

Как защитить ИТ-инфраструктуру в облаке с помощью NGFW



Станислав Погоржельский

Руководитель по технологической
поддержке облачных
и инфраструктурных решений



Какие темы мы с вами обсудим?

- ✓ **Определение NGFW (Next-Generation Firewall)**

и их роль в современных сетевых инфраструктурах

- ✓ **Зачем NGFW нужны в облачной среде провайдера**

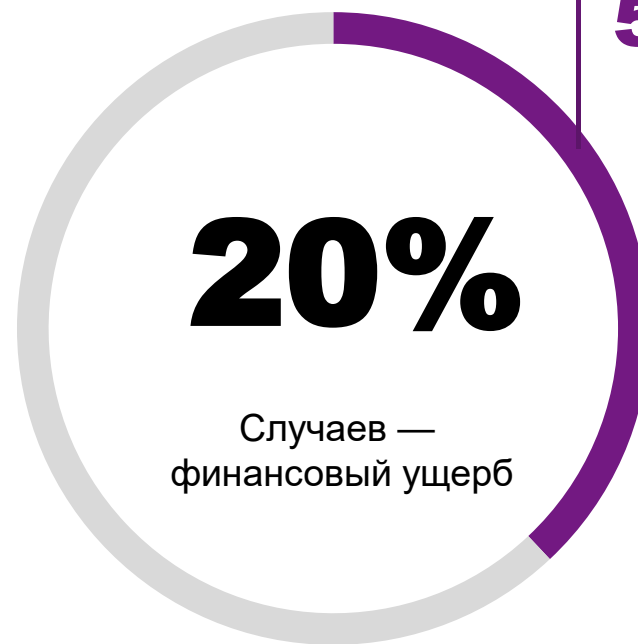
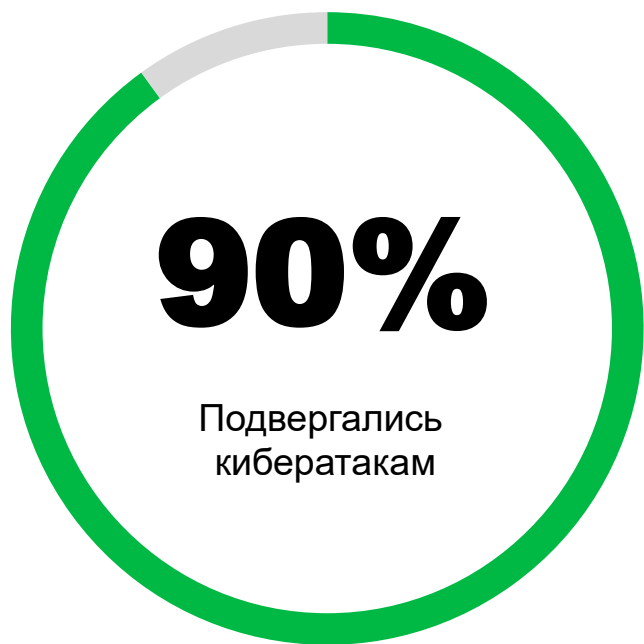
- ✓ **Преимущества использования NGFW в облаке провайдера**

- ✓ **Механизмы обеспечения отказоустойчивости NGFW**



Кибератаки 2021-2023

Статистика российского рынка



Из них каждая пятая компания оценила свой ущерб в более чем

5 млн ₽



Киберугрозы, с которыми столкнулись компании за год

Чаще всего угрозы выражены в заражениях вирусами. В более крупных компаниях с большим количеством инфраструктуры угрозы в целом возникают чаще, особенно часто встречаются атаки на веб-ресурсы (DDoS, взлом, заражение и т. д.).

Угрозы/атаки, с которыми столкнулись за год

Заражение вирусами (не шифровальщиками)



Атаки на веб-ресурсы организации (DDoS, взлом, заражение и т. п.)



