DIGITAL EDITION

FORTINET®

SECURITY DAY

Защищенный SD-WAN и SD-Branch от Fortinet

Максим Порицкий, системный инженер

6 апреля 2021 | Киев | Минск



Содержание



1 Традиционная WAN vs Secure SD-WAN

2 Архитектура и компоненты решения Secure SD-WAN

3 Независимые оценки

4 Варианты использования Secure SD-WAN

5 Secure SD-Branch

Традиционная WAN vs Secure SD-WAN

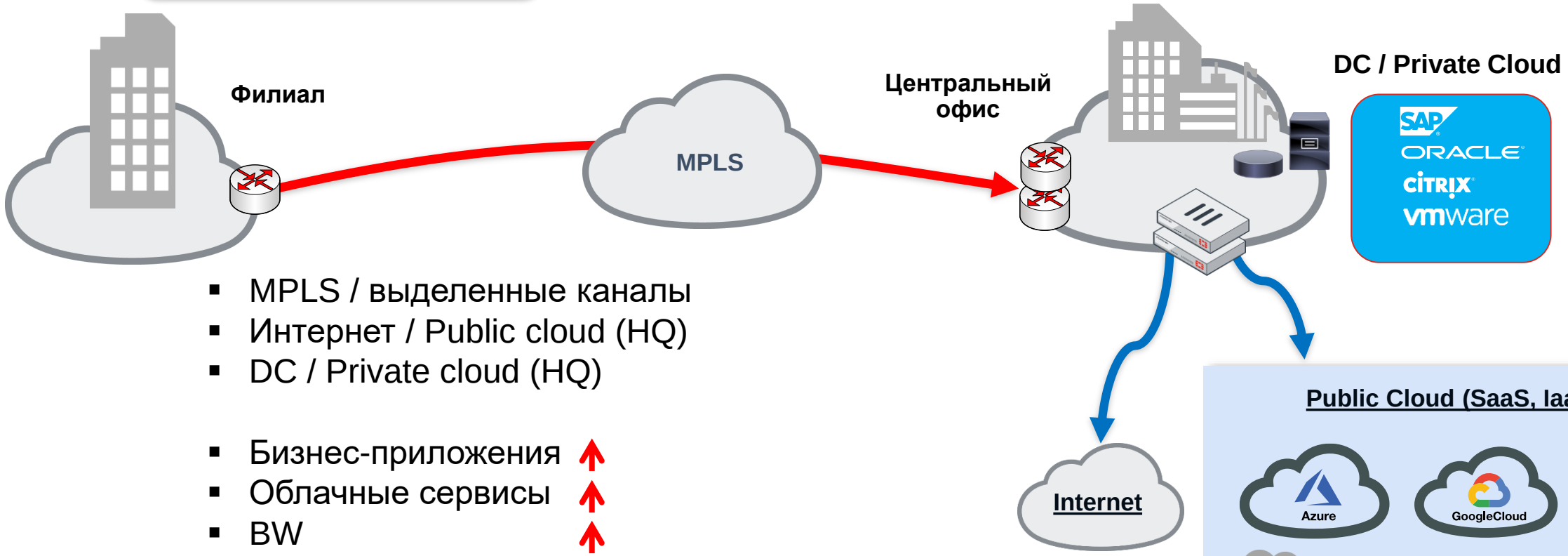
Традиционная WAN

Какие проблемы заставляют задуматься о модернизации WAN

MPLS/выделенные каналы
дорогие каналы связи

Весь трафик
маршрутизируется в HQ
инспектируется в HQ

Балансировка / резервирование
Без учета характеристик каналов в реальном времени



- MPLS / выделенные каналы
- Интернет / Public cloud (HQ)
- DC / Private cloud (HQ)

- Бизнес-приложения ↑
- Облачные сервисы ↑
- BW ↑
- Задержки ↑
- MPLS Cost ↑

© Fortinet Inc. All Rights Reserved.

Secure SD-WAN

Что это и кому будет полезно ?

