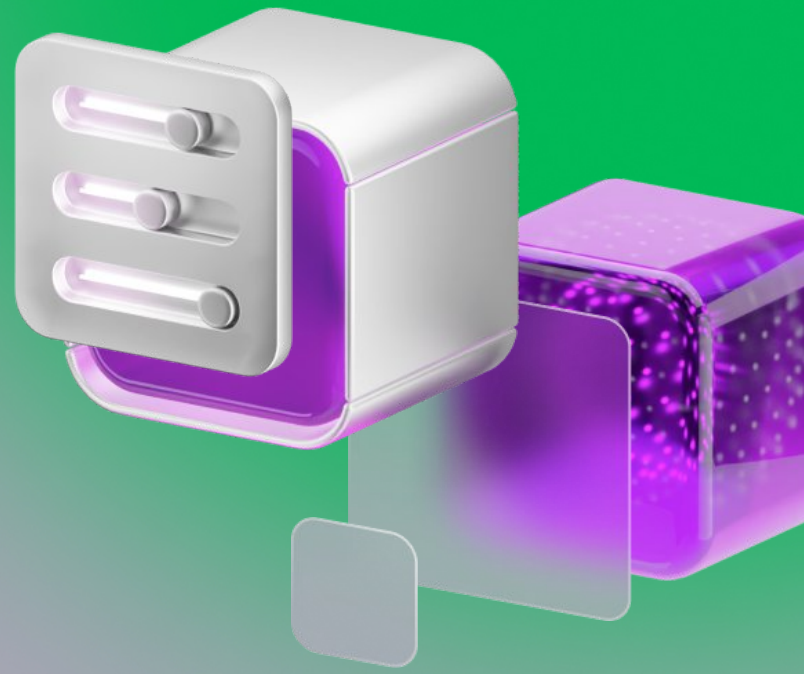
МегаФон | ПроБизнес

Безопасность ИТ-инфраструктуры



Внимание к информационной безопасности

со стороны государства многократно возрастает

МегаФон | ПроБизнес

Кейс

Решения кибербезопасности от МегаФона
как инструменты для защиты активов компании

Цель проекта:

- Выявить уязвимости в ИТ-инфраструктуре
- Предложить инструментарий для решения проблем
- Представить комплексное решение задач бизнеса
- Провести обучение для сотрудников компании по работе с персональными данными

МегаФон | ПроБизнес

Консалтинг

Анализ инфраструктуры по явным и возможным уязвимостям с последующим формированием отчета

- Проверили наличие используемого ПО в периметре организации
- Изучили версии ПО и наличие требуемого обновления, чтобы учесть актуальные сигнатуры
- Изучили сетевую топологию
- Составили основную модель угроз и перечень возможных «нарушителей»
- Проверили выполнение регламентирующих правил на наличие средств применения и оформления документации

