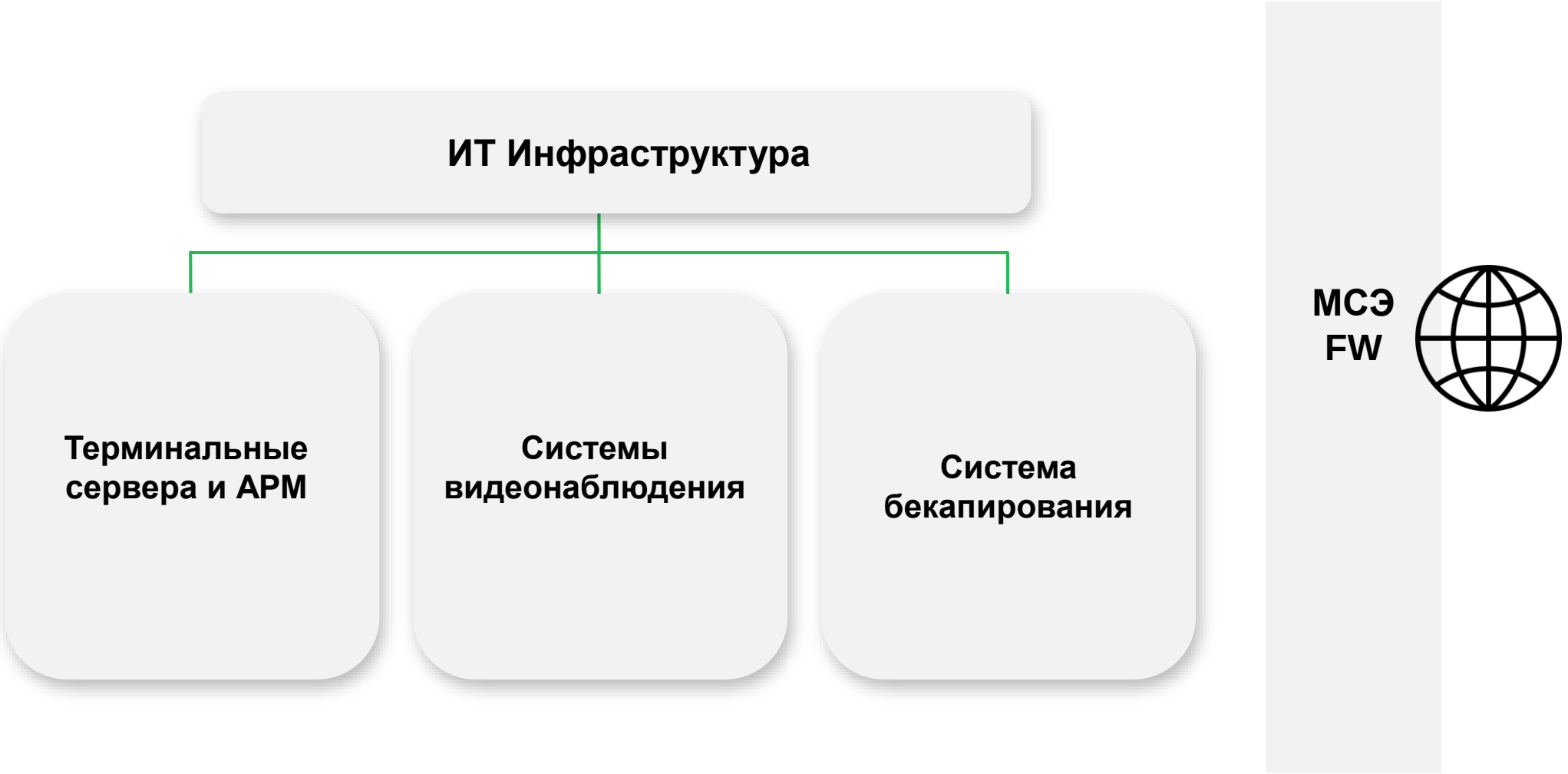
Инструменты

- Межсетевые экраны (firewalls)
- Системы предотвращения вторжений (Intrusion Prevention Systems, IPS)
- Системы обнаружения вторжений (Intrusion Detection Systems, IDS):
- Виртуальные частные сети (Virtual Private Networks, VPN)
- ДДоС-защита (Distributed Denial of Service protection)
- Системы авторизации и аутентификации
- Системы мониторинга безопасности