SD-WAN – набор технологий по построения современной WAN

1 **Улучшение производительности приложений (повышение удовлетворенности пользователей)**

- Интеллектуальная **идентификация приложений** и определения для них лучшего **канала связи** путем **контроля характеристик каналов** в режиме реального времени (packet loss, latency, jitter)

2 **Обеспечение безопасного доступа в Internet / Public Cloud**

- **Расширенный функционал безопасности** (NGFW+SSL Inspection) при доступе в Internet и Public Cloud из филиала / центрального офиса

3 **Упрощение дизайна WAN**

- **Интеграция в одном устройстве** сервисов WAN Edge: **интеллектуальная маршрутизация,** QoS, FEC/PD, балансировка, failover, **сетевая безопасность ….**

© Fortinet Inc. All Rights Reserved.

Secure SD-WAN

Что это и кому будет полезно ?

4 **Упрощение управления и внедрения**

- Единая **централизованная система управления** “Security + SD-WAN + switching + wireless”
- Система внедрения **ZTP**

5 **Экономия затрат (OpEx, CapEx) и гибкость подключения**

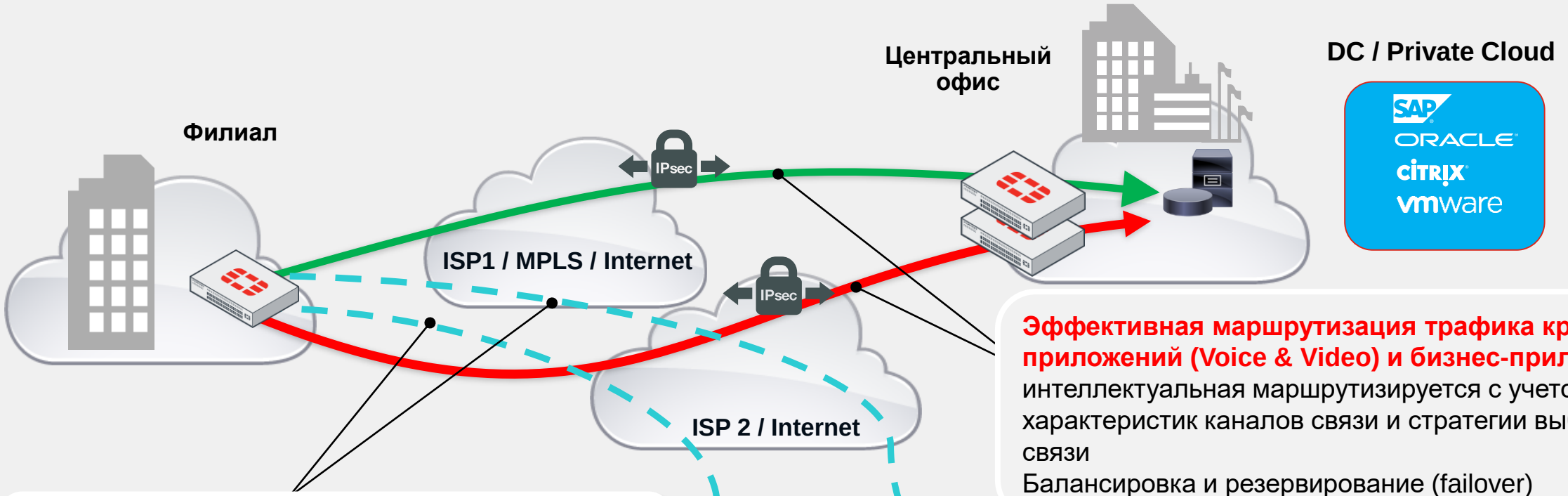
- **Уменьшение операционных расходов** за счет использования **различных каналов связи** (broadband, MPLS, 4G/LTE) для подключения филиалов
- **Консолидация функций в одном устройстве**

6 **Интеграция с LAN инфраструктурой (Secure SD-Branch)**

- Интегрированный **контроллер коммутаторов и ТД** (управление, конфигурация и мониторинг), FOS NAC
- **Интеграция** с FNAC, FSA, FAC
- **Безопасность пользовательских устройств** (FCL)
- **2FA**

© Fortinet Inc. All Rights Reserved.

