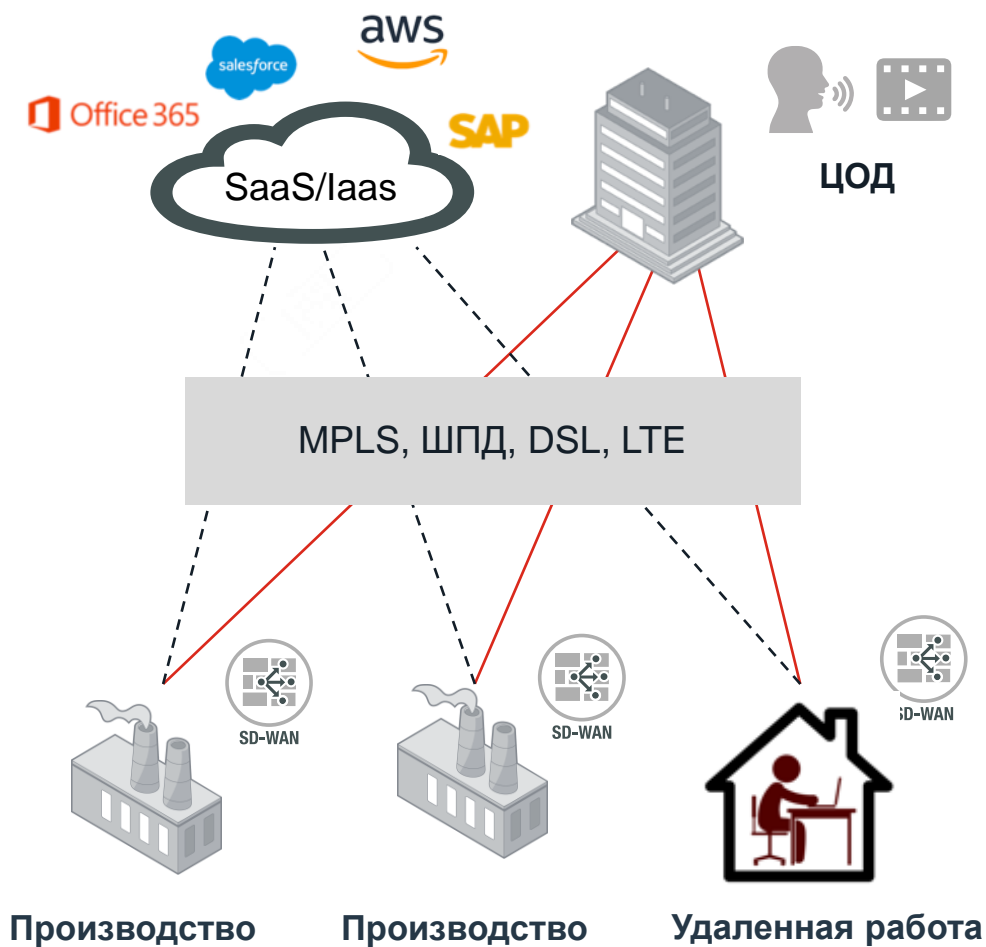




SD-WAN – сокращение OPEX тогда, когда это нужно

Алексей Андрияшин

Предпосылки возникновения SD-WAN



Корпоративный сектор

- Возможность управления сложной инфраструктурой

Средний и малый бизнес

- Эффективная работы с публичными облаками

MSSP

- Переход к сервисной модели потребления от аппаратных и программных решений



Основные **причины** перехода на SD-WAN



Развитие бизнеса

Новые филиалы
(слияния / поглощения).
Увеличение клиентской
базы (для MSSP).



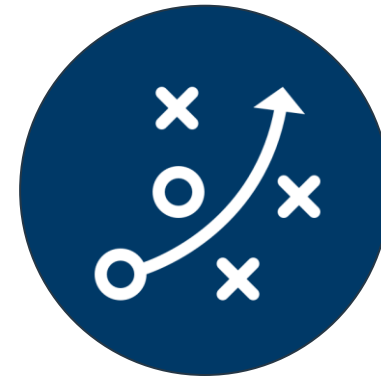
Сокращение расходов WAN

Как OPEX, так и
CAPEX.
MPLS дорог.
Старое
оборудование.



Высокая эффективность

Улучшение
производительности
бизнес-приложений.
Контроль качества
каналов и видимость.



Гибкость и безопасность

Переход в облака.
Повышение уровня
защищённости при
доступе к сети
Интернет.



Масштабируемость

Простое и удобное
управление всей сетью и
филиалами.
Возможность
предоставление
дополнительных сервисов.

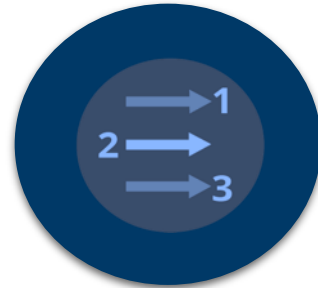
Типовые требования современных организаций к организации WAN

Быстрая адаптация среды передачи данных под изменяющиеся условия

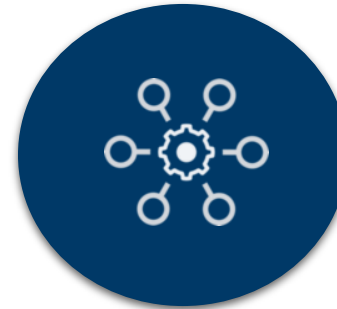
Преодоление сетевых проблем для оптимального взаимодействия

WAN Remediation Technique

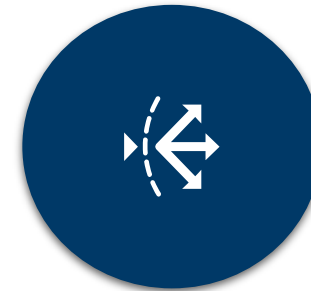
Упреждающая коррекция ошибок (FEC)