17% Среди компаний сегмента SoHo
47% Среди компаний сегмента LA

Заражение вирусами-шифровальщиками



Фишинговые атаки



15% Среди компаний сегмента SoHo
45% Среди компаний сегмента LA

Кража/подмена/уничтожение данных



7% Среди компаний сегмента SoHo



Причины утечки данных

95%



- ✓ Данные
- ✓ Приложения
- ✓ Базы данных
- ✓ Операционная система

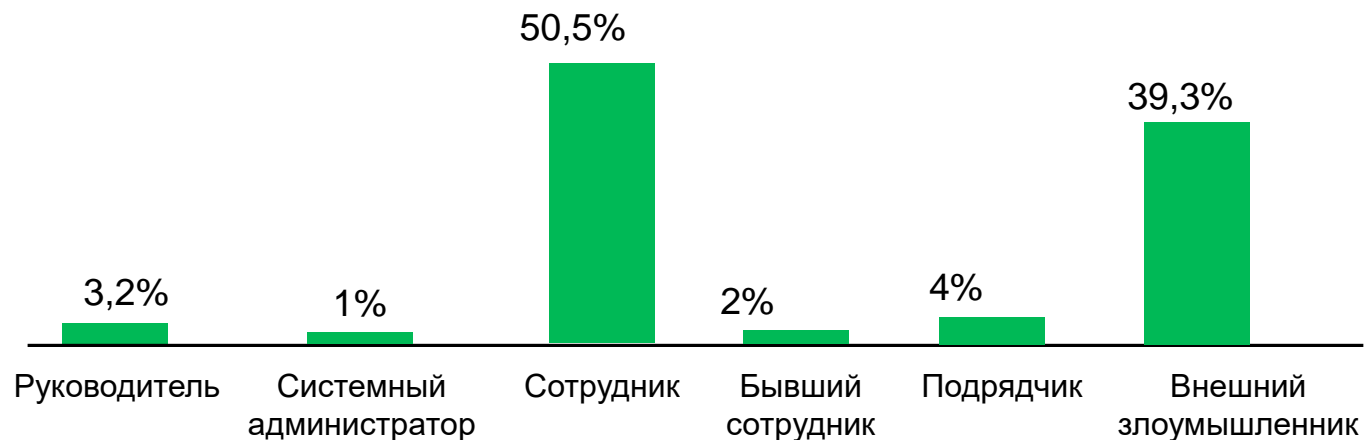
5%



- ✓ Виртуализация
- ✓ Физический сервер
- ✓ Сети, хранилища
- ✓ Дата-центр

Виновники утечек

- Внутренний злоумышленник
- Внешний злоумышленник



Причины утечки данных

ИТ-Инфраструктура



Терминальные сервера и APM



Системы видеонаблюдения



Система бекапирования



МСЭ
FW





Пробизнес

Защита внешнего периметра организации от киберугроз



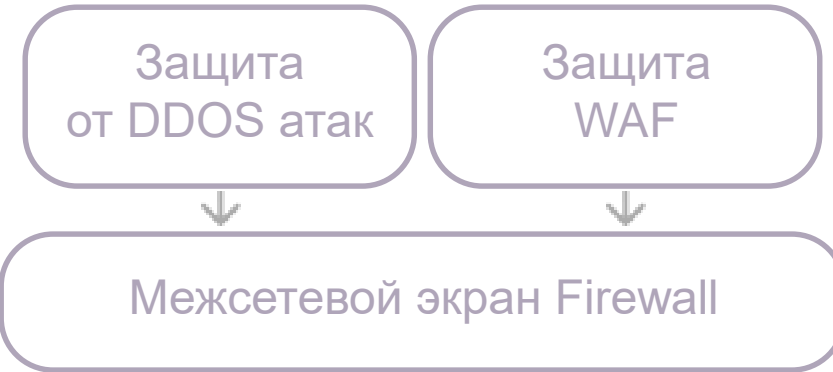
Защита в облаке с помощью NGFW

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



Защита NGFW



Внешний периметр

ИТ-Инфраструктура



Что такое внешний периметр безопасности?