МегаФон | ПроБизнес

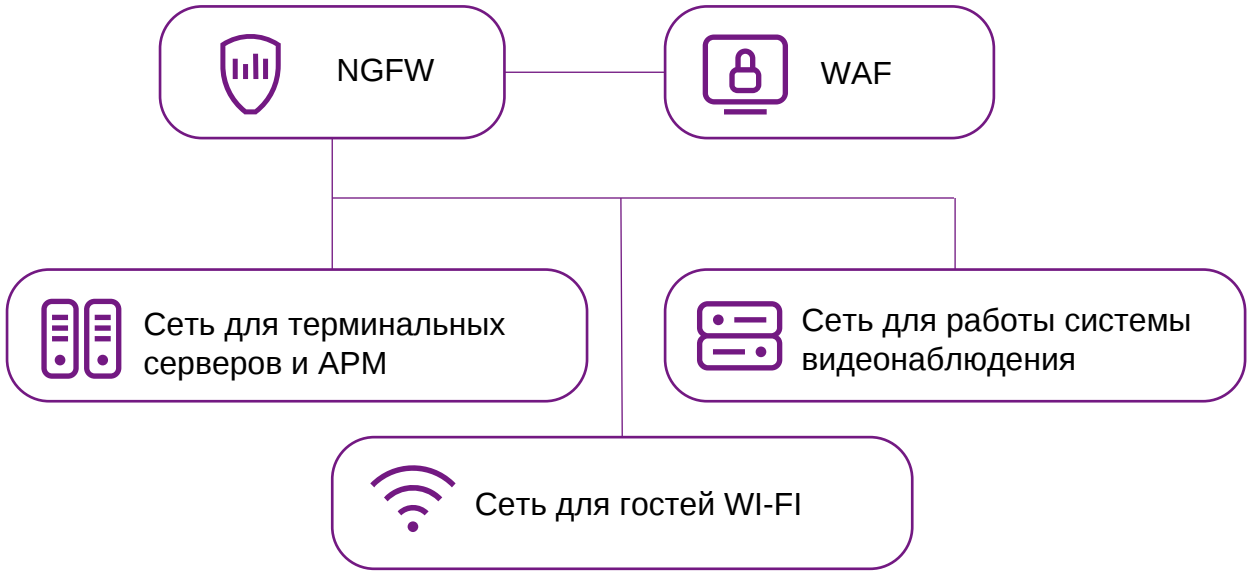
Выводы

- Заказчик использует ПО, которое давно не обновлялось
- Не было защиты извне (публичный интернет-канал)
- Не выполнялись требования нормативной функции, или ПО было снято с поддержки от вендора
- Отсутствует разделение сетей, т.е. не было DMZ для гостевого WI-FI

МегаФон | ПроБизнес

Решение и реализация

Разделили сети заказчика на группы и установили новое ПО



Выводы

Заменили текущий МСЭ на UserGate, т.к. вендор оборудования не может оказывать услуги

Разделили сети, чтобы минимизировать ущерб от злоумышленника при его попадании в корпоративную сеть

Предоставили WAF для сайта

Новое ПО МСЭ предоставили в аренду, чтобы можно было оперативно наращивать ресурсы и модули ИБ

Решили вопрос с регуляторами, т.к. UserGate находится в реестре российского ПО и имеет сертификат ФСТЭК России

МегаФон | ПроБизнес

Работа с пользователями

- Сотрудники не знают основ цифровой гигиены, халатное отношение к информационной безопасности
- У руководителей отсутствует возможность контролировать уровень знаний своих сотрудников
- Нельзя проверить действия сотрудников в ситуациях, приближенных к реальной атаке
- У руководителей нет подробной аналитики по уровню подготовки сотрудников и степени их уязвимости к действиям злоумышленника

Провели тестовую фишинговую рассылку

Security Awareness от МегаФона: платформа для повышения осведомленности сотрудников

Платформа в легкой и понятной форме повышает осведомленность сотрудников в сфере информационной безопасности и цифровой гигиены.

С помощью имитации фишинговых рассылок компания может проверить степень уязвимости сотрудников к действиям злоумышленника.

Теория	Практика
Обучающие курсы	Тестовые задания
Имитация фишинга	Вирусные вложения
Подробная аналитика	Выявление уязвимых сотрудников

МегаФон | ПроБизнес

Выводы

1

Внедрили логирование на все сетевые события ИТ и ИБ

2

Применяемые ранее средства ИБ не работают в настоящее время

3

Обновление и поддержка от вендора – важная составляющая в любой ИТ-инфраструктуре

4

Социальный хакинг важный фактор ИБ, который нужно учесть, а также проводить тестовые учебные фишинговые рассылки

МегаФон | ПроБизнес

МегаФон | ПроБизнес

Защита внешнего периметра организации от киберугроз

Что такое внешний периметр безопасности?