Многофакторный контроль состояния



Адаптивное управление трафиком



Набор приложений

Бизнес

Аудио/Видео

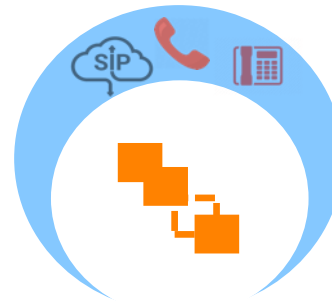
SaaS

UCaaS

Оптимизация производительности



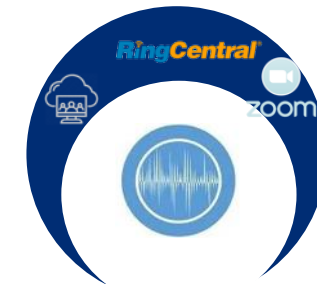
Субсекундное переключение



Уменьшение потери



Минимизация задержек



Нормализация джиттера

Безопасность – основное препятствие для SD-WAN

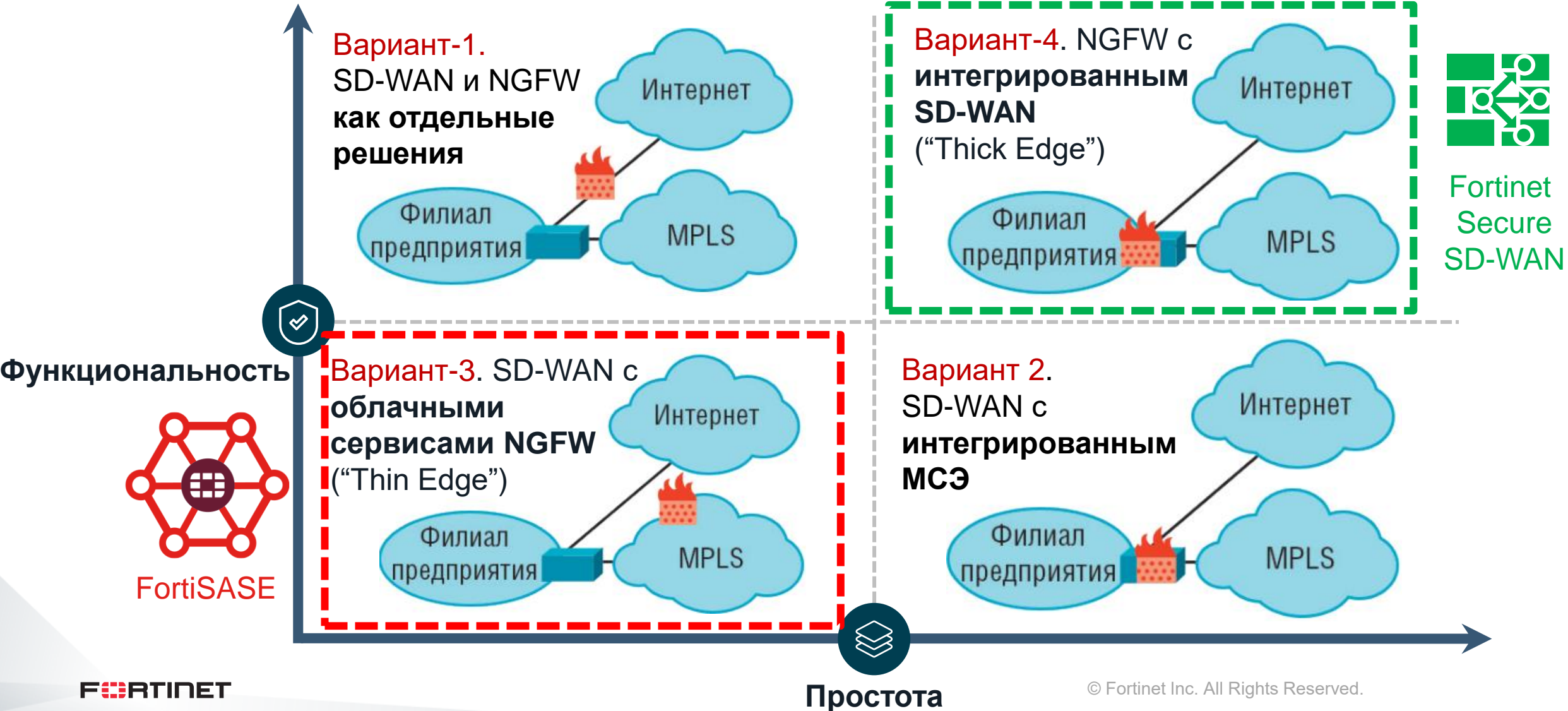


Base: Total, excluding no specific concerns; n = 303
Q07: What the top three biggest concerns (if any) with your overall WAN today?
ID: 355369

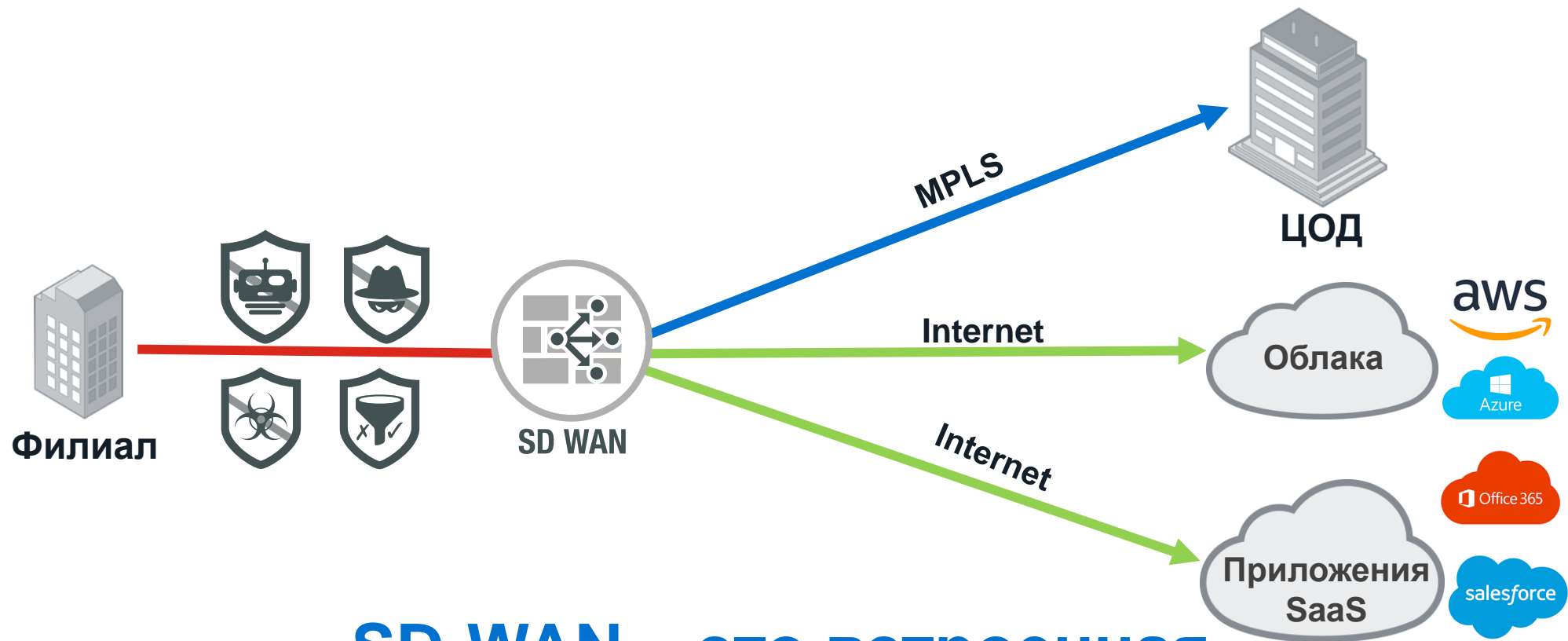
Информационная безопасность вызывает наибольшую обеспокоенность (72%) в проектах SD-WAN, наряду с производительностью (58%) и стоимостью (47%)

Gartner Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth, Naresh Singh, 12 November 2018

Архитектуры безопасности для SD-WAN



FortiGate NGFW с интегрированным SD-WAN



**SD-WAN – это встроенная
функциональная возможность FortiGate,
которая не требует лицензии**

FortiGate – лидерство и инновации NGFW



“Leader” - Magic Quadrant от Gartner (Network Security Firewall)



“Recommended” от NSS Labs (NGFW, DCIPS, ATP, DCSG, NGIPS и другие)

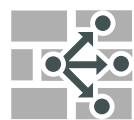
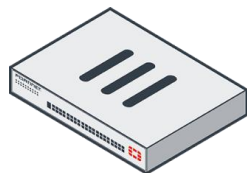


#1 – по количеству устройств безопасности (согласно IDC)

Защищённый SD-WAN

SD-WAN

NGFW



SD-WAN



Routing and Traffic Shaping

+



VPN

+



App Control

+



Intrusion Prevention

+



Antivirus

+



URL Filtering

+



Sandboxing

+



SSL Inspection

Высокая производительность и масштабируемость

Тесная интеграция решений и расширенная видимость



FORTINET

© Fortinet Inc. All Rights Reserved.