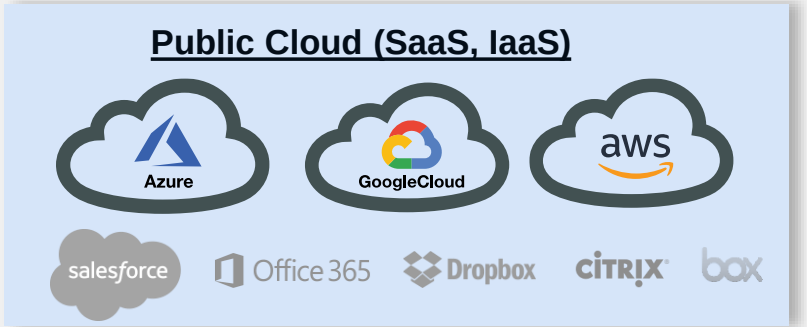
Реализация WAN с использованием Secure SD-WAN



Эффективная маршрутизация трафика критичных приложений (Voice & Video) и бизнес-приложений
интеллектуальная маршрутизируется с учетом характеристик каналов связи и стратегии выбора каналов связи
Балансировка и резервирование (failover)

Безопасный доступ в сеть Интернет и к сервисам в Public Cloud
Балансировка и резервирование (failover)

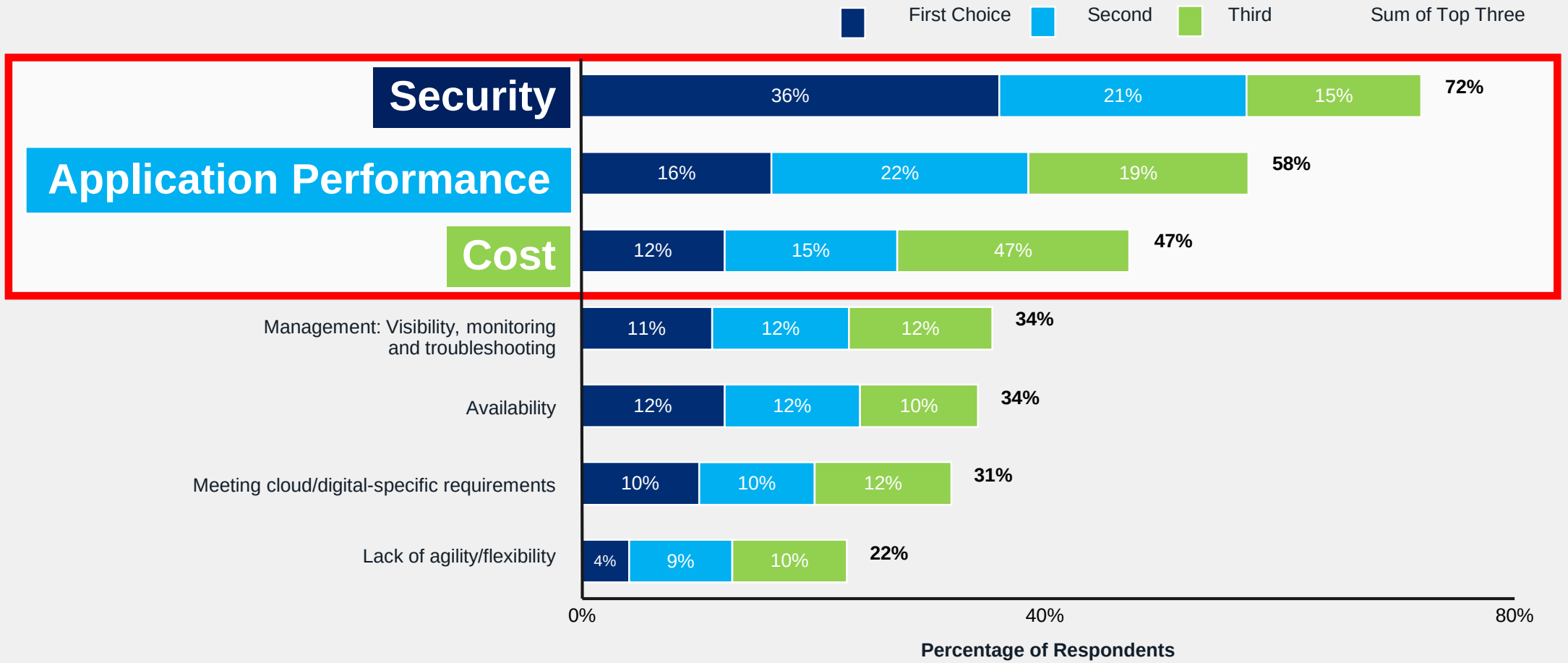




SD-WAN технологии входят в состав ОС FortiOS и не требуют отдельного лицензирования

© Fortinet Inc. All Rights Reserved.