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





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

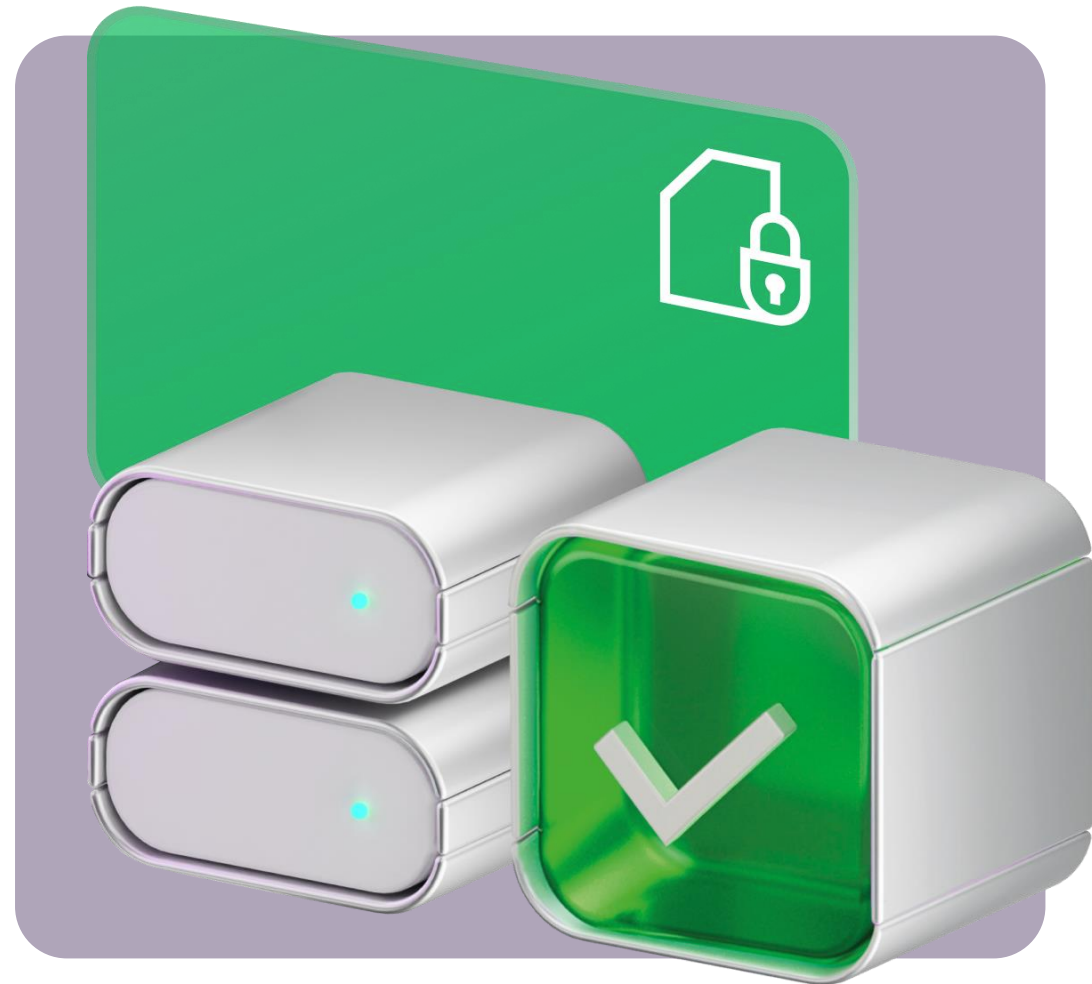
Virtual Private Networks, VPN

DDOS-защита

Distributed Denial of Service protection

Системы авторизации и аутентификации

Системы мониторинга безопасности



ЧТО ТАКОЕ NGFW

NGFW – многофункциональный продукт

Функции NGFW

- ✓ Межсетевое экранирование
- ✓ Обнаружение и предотвращение атак
в т.ч. атаки на веб-приложения
- ✓ Антиспам
- ✓ Поточковый антивирус
- ✓ Контроль приложений
- ✓ Фильтрация интернет-запросов пользователей
- ✓ VPN
- ✓ Анализ событий/формирование отчетов



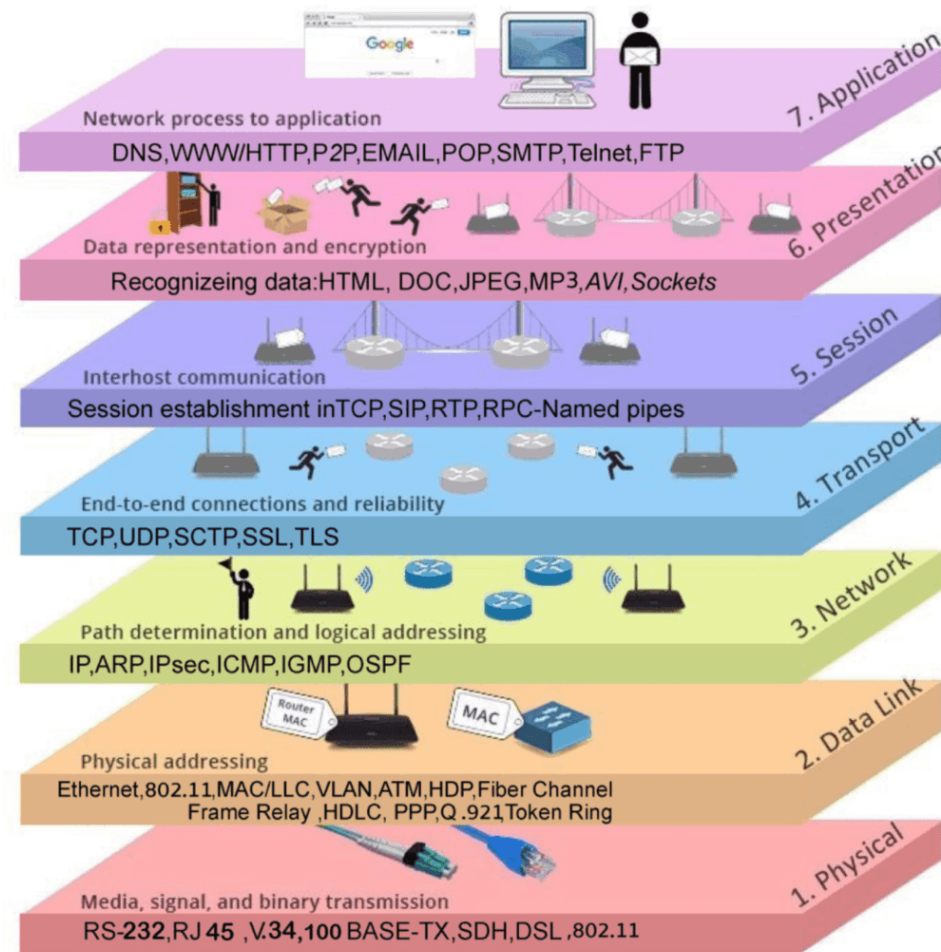


Модель OSI для облачного NGFW



Модель OSI для облачного NGFW

Уровень	Функции	PDU	Примеры
7. Прикладной	Некоторое высокоуровневое API	Данные	HTTP, FTP
6. Представительский	Представление данных между сетевым сервисом и приложением	Данные	ASCII, EBCDIC, JPEG
5. Сеансовый	Управление сеансами: продолжительный обмен информацией в виде множества передач между нодами	Данные	RPC, PAP
4. Транспортный	Надёжная передача сегментов между двумя нодами в сети	Сегменты/Д атаграммы	TCP, UDP
3. Сетевой	Структуризация и управление множеством нод в сети	Пакеты	IPv4, IPv6
2. Канальный	Надёжная передача датафреймов между двумя нодами соединённых физическим уровнем	Фреймы	PPP, IEEE 802.2, Ethernet
1. Физический	Передача и приём потока байтов через физическое устройство	Биты	USB, витая пара



Модель OSI для облачного NGFW

Уровень 3

Сетевой уровень

Network Layer

Фильтрация IP-трафика

Проводит анализ IP-пакетов, проверяя их заголовки на наличие источника, назначения и других параметров.