Специализированный для SD-WAN чип ASIC

Процессор FortiSOC4



Спроектирован
для **SD-WAN** и
SD-Branch

3X
Больше
производительности
в сравнении с SoC3

Поддержка
интерфейсов
10G

20G FW
12G IPSEC
1G SSL

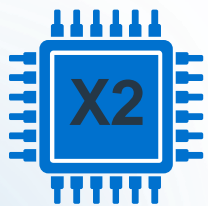
Новые шлюзы

FG-40F, FG-60F

FG-80, FG-100F

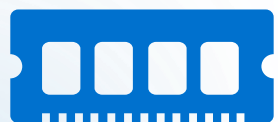


Модуль аппаратного ускорения **SD-WAN ASIC**



A53 QUAD

@ 1.4GHZ



DDR4-32B

@ 2400 MHZ



28,000

DMIPS



18X

NETWORK PORTS

SOC4



20 GBPS

THROUGHPUT



12 GBPS

IPSEC THROUGHPUT

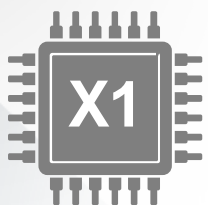


CAPWAP

SUPPORT

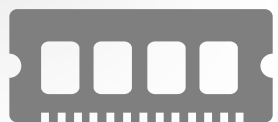
A9 QUAD

@ 1GHZ



DDR3-32B

@ 2400 MHZ



10,000

DMIPS



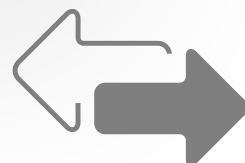
10X

NETWORK PORTS



10 GBPS

THROUGHPUT



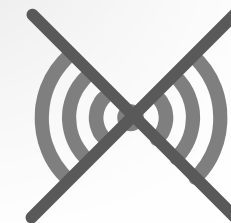
3 GBPS

IPSEC THROUGHPUT



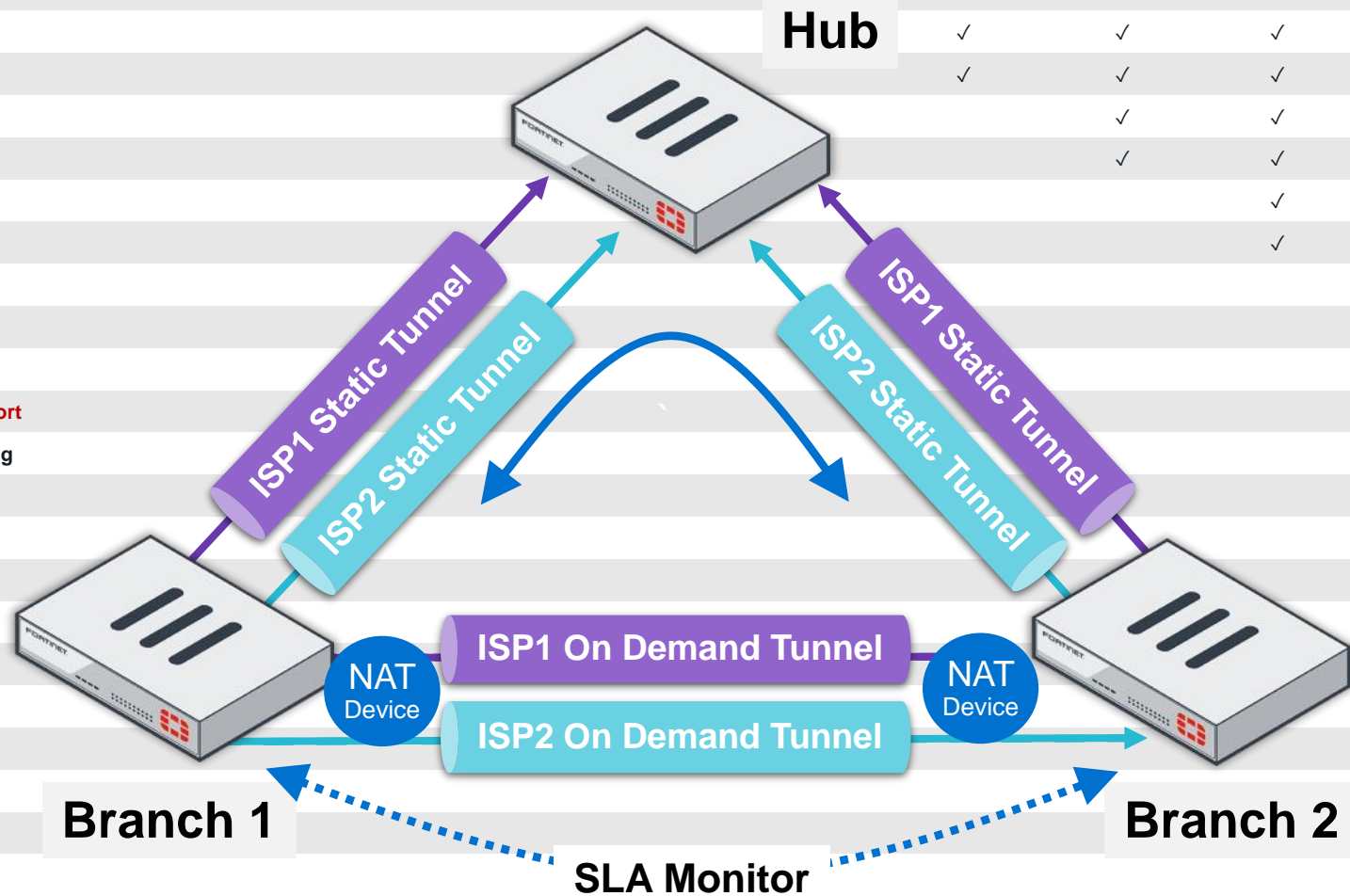
CAPWAP

SUPPORT

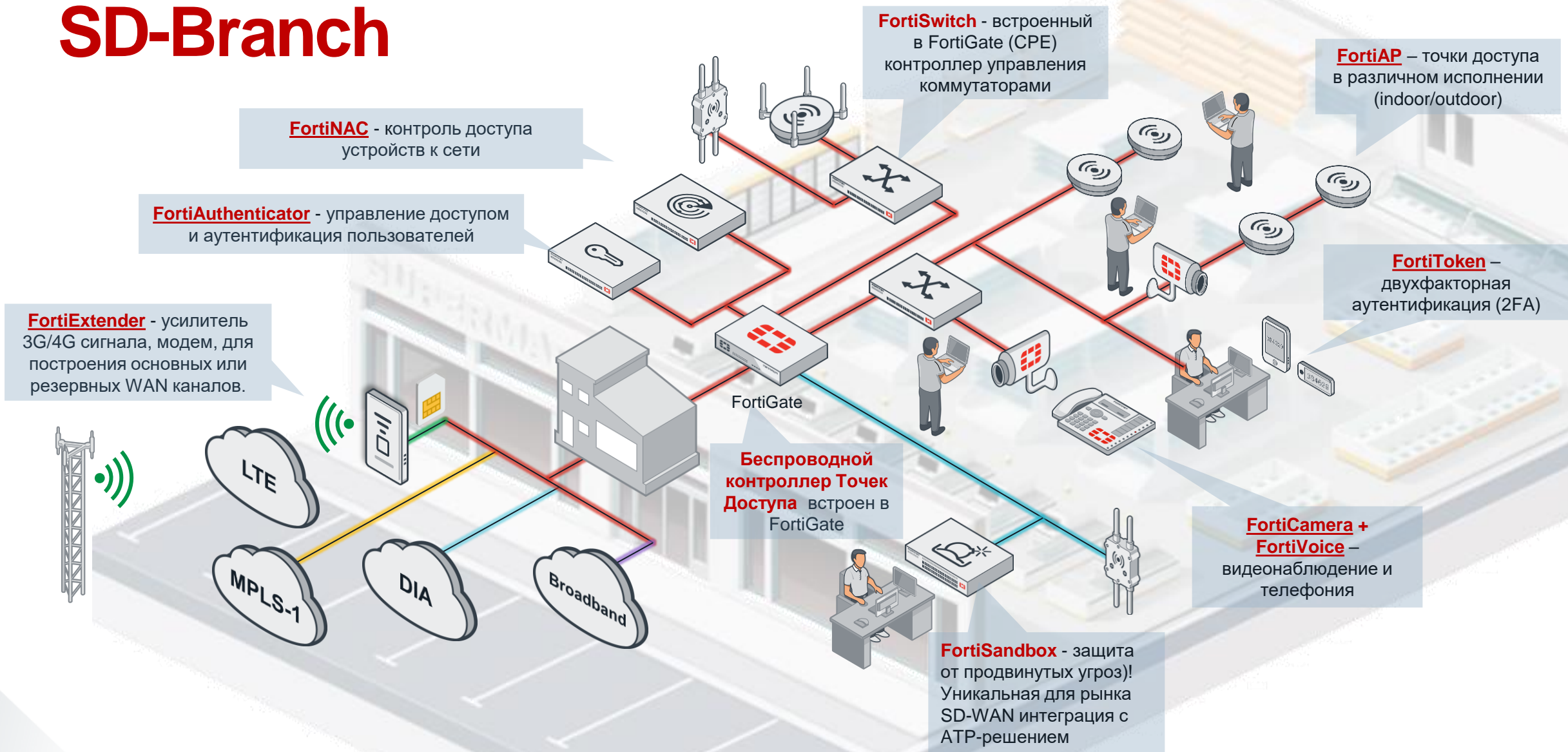


FortiOS – эволюция SD-WAN

Функциональные возможности SD-WAN в FortiOS	2.8	3.0	5.2	5.4	5.6	6.0	6.2	6.4
Policy Route	✓	✓	✓	✓	✓	✓	✓	✓