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

МегаФон | ПроБизнес

Инструменты безопасности внешнего периметра

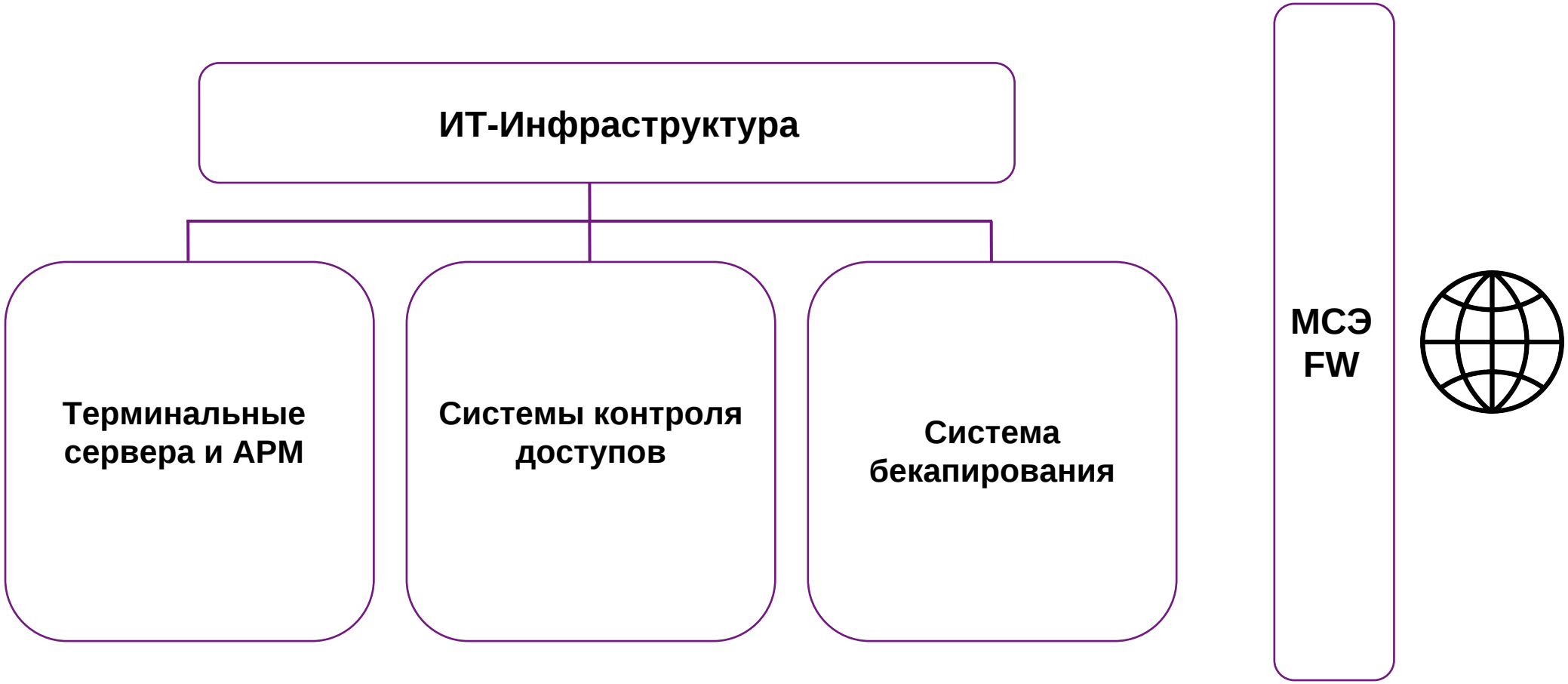
Инструменты

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

МегаФон | ПроБизнес

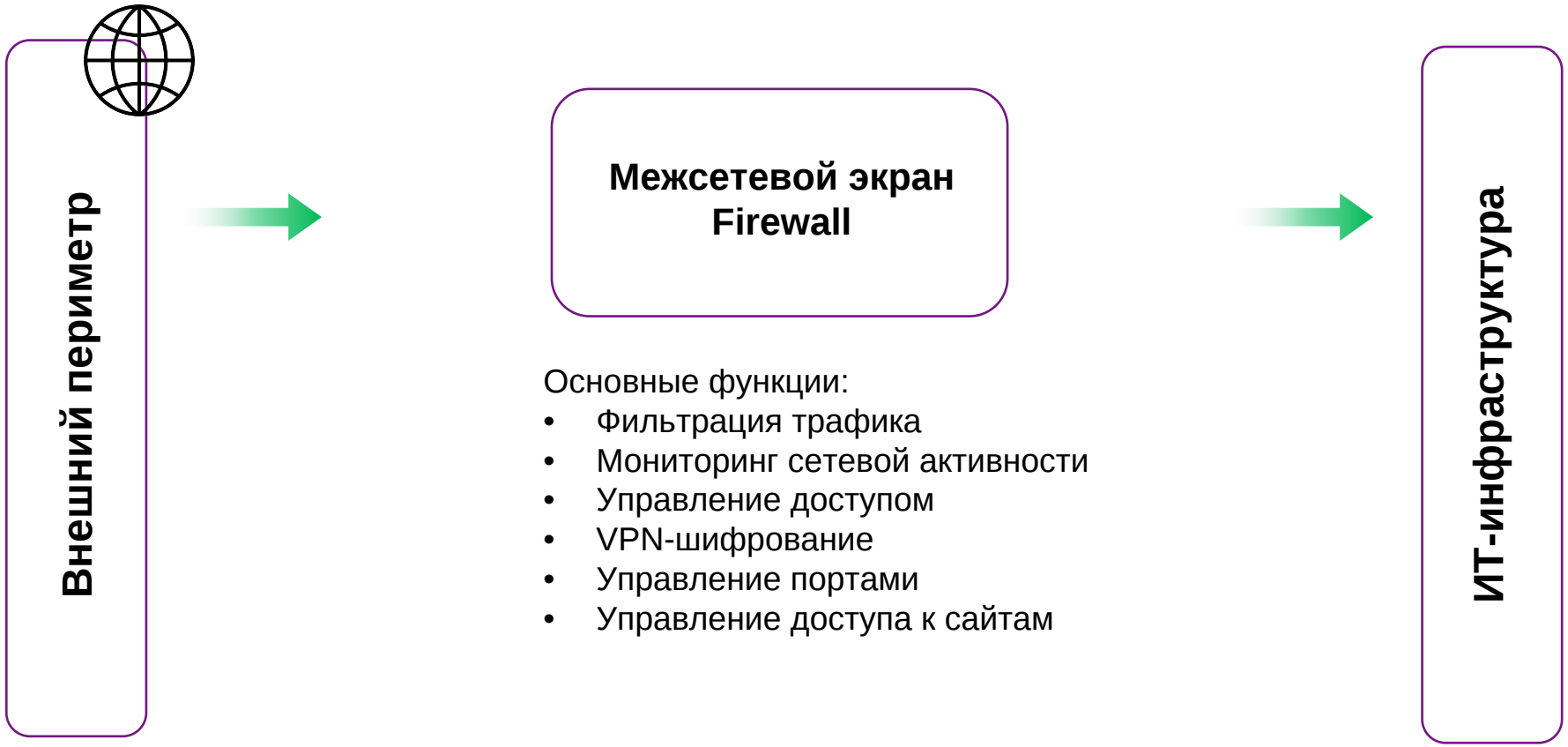
Как приблизиться к идеальной защите?

Минимальный состав ИТ-инфраструктуры предприятия



Защита внешнего периметра МСЭ

Межсетевой экран — контроль и фильтрация проходящего сетевого трафика
в соответствии с заданными правилами



Основные функции:

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

МегаФон | ПроБизнес

А можно ли сделать защиту дешевле? Например, альтернативными инструментами

Защита с помощью NGFW

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

Основные функции NGFW:

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

МегаФон | ПроБизнес

А что если придёт DDoS трафик?

Защита от DDoS-атак

DDoS-атака - тип кибератаки, при которой злоумышленник перегружает целевую систему или сеть путем отправки потоков данных с множества источников одновременно. Цель атаки - отказ в обслуживании, что приводит к недоступности ресурса для пользователей.