Маршрутизация

NGFW обладают функциями маршрутизации, которые позволяют оптимизировать потоки трафика и управлять их направлением с учетом правил безопасности и политик маршрутизации.

Уровень 4

Транспортный уровень

Transport Layer

Фильтрация трафика по портам

Анализирует TCP и UDP порты в заголовках пакетов для идентификации конкретных сервисов и приложений.

Обнаружение и предотвращение атак

Может использоваться для обнаружения и блокировки различных атак на транспортном уровне, таких как атаки DDoS, SYN flood и другие.

Уровень 5

Прикладной уровень

Application Layer

Идентификация приложений

Способен определять конкретные приложения и сервисы, используемые в сети, не только на основе портов, но и на основе глубокого пакетного анализа.

Глубокий пакетный анализ

NGFW проводит анализ содержимого пакетов данных на прикладном уровне, что позволяет выявлять вредоносный или запрещенный трафик, скрытый внутри протоколов прикладного уровня.

Контроль доступа

NGFW применяет политики доступа на основе идентификации приложений, пользователей и групп пользователей.

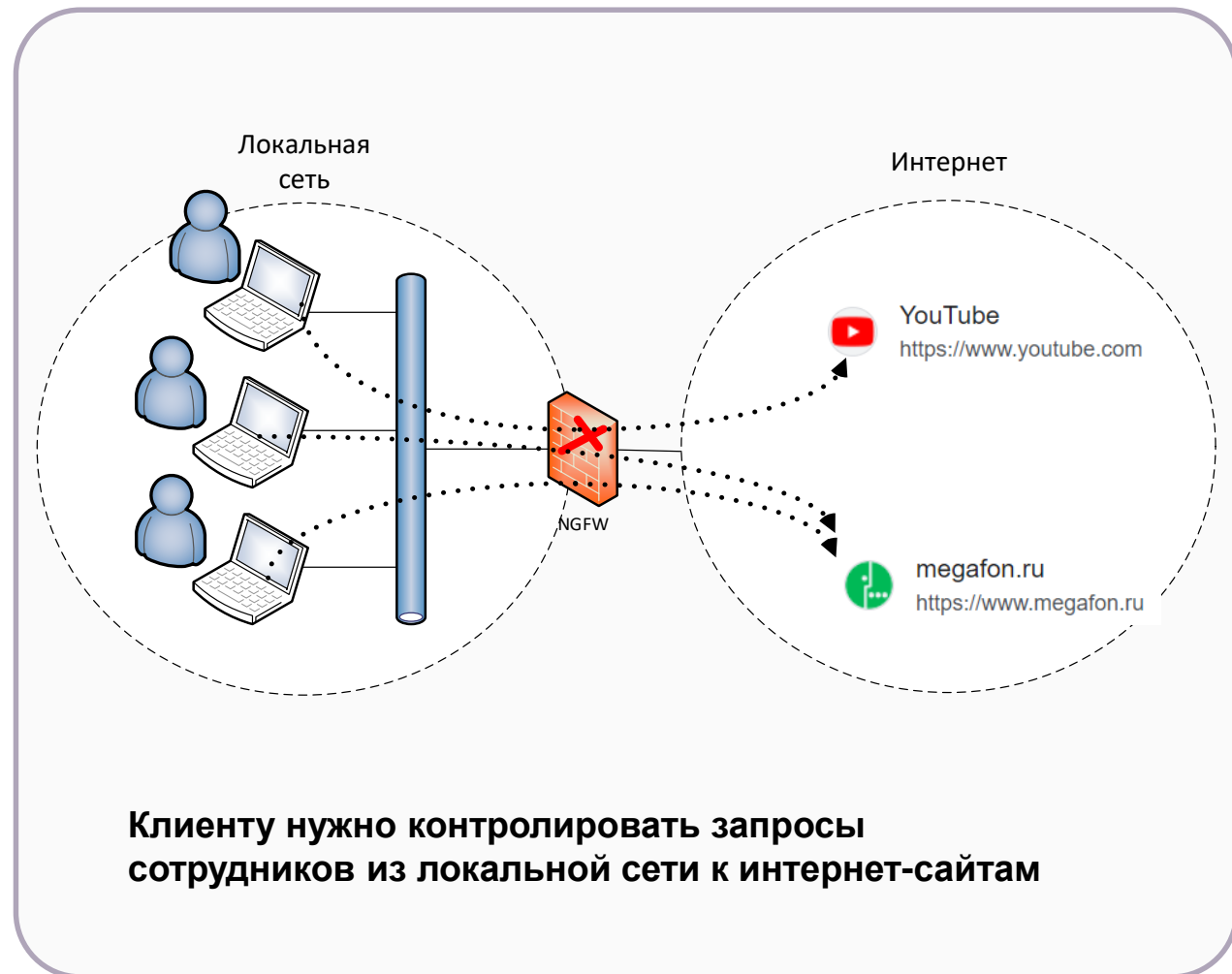
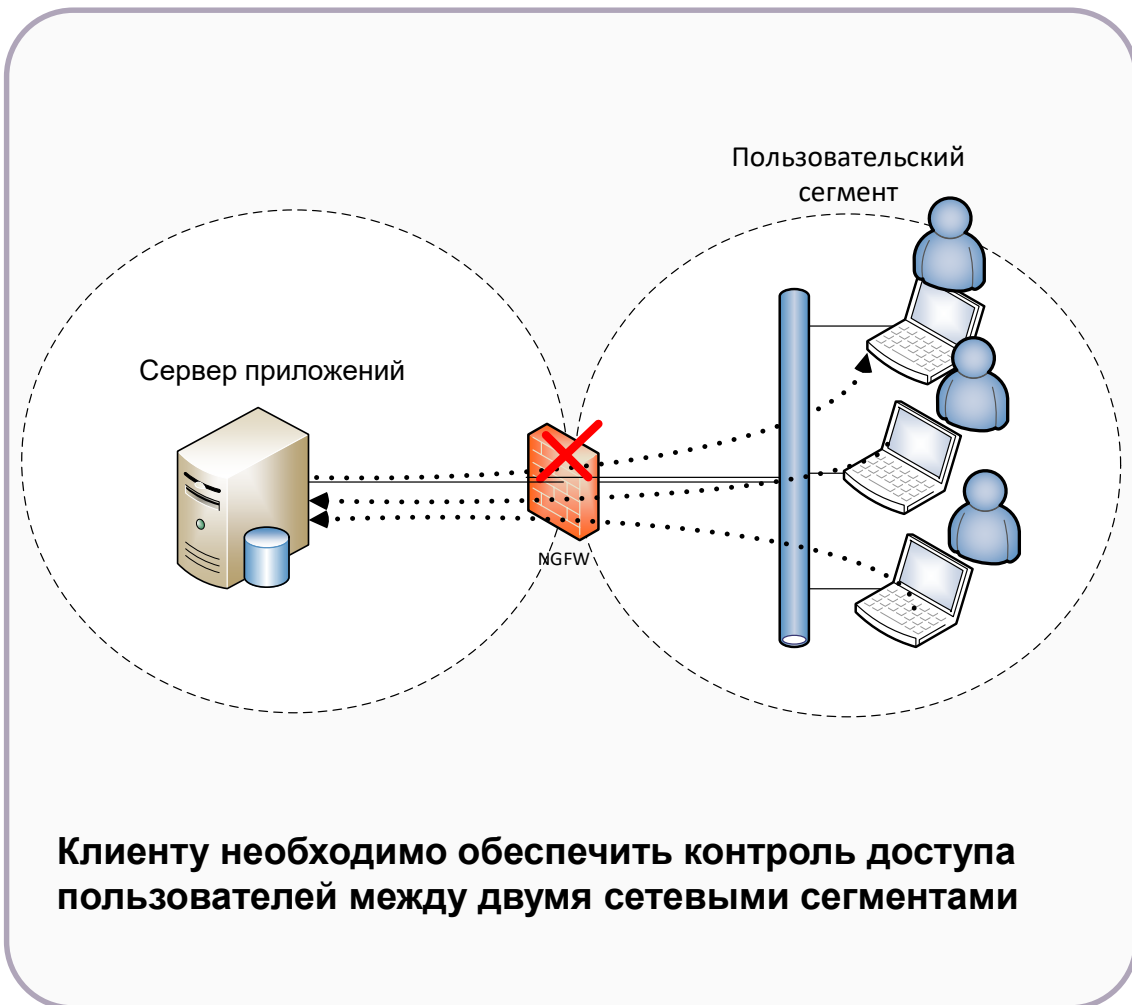