Equal-cost multipath (ECMP)		✓	✓	✓	✓	✓	✓	✓
Dead Gateway Detection		✓	✓	✓	✓	✓	✓	✓
Wan Link Load Balance			✓	✓	✓	✓	✓	✓
Zero Touch			✓	✓	✓	✓	✓	✓
ISDB				✓	✓	✓	✓	✓
Best Path Selection				✓	✓	✓	✓	✓
SD-WAN Interface					✓	✓	✓	✓
Security Fabric					✓	✓	✓	✓
Minimum SLA enforcement link steering						✓	✓	✓
Application Control						✓	✓	✓
FortiManager Template and Monitor						✓	✓	✓
Dynamic Routing (BGP) + Full IPv6 support						✓	✓	✓
Interface percentage based traffic shaping						✓	✓	✓
Forward Error Correction							✓	✓
SD-WAN rule load balance							✓	✓
Per packet load balance							✓	✓
Additional BGP path							✓	✓
ADVPN							✓	✓
Cloud-Assist Monitoring							✓	✓
Factory default health checks							✓	✓
VRF based segmentation								✓
Weighted aggregated IPSEC tunnels								✓
Multiple SLA metrics link steering								✓
ADVPN health check probes								✓



Консолидация сервисов в SD-Branch



Приоритезация и классификация приложений



Расширенная база обновляемых приложений и веб-категорий

Динамически-обновляемая база данных облачных приложений (на основании IP адресов и портов)