От чего нужно защищаться:

- Атаки на уровне OSI-модели
- Атаки на уровне приложений и протоколов
- Управление доступом
- HTTP flood атаки
- DNS-атаки
- SNMP-атаки
- Slowloris-атаки

МегаФон | ПроБизнес

А что, если атака будет на web-приложение? Например, на интернет-магазин популярного CMS

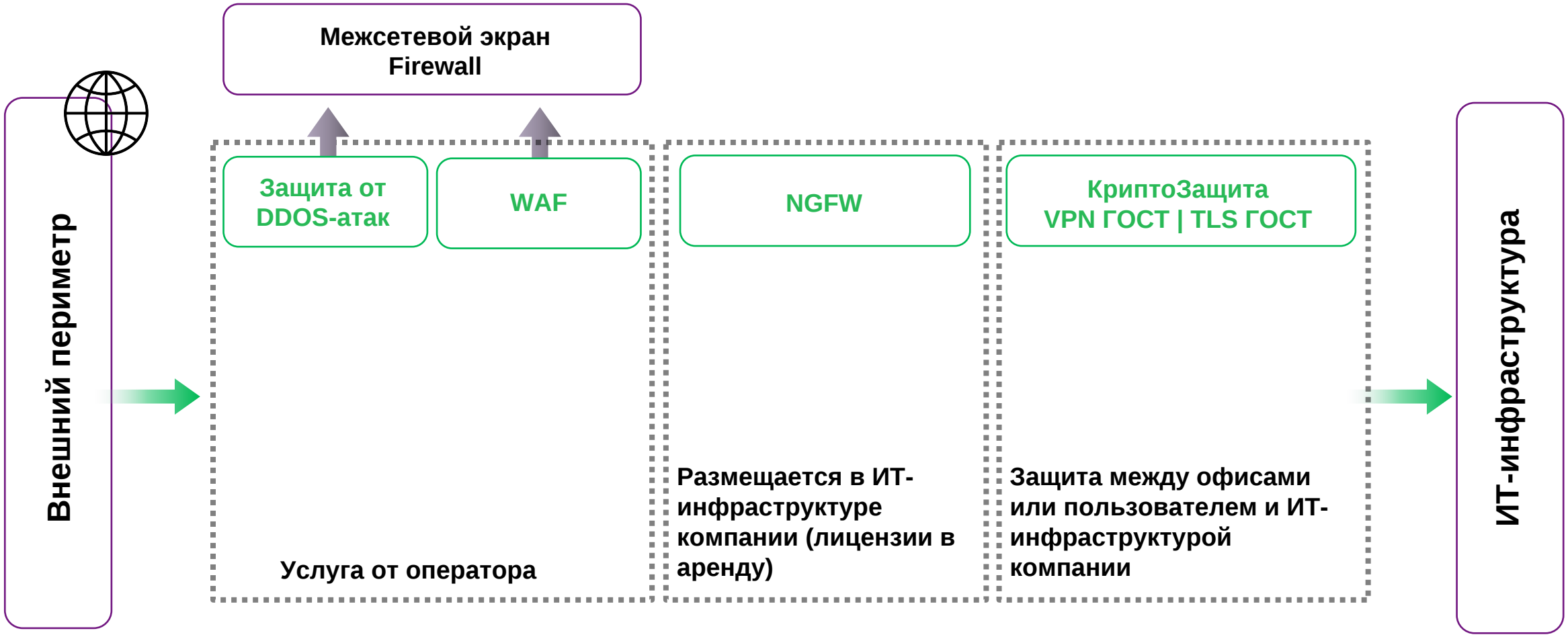
Защита с помощью WAF

WAF - совокупность мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на web-приложение

От чего нужно защищаться:

- Атаки на уязвимости веб-приложений
- Атаки на слабые пароли и попытки перебора пароля
- Атаки на управление сессией
- Атаки ZERO DAY и OWASP TOP10
- SQL-инъекции
- XSS-атаки
- CSRF

Выводы


Межсетевой экран
Firewall
Внешний периметр
Защита от
DDOS-атак
WAF
NGFW
КриптоЗащита
VPN ГОСТ | TLS ГОСТ
ИТ-инфраструктура
Услуга от оператора
Размещается в ИТ-инфраструктуре компании (лицензии в аренду)
Защита между офисами или пользователем и ИТ-инфраструктурой компании

МЕГАФОН | ПроБизнес

Технологии включают бизнес

Денис Нигматуллин
Менеджер по внедрению цифровых решений

ПроБизнес

Индекс кибербезопасности