Как приблизиться к идеальной защите



Минимальный состав ИТ предприятия



ПроБизнес

Защита внешнего периметра МСЭ

ИТ Инфраструктура

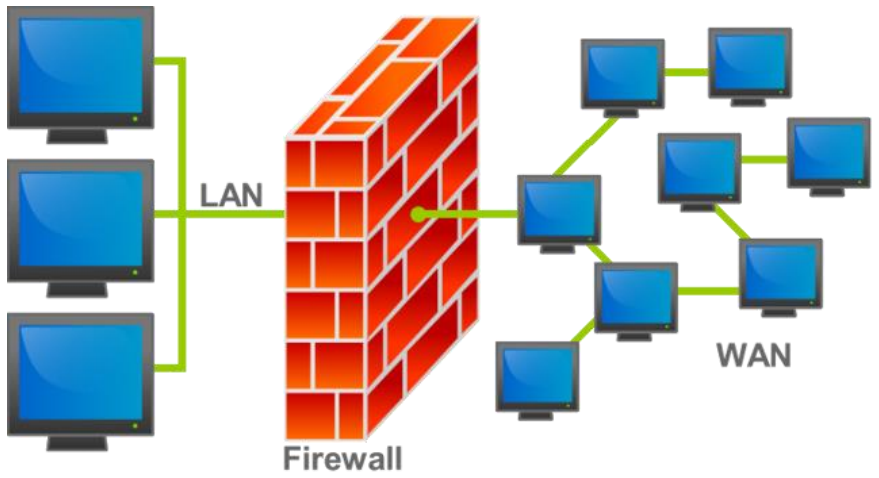
Внешний периметр

Межсетевой экран
Firewall

МСЭ - осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами

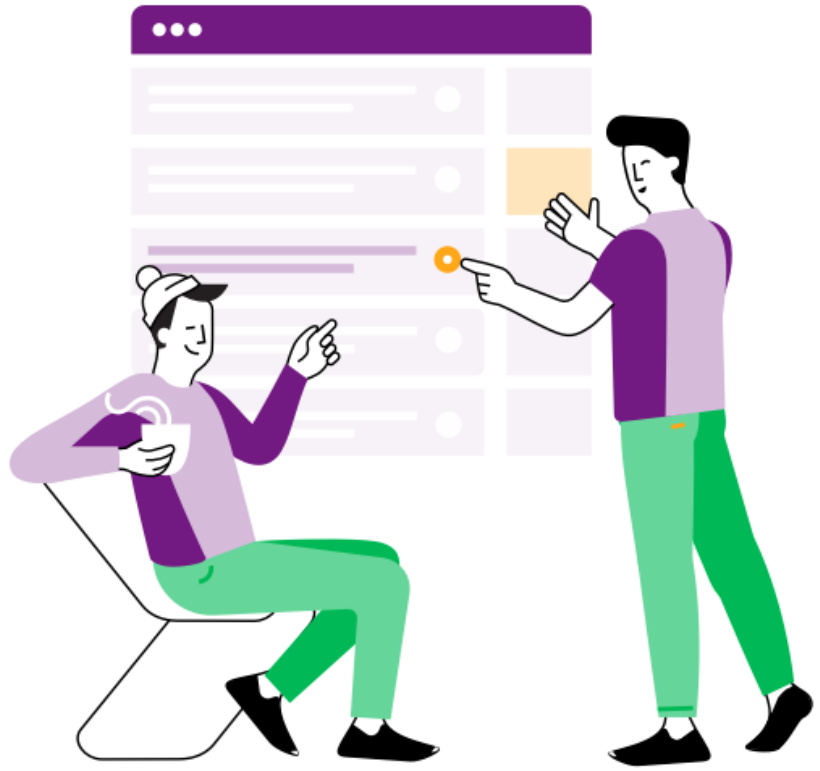
Основные функции:

- Фильтрация трафика
- Мониторинг сетевой активности
- Управление доступом
- VPN-шифрование
- Управление портами
- Управление доступа к сайтам