Классификация и направления приложений по первым пакетам

Видимость, мониторинг и контроль приложений и порталов



Отслеживание качества SLA



SLA ПО ГРУППАМ И ПРИЛОЖЕНИЯМ



Latency < 100ms
Packet Loss < 1%
Jitter < 30ms



Skype
for Business



**НЕСКОЛЬКО МЕТОДОВ
ОТСЛЕЖИВАНИЯ
КАЧЕСТВА**

- Ping
- HTTP
- TCP Echo
- UDP Echo
- TWAMP



**ГИБКОЕ ЗАДАНИЕ
ПАРАМЕТРОВ**



Настройка интервалов

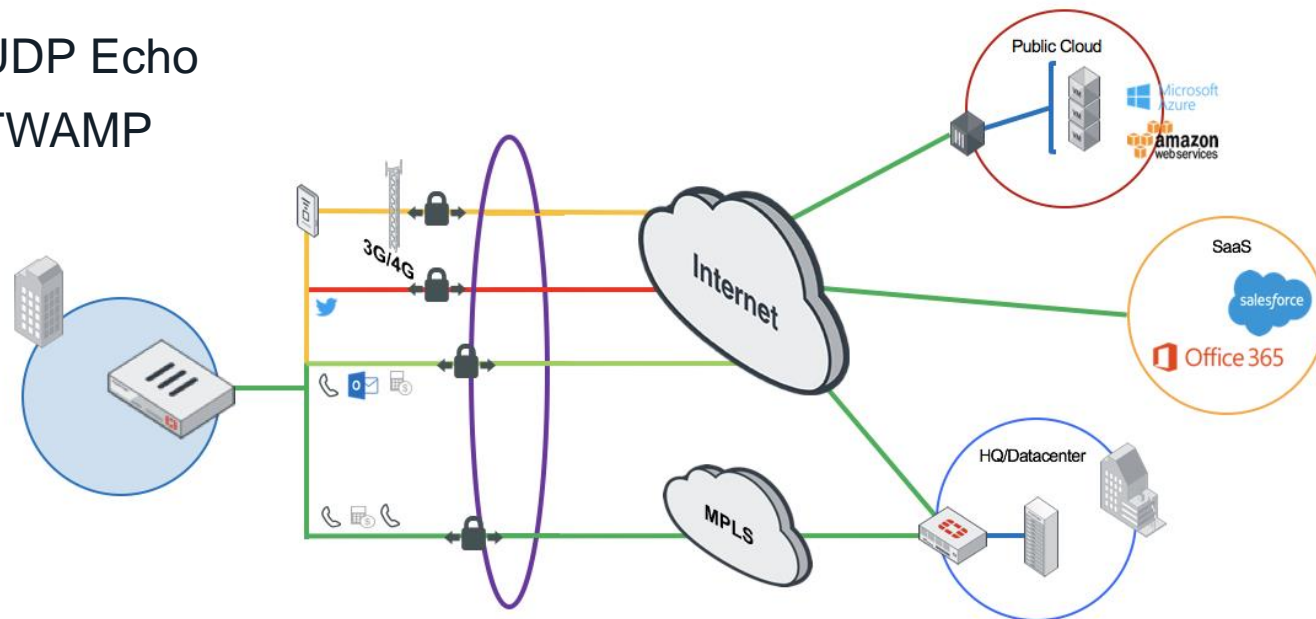


Исключение flapping

Traffic Shaper

Параметры QoS

Динамическое переключение



SDWAN и централизованное управление



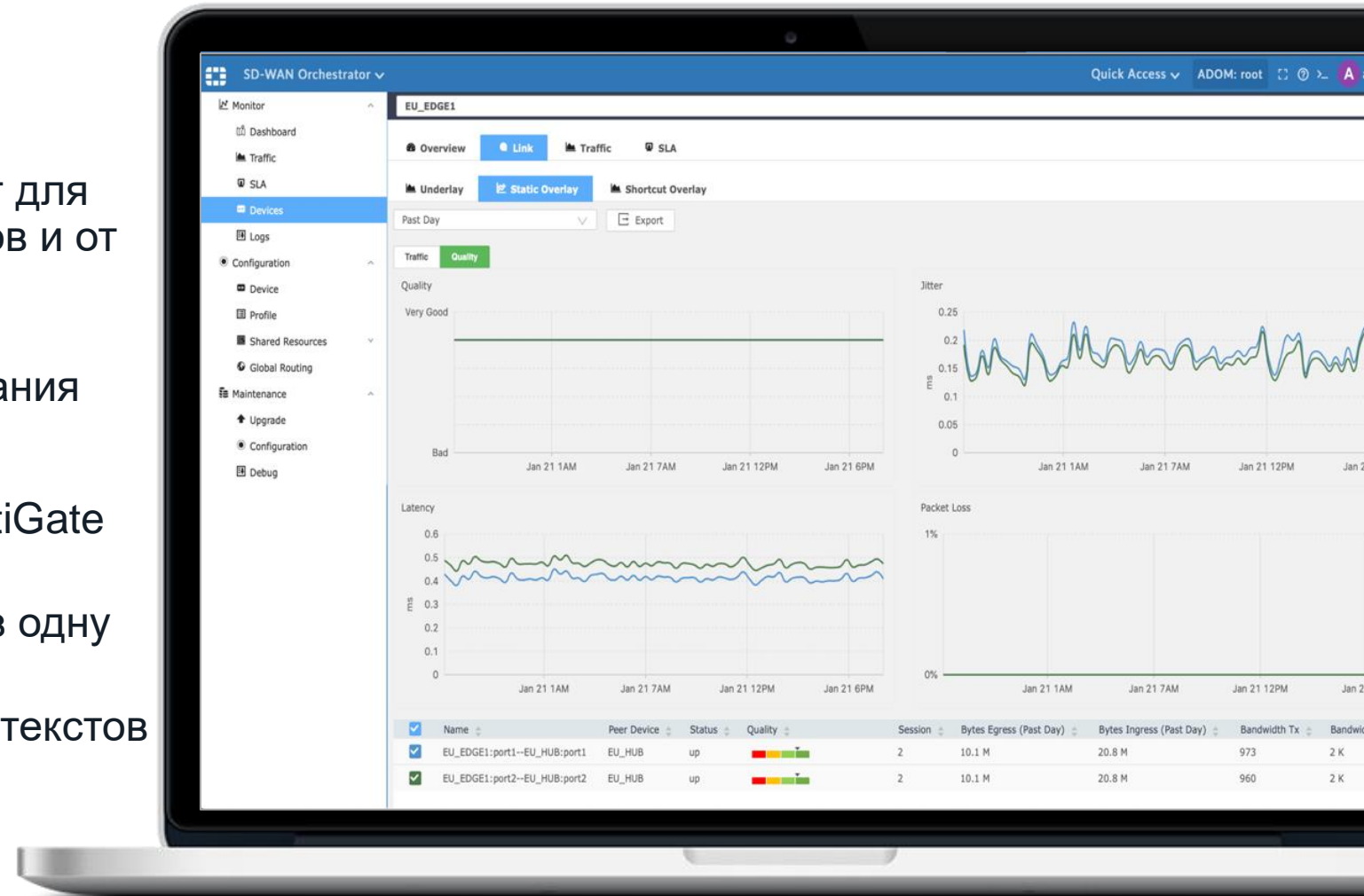
Гибкое масштабирование операций управления

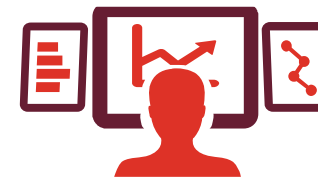
• Требования бизнеса

- Минимизация ошибок на этапе развёртывания сервисов и услуг для снижения рисков сетевых отказов и от киберугроз
- Упрощение и повышение эффективности администрирования

• Ключевые особенности

- Масштабирование до 100k+ FortiGate
- Управление SD-Branch (точками доступа и коммутаторами) через одну консоль
- Гибкость при использовании контекстов ADOM (multi-tenancy)
- Ролевой доступ к управлению, аудит действий