Gartner: “Какие три основные проблемы (если таковые имеются) с вашей WAN сегодня ?”



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

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

Заказчики считают, что безопасность является основным вопросом в рамках существующих WAN, за которыми следуют производительность приложений и стоимость решения WAN

Компоненты решения Secure SD-WAN

Secure SD-WAN

Компоненты решения

1.  **FortiGate** – корпоративный Firewall с функционалом SD-WAN (FGT)

2.  **FortiManager** – централизованная система управления и мониторинга (FMG)

3.  **FortiAnalyzer** – централизованная система сбора, анализа и корреляции журнальных файлов (логов) и обеспечение отчетности (FAZ)

4.  **FortiGate Cloud** – облачная централизованная система управления и мониторинга

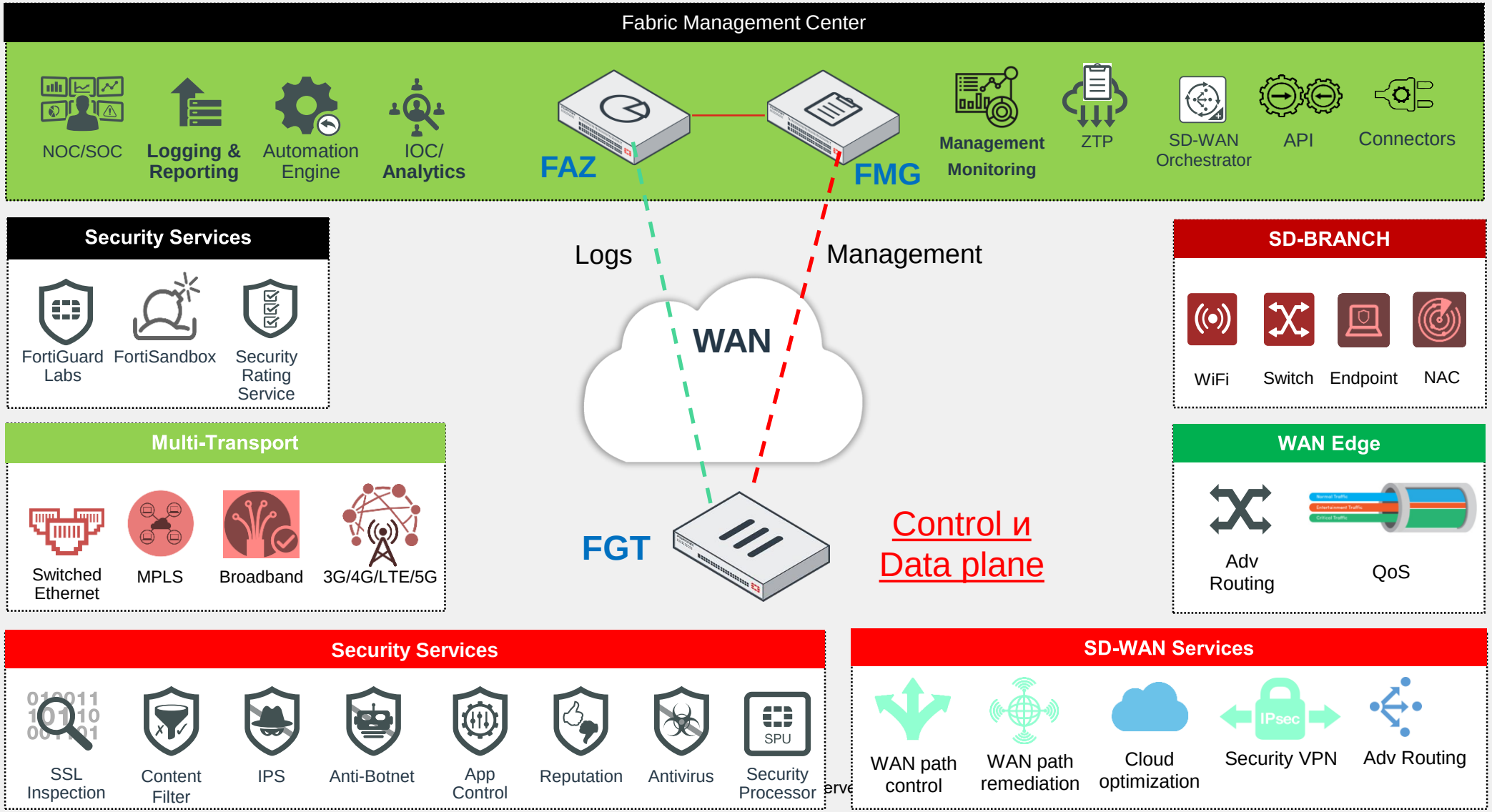
   FortiDeploy – компонент ZTP в составе FortiGateCloud

© Fortinet Inc. All Rights Reserved.