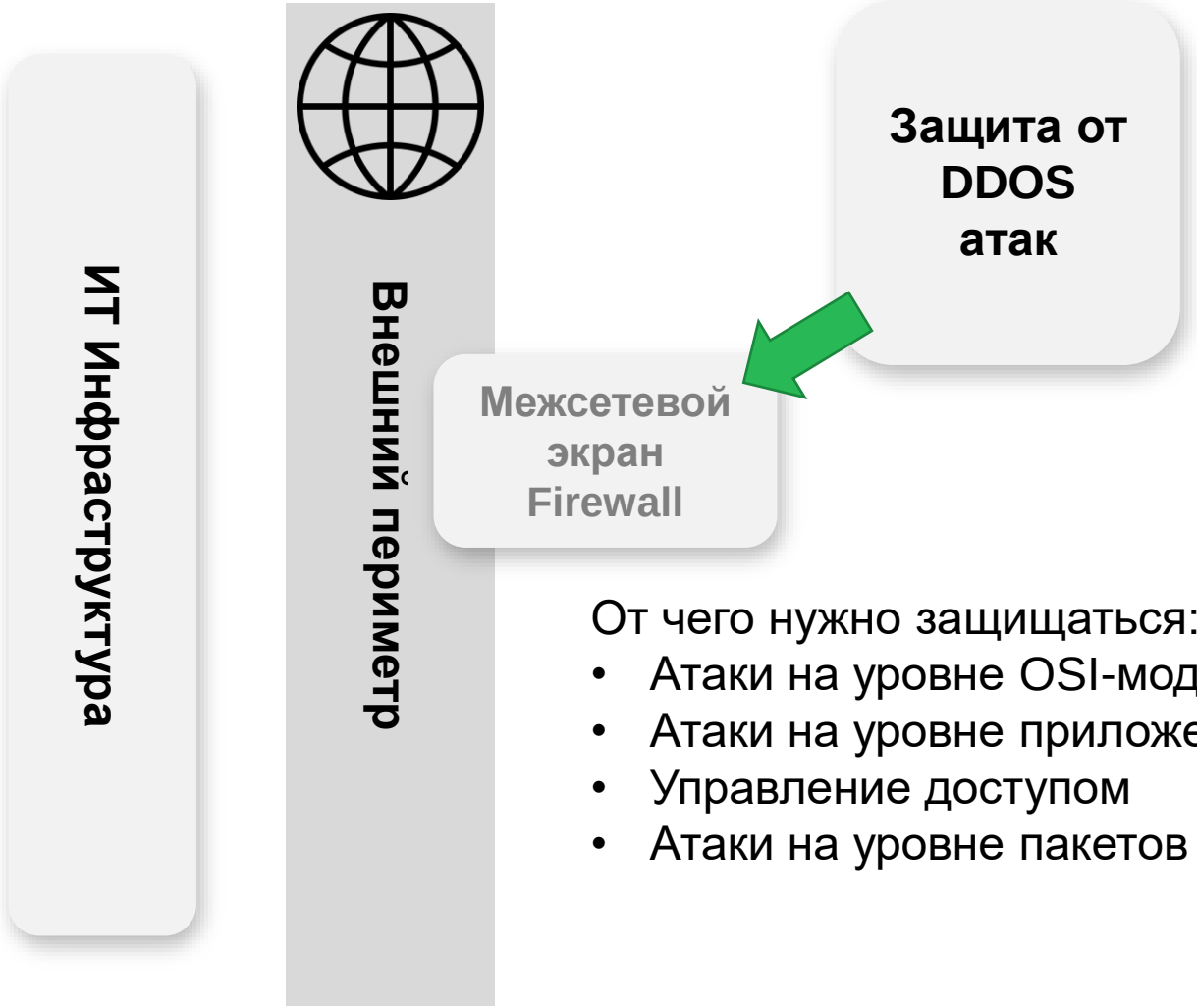


ПроБизнес

А что если придёт DDOS трафик?



Защита от DDOS (Distributed Denial of Service)



- Это тип кибератаки, при которой злоумышленник перегружает целевую систему или сеть путем отправки потоков данных с множества источников одновременно. Целью атаки является приведение к отказу в обслуживании, что приводит к недоступности ресурса для обычных пользователей.