Отчётность и аналитика SD-WAN

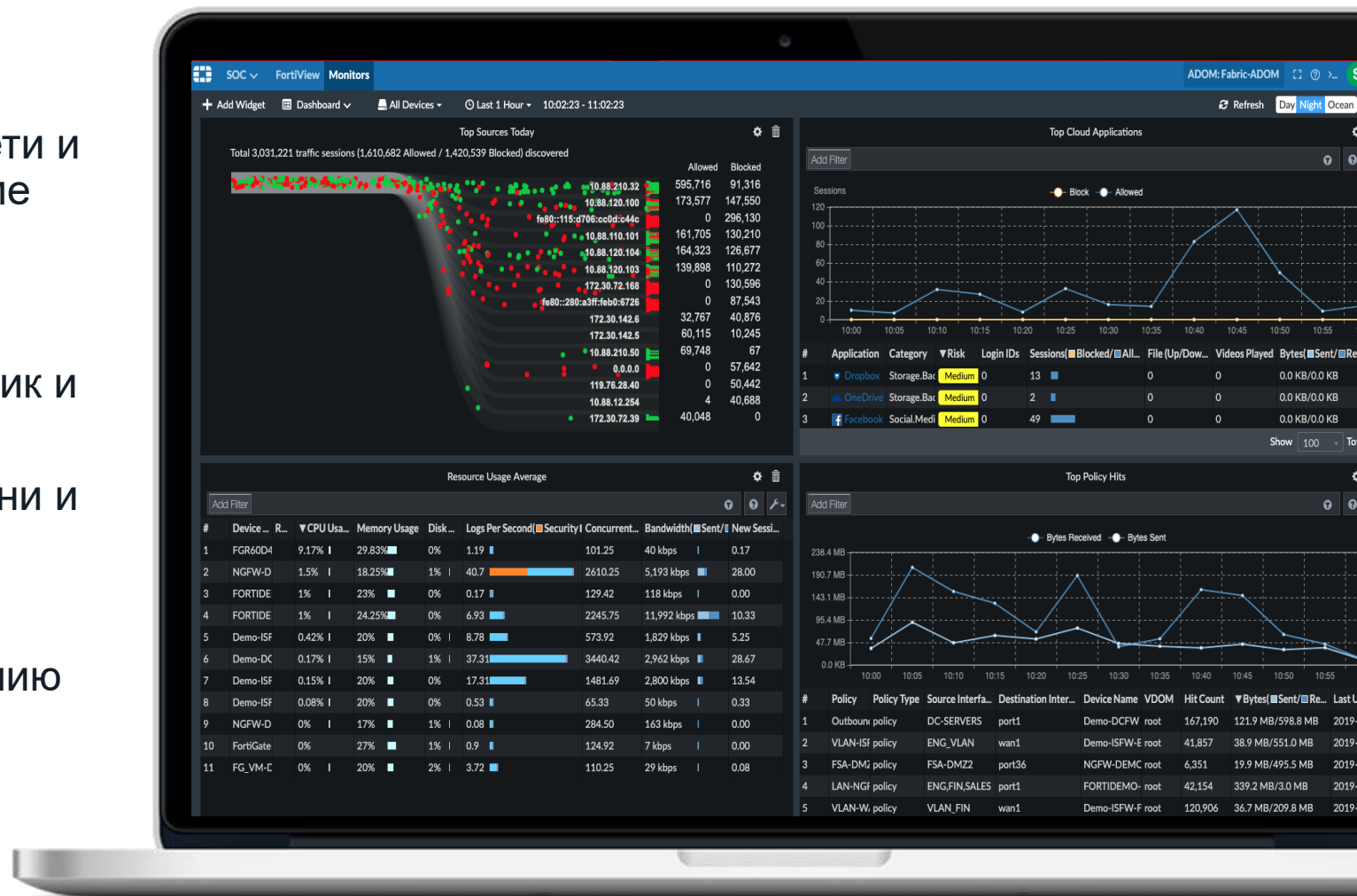
Продвинутый мониторинг

• Требования бизнеса

- Оценка и измерение состояния сети и состояния защищённости в режиме реального времени

• Ключевые особенности

- Видимость ключевых характеристик и параметров сети
- Отчёты по SLA в реальном времени и историческом разрезе
- Мониторинг VPN-туннелей
- Виджеты и отчёты по использованию приложений, сетевых атак и др.
- Программирование обработчиков событий
- Мониторинг **NOC** и **SOC**





SDWAN и Zero Touch Provisioning (ZTP)

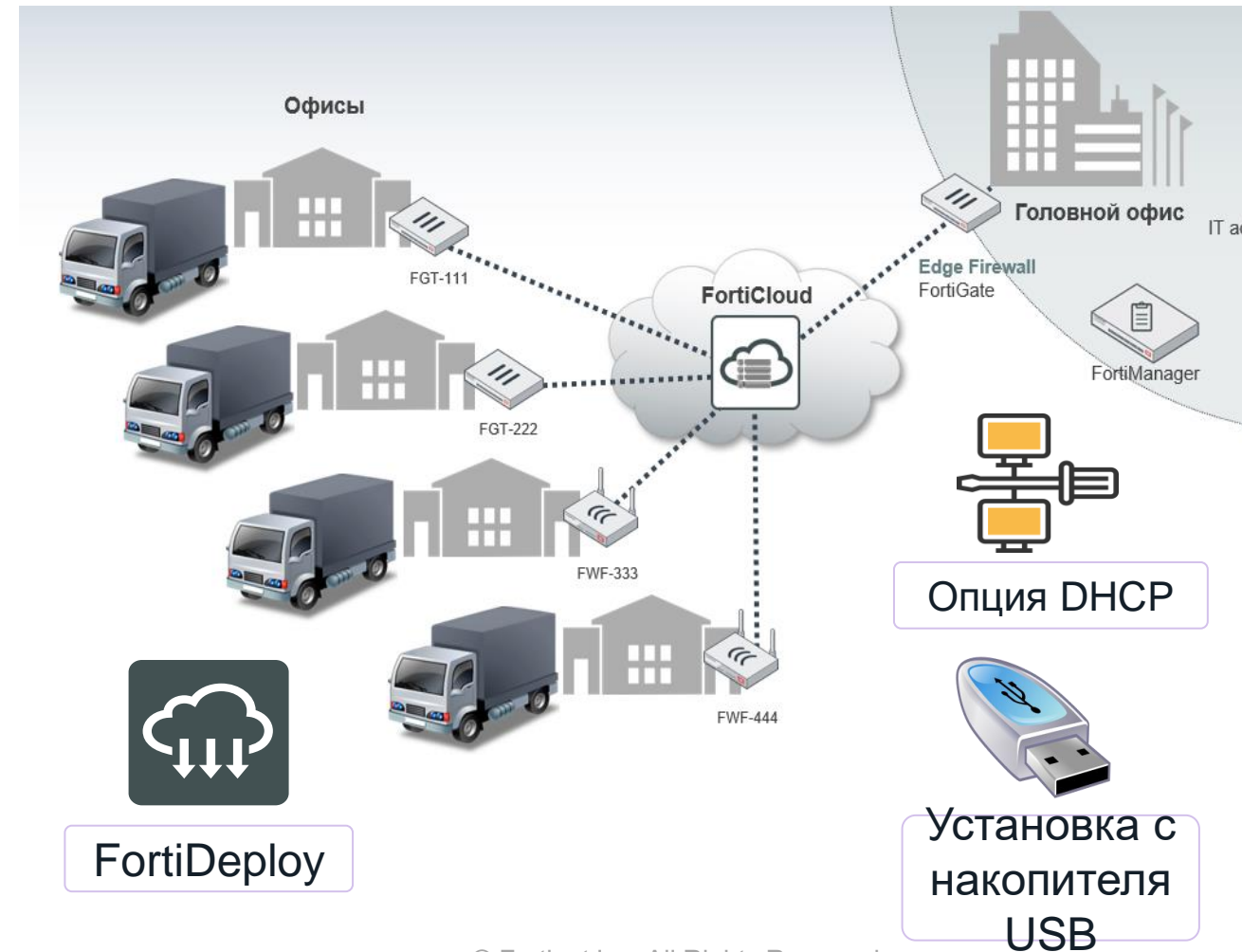
Быстрое развёртывание

- **Требования бизнеса**

- Повышение эффективности управления
- Уменьшение времени на развёртывание, оптимизация затрат