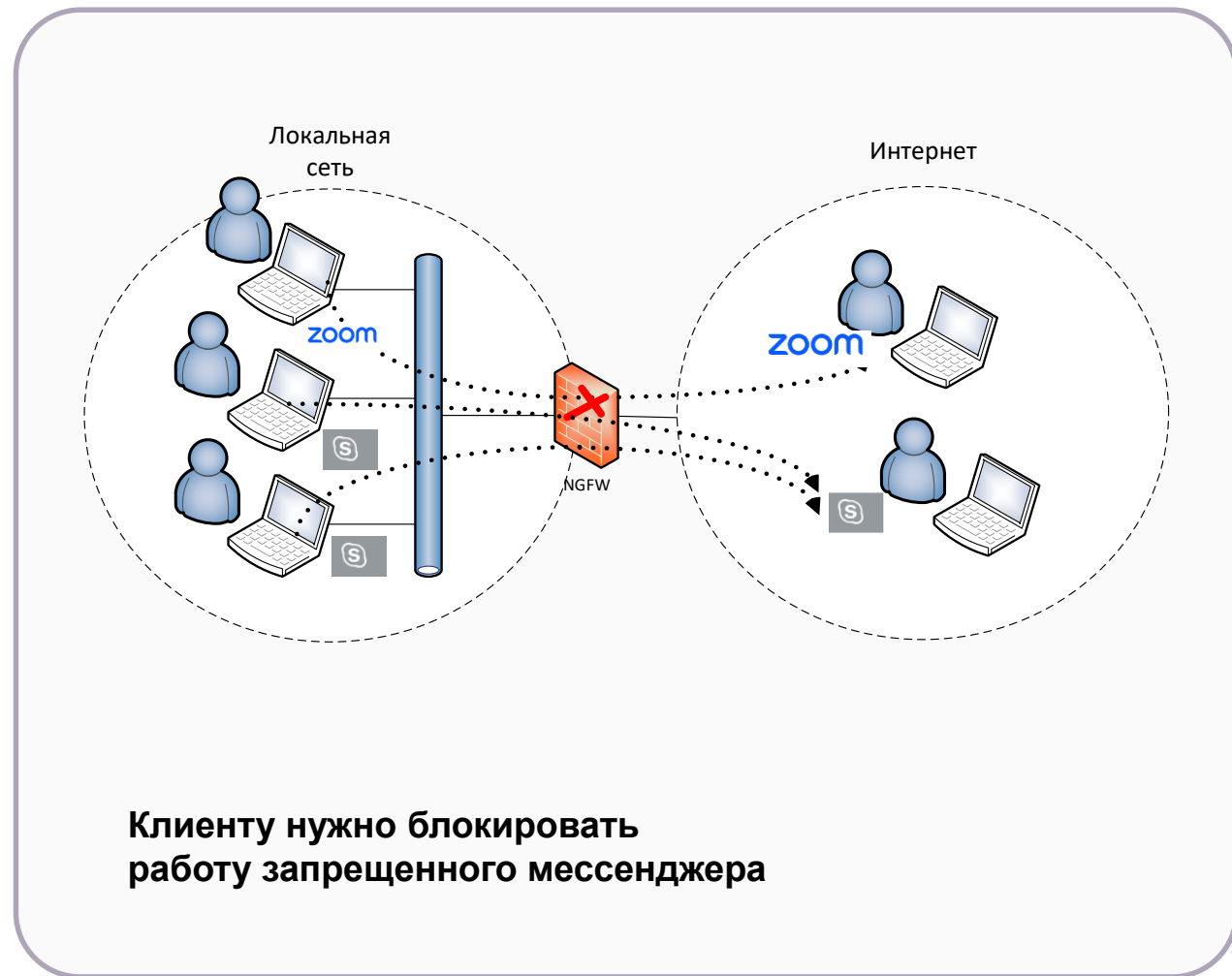
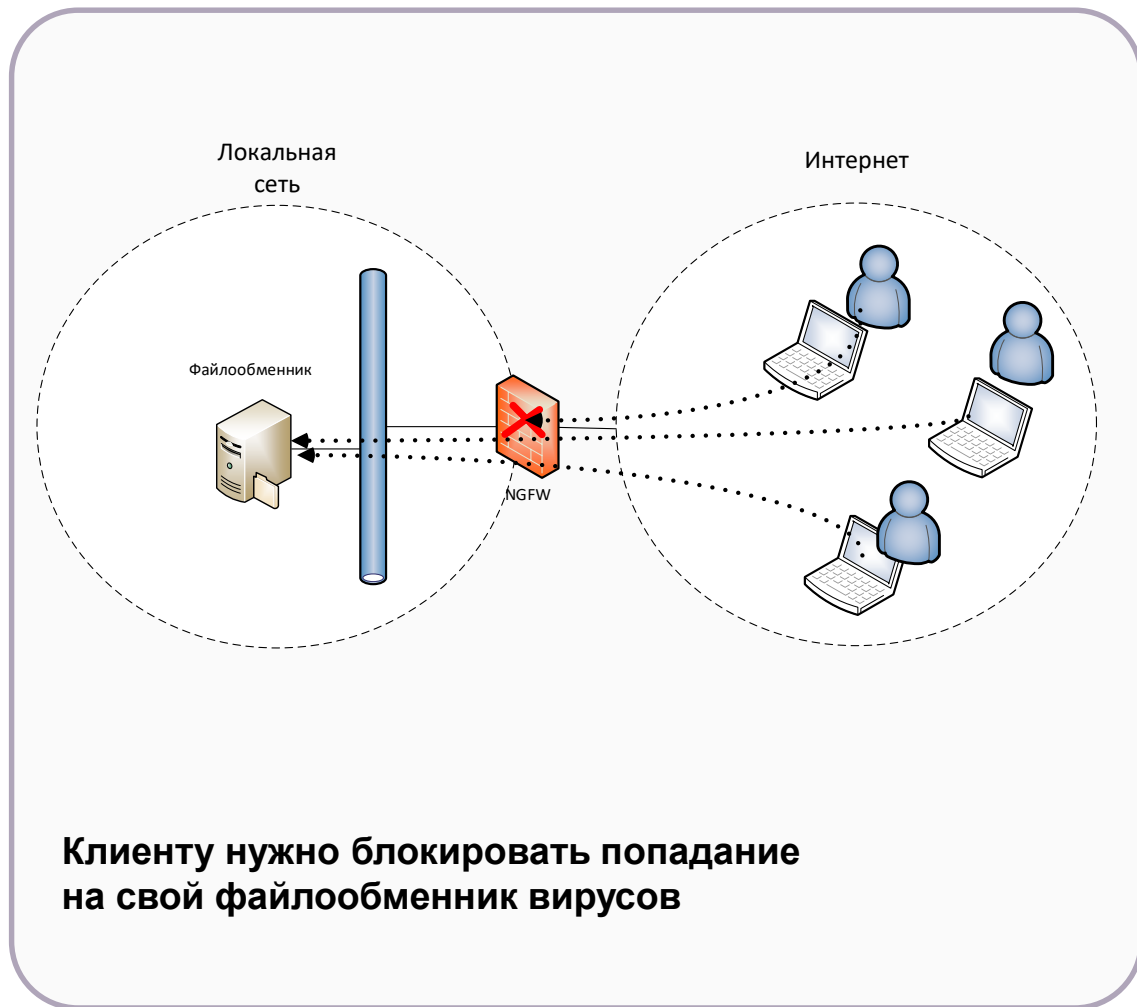
Сценарии использования NGFW