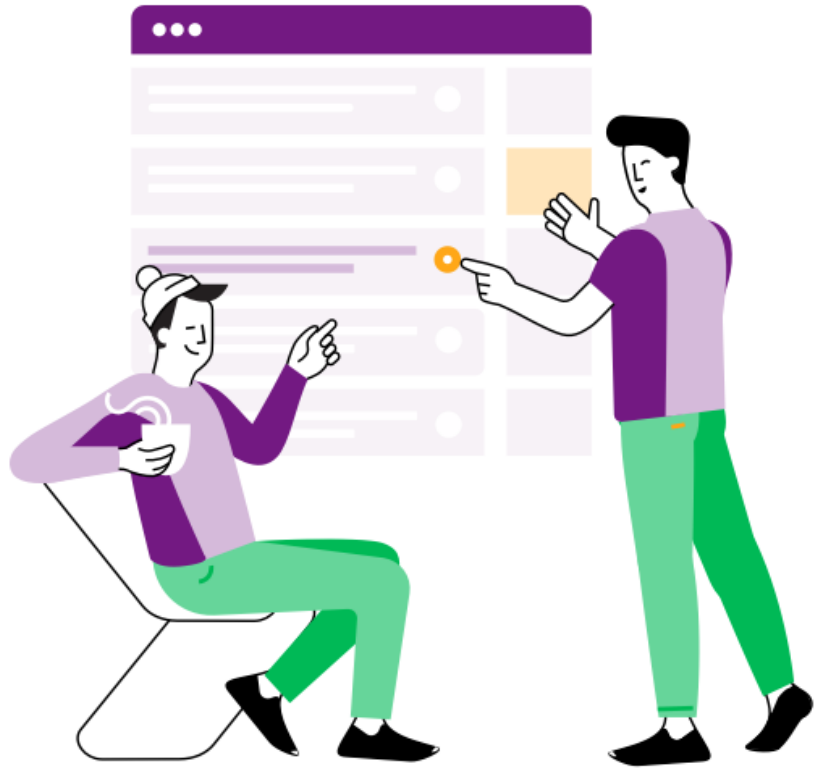
От чего нужно защищаться:

- Атаки на уровне OSI-модели
- Атаки на уровне приложений и протоколов
- Управление доступом
- Атаки на уровне пакетов

- HTTP flood атаки: направленные на перегрузку сервера запросами HTTP.
- DNS атаки.
- SNMP атаки: использование отраженного трафика SNMP (Simple Network Management Protocol).
- Slowloris атаки: направленные на исчерпание ресурсов сервера путем отправки медленных и неполных HTTP-запросов.
- И т.д

ПроБизнес

А что атака будет на уязвимость приложения? Например, на интернет магазин популярного CMS



Защита с помощью WAF

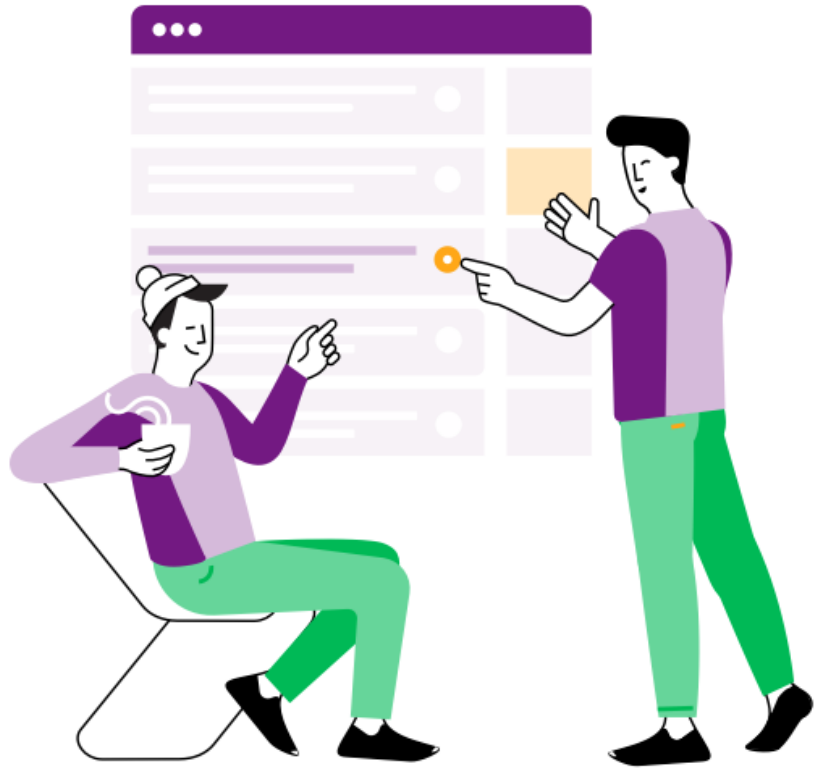
- Это овокупность мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение

От чего нужно защищаться:

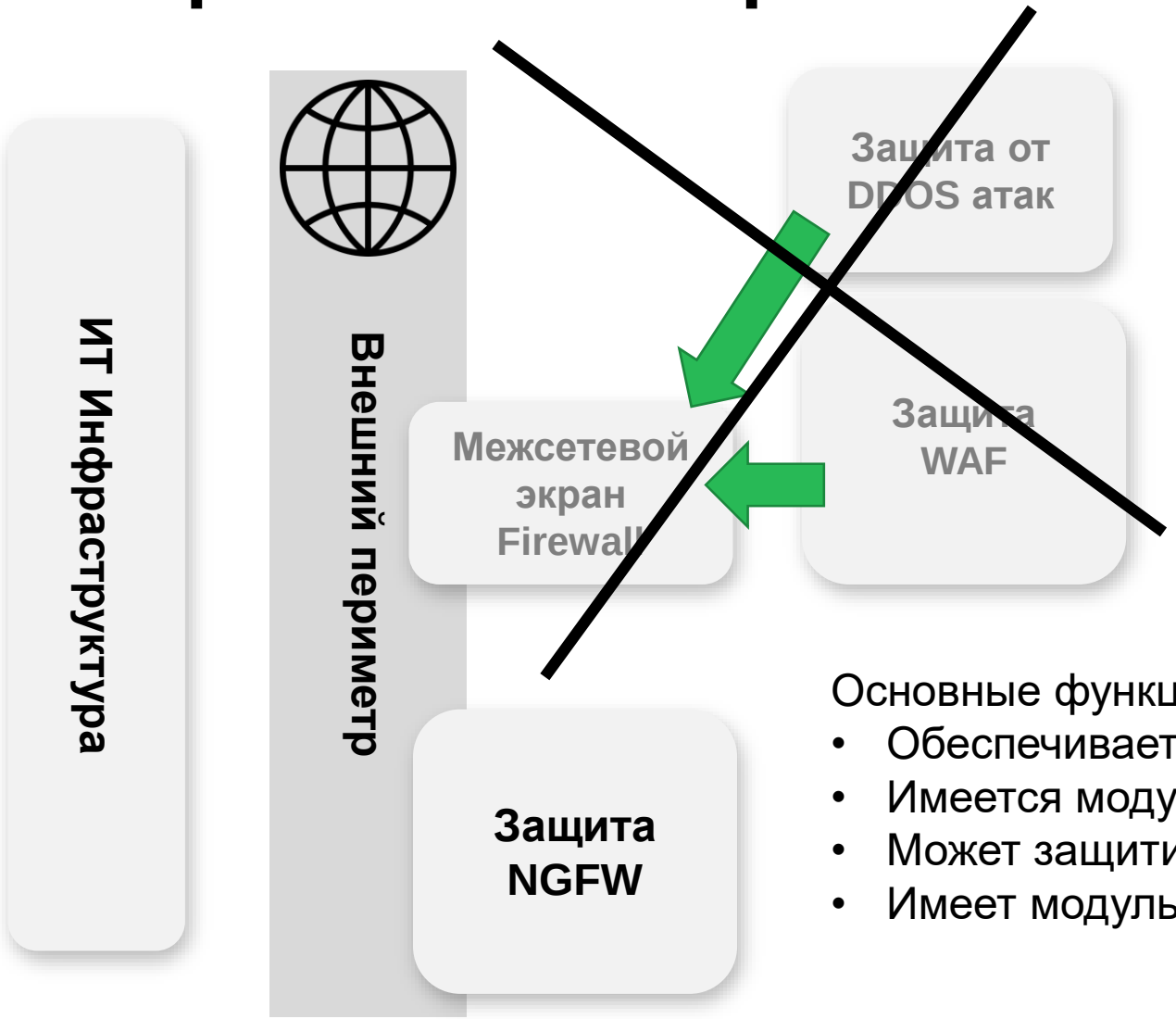
- SQL-инъекции
- XSS-атаки (межсайтовый скриптинг)
- CSRF (межсайтовая подмена запроса)
- Атаки на уязвимости веб-приложений
- Атаки на слабые пароли и попытки перебора пароля
- Атаки на управление сессией
- Атаки ZERO DAY и OWASP TOP 10
- И т.д.

ПроБизнес

А можно ли сделать защиту дешевле? Например, Альтернативными инструментами.



Защита с помощью NGFW (Next Generation Firewal)



- Это межсетевой экран для глубокой фильтрации трафика, интегрированный с IDS (Intrusion Detection System, система обнаружения вторжений) или IPS (Intrusion Prevention System, система предотвращения вторжений) и обладающий возможностью контролировать и блокировать трафик на уровне приложений

Основные функции NGFW:

- Обеспечивает функционал МСЭ
- Имеется модуль защиты от DDOS
- Может защитить Приложения по сигнатурам
- Имеет модуль IPS IDS

ПроБизнес

Выводы

Выводы

ПроБизнес

Технологии включают бизнес

Погоржельский Станислав
Руководитель технической поддержке по облачным и инфраструктурным решениям МегаФона

stanislav.pogorzhels@Megafon.ru

ПроБизнес

8 800 550 05 55
b2b.megafon.ru

МегаФон | ПроБизнес