- **Ключевые особенности**

- Zero Touch Provisioning < 6 минут (проверено by NSS labs)
- Шаблоны конфигураций для SD-WAN, SD-Branch & NGFW
- Сценарии автоматизации и скрипты (Ansible, DevOps)
- Управление резервными копиями и ревизиями конфигураций



Fortinet SD-WAN – признан Gartner



- Fortinet SD-WAN **должен находиться в списке решений** для всех активностей по теме **WAN edge**
- **Видение рынка и планы развития** соответствуют взгляду Gartner на потребности клиентов: SD-WAN, продвинутые сетевые возможности и безопасность в одном решении
- Fortinet инвестирует в разработку специализированных модулей **аппаратной обработки** трафика SD-WAN
- Может быть основным решением как для **Enterprise**, так и **операторов MSP/MSSP**

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Множество **рубежей** должны быть защищены

Всегда и везде

Удалённая работа

70% положительно относятся к удалённой работе

2020 State of Remote Work, Buffer

Единая защита

Единые сервисы безопасности для пользователей и устройств, как в сети, так и за её пределами

2020 FortiGuard Threat Report, Fortinet

Миграция в облака

93% организаций готовы к переходу в облака

2020 State of the Cloud Report, Flexera



SASE (Secure Access Service Edge) – термин Gartner

К 2024 году до 40% заказчиков примут стратегии применения технологий SASE



Клиенты предъявляют требования к простоте, масштабируемости, гибкости, низким задержкам и объединению решений WAN Edge и сетевой безопасности

Gartner.

Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge – 29 July 2019

Source: Gartner

Сеть-как-Сервис



Подключить

- SD-WAN
- WAN-оптимизация
- Маршрутизация
- Bandwidth Aggregators
- Networking Vendors

Безопасность-как-Сервис



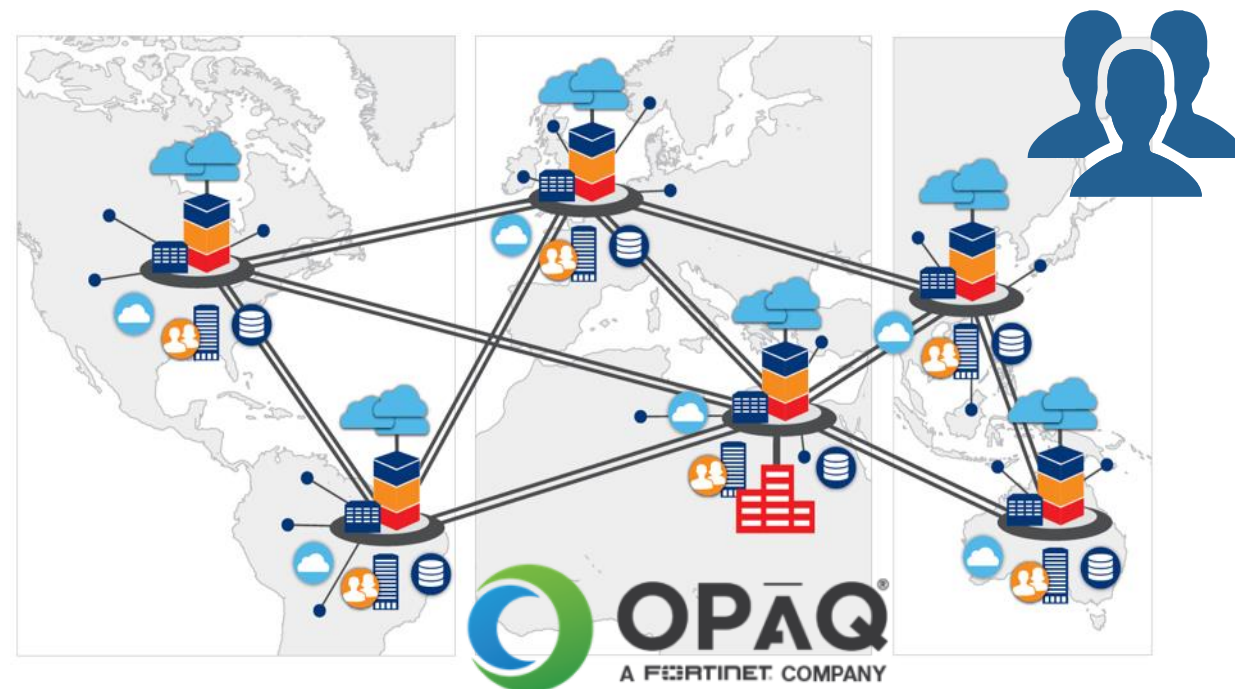
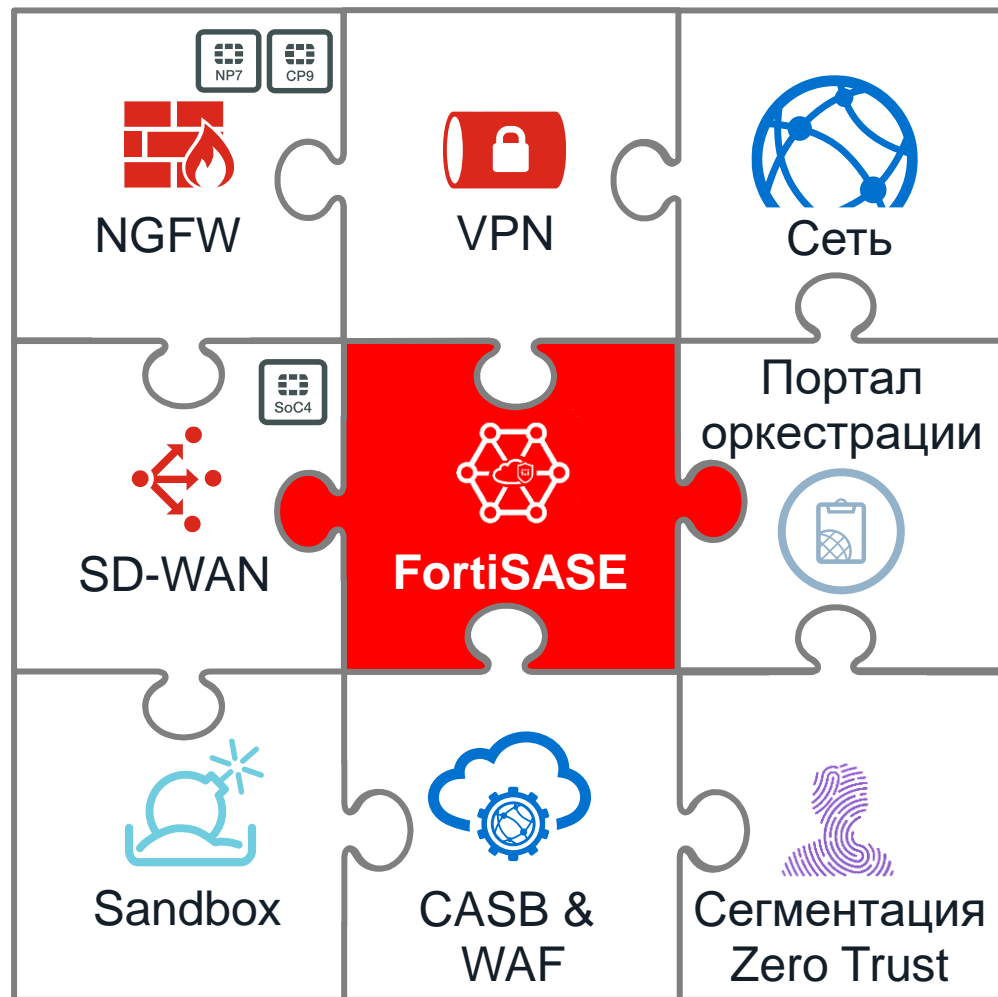
Защитить