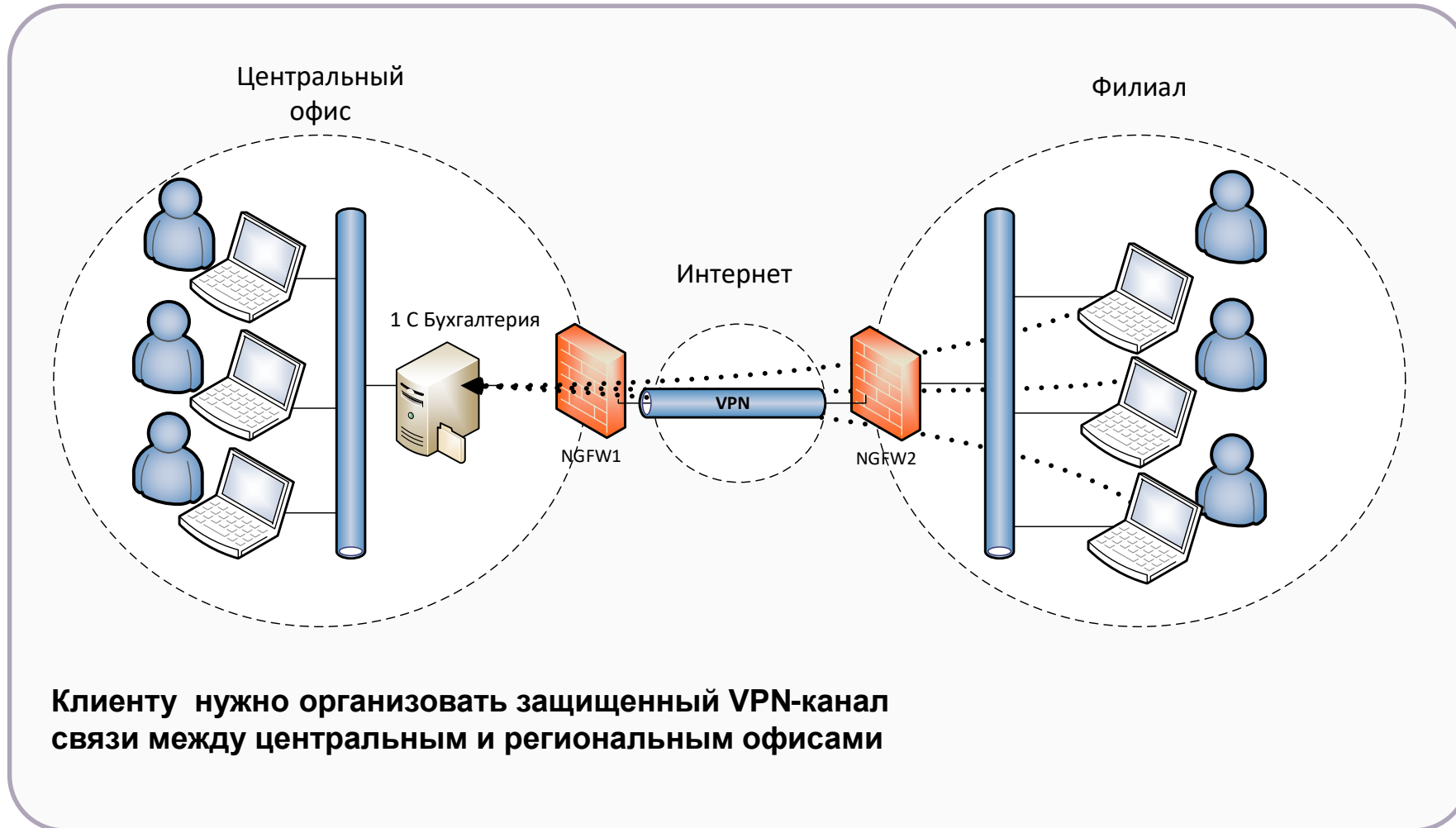
Пример схем подключения NGFW



Пример схем подключения NGFW



Пример схем подключения NGFW





Пробизнес

NGFW в облаке



Сравнение NSX и NGFW

NGFW

Это тип брандмауэра с широким спектром функций, которые обеспечивают защиту сети от различных угроз.

Основной упор в NGFW делается на обеспечение безопасности сети путем анализа трафика на основе более сложных критериев, чем просто IP-адреса и порты.

NSX

Это программно-определяемая сетевая платформа, разработанная VMware.