Архитектура Secure SD-WAN

Архитектура Fortinet Secure SD-WAN (Controllerless)

Orchestration и Management plane

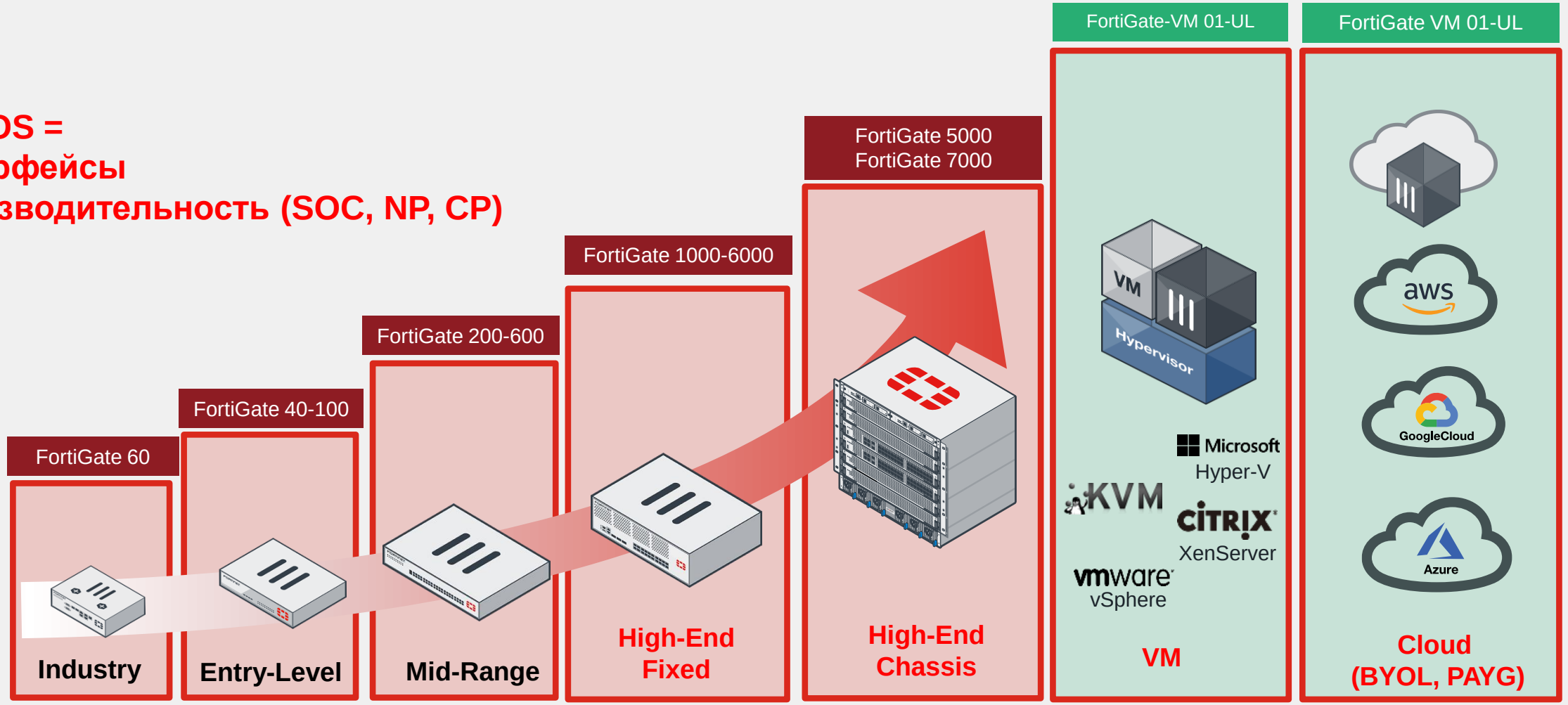


FortiGate

FortiGate – модельный ряд*

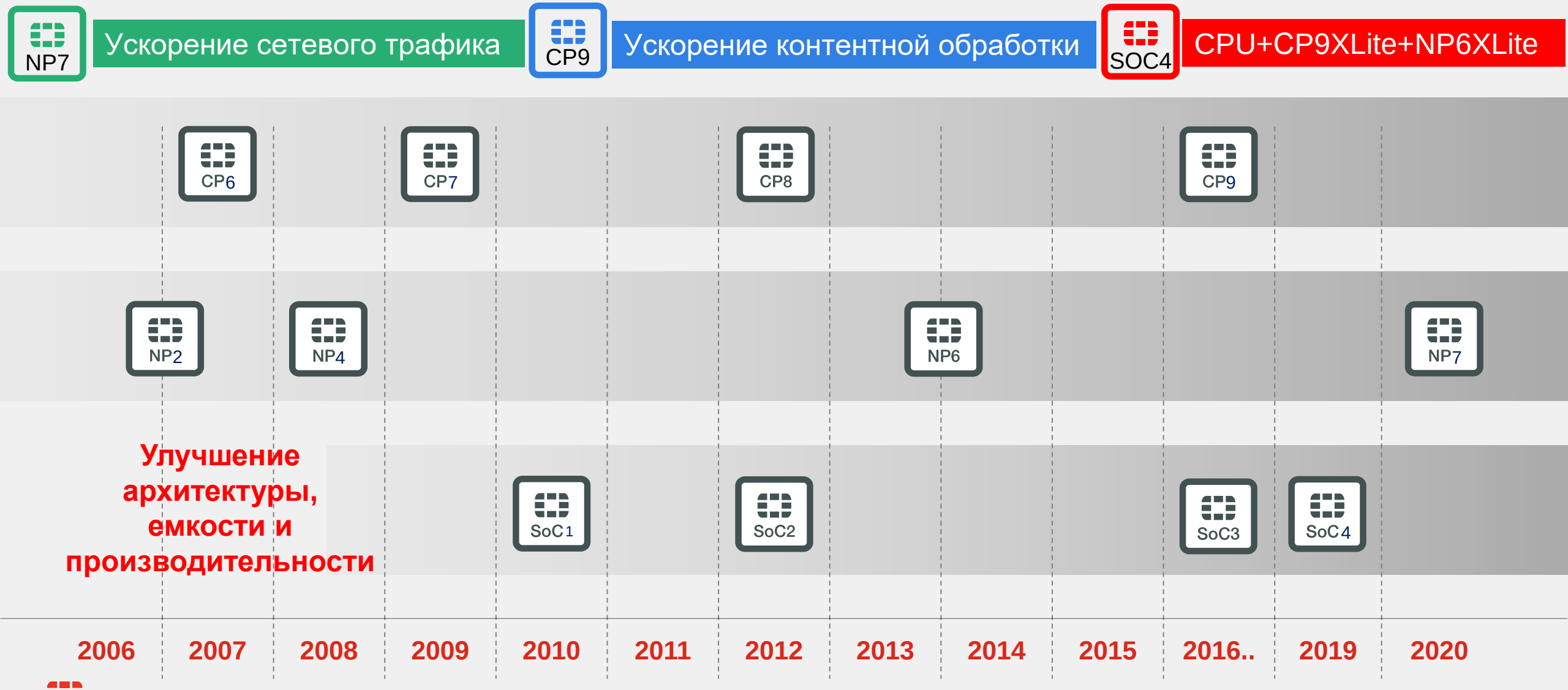
От небольших филиалов до крупных ЦОД

FortiOS =
Интерфейсы
Производительность (SOC, NP, CP)



*Top Selling Models - https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf

Эволюция Fortinet Security Processor Unit (SPU)



© Fortinet Inc. All Rights Reserved.