- Сетевая безопасность
- FW как сервис (FWaaS)
- Облачный брокер CASB
- Облачный прокси (SWG)
- ZTNA (Zero Trust Network Access)
- VPN
- Защита DNS
- RBI (Remote Browser Isolation)

**Secure Access
Service Edge**

© Fortinet Inc. All Rights Reserved.

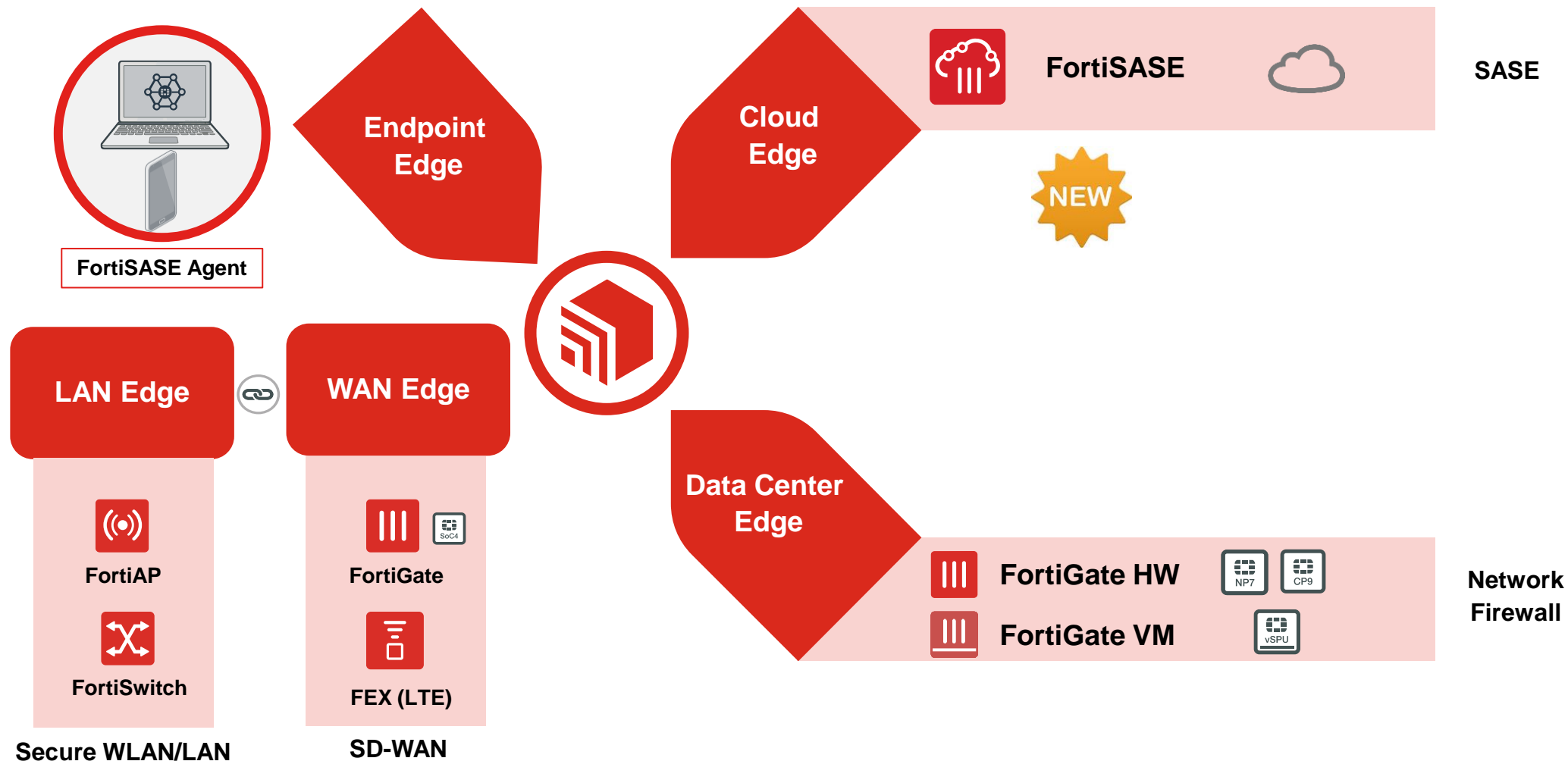
FortiSASE – дополнительные преимущества



- Распределённая структура
- Множество точек присутствия на всех континентах
- Прямые пиринговые подключения к популярным SaaS, IaaS, и крупным ЦОД
- Компетенции и экспертиза DevOps, SDN и сети

Архитектура Security-Driven Networking

У вас есть выбор, где применить меры защиты



Заключение: почему Fortinet?

Цифровая трансформация



Продвинутая безопасность, широкая поддержка облачных сервисов и приложений



Видимость и инспекция трафика (SSL Deep Inspection)



Гибкое управление доступом на уровне пользователей, приложений

Оптимизация затрат



Лучшие в индустрии оценки TCO



Обеспечение высокой доступности, качественные механизмы балансировки



Высокая производительность и масштабируемость

Расширение до SD-Branch



Единая консоль управления, видимости и ZTP



Входит в состав Fortinet Security Fabric: расширение сервисов в филиале



Автоматизация (помещение в карантин, механизмы защиты на уровне порта/устройства)

FORTINET[®]

SD-WAN от Fortinet одним слайдом

- ✓ Включён в состав FortiOS
- ✓ Работает на всех FortiGate
- ✓ Не лицензируется

- ✓ Отслеживание SLA (джиттер, задержки, потери и др.)
- ✓ Гибкие правила управления трафиком
- ✓ Учёт качества в реальном времени

Это **функциональность** FortiGate для **интеллектуальной балансировки**

сервисов, приложений на основании их критичности и **требований к QoS**

по **оверлейной сети** с применением **безопасности NGFW.**

- ✓ Протоколы и сервисы
- ✓ База интернет-ресурсов (ISDB)
- ✓ Видимость, управления на уровне приложений L7 и FQDN (Application awareness)

- ✓ Любой тип WAN подключений
- ✓ Ускорение на чипах ASIC
- ✓ Мобильные сети 3G/4G
- ✓ Туннели VPN, GRE...

- ✓ Функции безопасности NGFW от FortiGate
- ✓ Инспекция SSL (включая TLS 1.3)

- ✓ Очереди, приоритезация и шейпирование
- ✓ Гарантирование полосы