Основной упор в NSX делается на виртуализацию сети, предоставляя возможности создания виртуальных сетевых абстракций поверх физической сетевой инфраструктуры.

NSX и NGFW
являются разными технологиями,
применяемыми для разных целей

NSX - для виртуализации и управления сетью,
а NGFW - для обеспечения безопасности сети.

В некоторых случаях они могут использоваться вместе для достижения полной и безопасной виртуализированной инфраструктуры



Зачем NGFW нужны в облачной среде провайдера?

Защита от внешних атак

Облачные провайдеры часто являются целью внешних атак из-за объема хранимых данных и обработки трафика.

NGFW позволяют провайдерам фильтровать и мониторить весь входящий и исходящий трафик, что помогает предотвратить атаки, такие как DDoS, SQL-инъекции и многие другие.

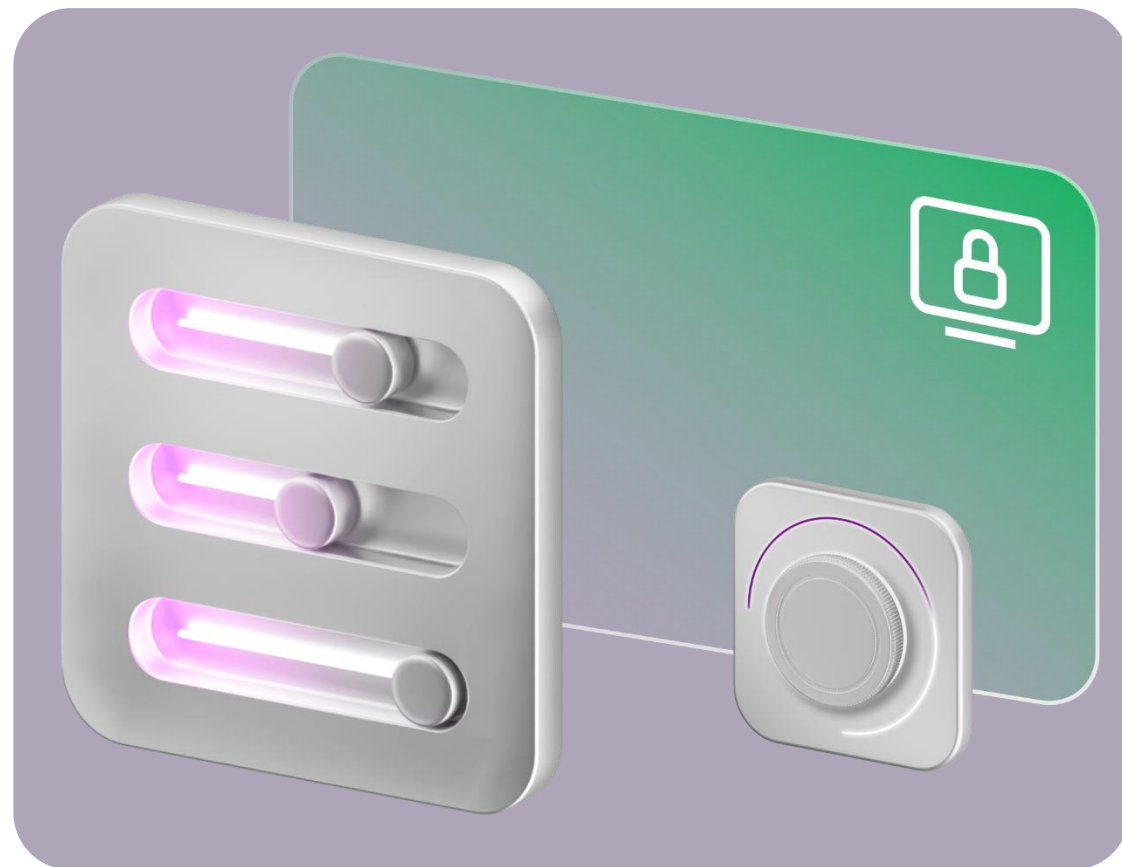


Зачем NGFW нужны в облачной среде провайдера?

Контроль доступа и безопасность данных

Облачные провайдеры помогают обрабатывать данные клиентам.

NGFW обеспечивают возможность управления доступом к этим данным, применение политик безопасности и шифрование трафика, чтобы предотвратить утечку или несанкционированный доступ



Плюсы NGFW в облачной среде провайдера

В облаке уже реализованы требования регуляторов ИБ:



Лицензии

ФСТЭК России
ФСБ России



Аттестаты

К1 и 1Г (согласно 17 приказу ФСТЭК)
УЗ-1 (в соответствии с ФЗ -152)



Сертификаты

ISO 9001, 20000, 27001
27017, 27018, ГОСТ Р
57580, соответствие
PCI DSS



Заключение

Размещая в облаке NGFW вы получаете:

- ✓ Готовую безопасность от провайдера на сетевом и физическом уровне
- ✓ Удобную модель лицензирования NGFW
- ✓ Готовое отказоустойчивое решение на уровне ИТ инфраструктуры
- ✓ Возможность управлять нагрузкой на ресурсы



Технологии включают бизнес

**Станислав
Погоржельский**

Руководитель по технологической
поддержке облачных
и инфраструктурных решений

stanislav.pogorzels@Megafon.ru