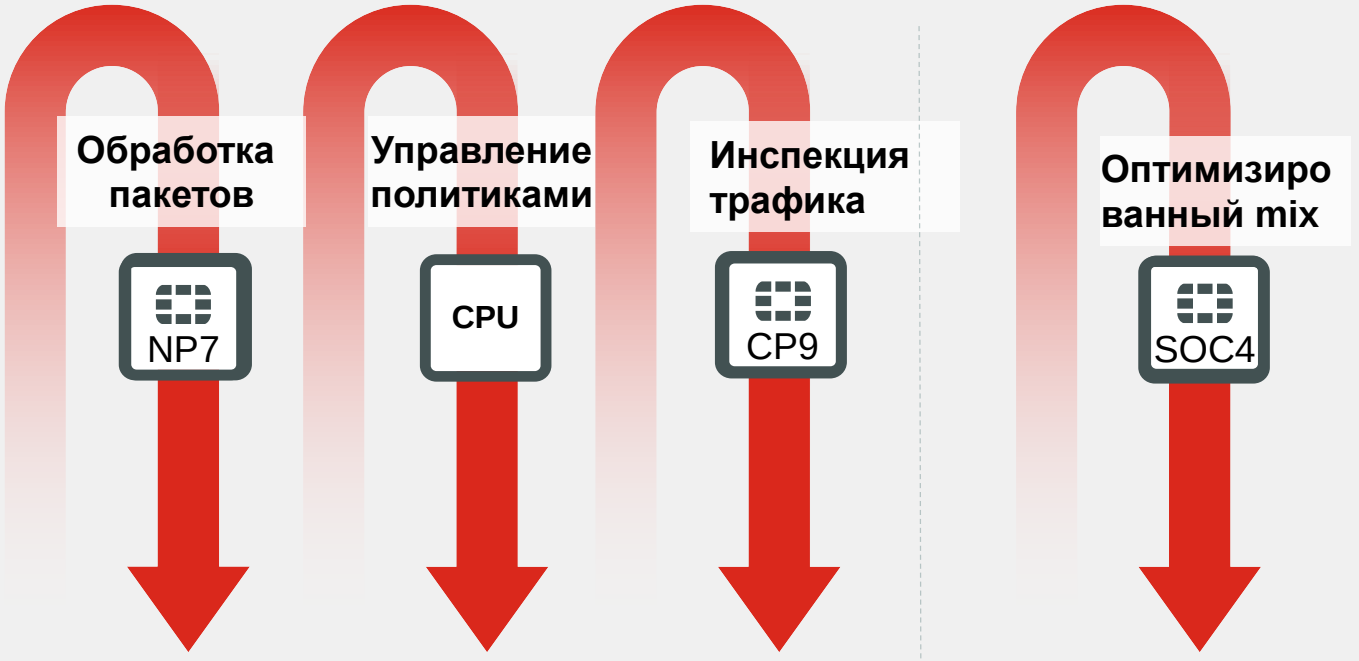
Преимущества использования SPU

CPU Only «классический подход»



Большинство производителей оборудования

Архитектура Fortinet Parallel Path Processing (PPP)



- IPv4/IPv6 FW
- IPSec VPN
- Multicast

- Session est
- Configuration
- Logging
- Reporting

- SSL VPN
- SSL Deep Inspection
- UTP (IPS, AC, Anti-Malware)



Выше производительность



Меньше задержка

© Fortinet Inc. All Rights Reserved.

Функционал безопасности FGT

1 Application Control



5 WEB- и DNS-filter



2 IPS



6 IPSec, SSL/TLS VPN, ADVPN



3 Anti-Botnet



7 SSL/TLS Inspection



4 Anti-Malware



8 FSA Integration



© Fortinet Inc. All Rights Reserved.

Функционал SD-WAN FGT

1 **Управление маршрутизацией через WAN (path control)**

- Идентификация приложений (FortiGuard, 5000+)
- Мониторинг характеристик каналов связи + SLA
- Динамический выбор канала на основе правил
- Переключение маршрутизации (→ path failover)

2 **Восстановление/улучшение работы на WAN (path remediation)**

- Forward error correction (→ восстановление)
- Дублирование пакетов (→ восстановление)
- Балансировка трафика через Aggregation IPSec VPN (per packet / by the weight → увеличение BW)

3 **Маршрутизация трафика приложений на основе пользовательских групп (User Identity Based)**

© Fortinet Inc. All Rights Reserved.

FortiManager

FortiManager

1 Управление, конфигурация, мониторинг

- Централизованная система управления и конфигурации FW, коммутаторов, ТД
- Маршрутизация, коммутация, wireless, SD-WAN, security, VPN ….

2 Multi-Tenancy и Role-Based Administration

- Многопользовательское (ADOM) и ролевое администрирование

3 SD-WAN Orchestration и Analytics

- Упрощение и автоматизация ряда конфигураций для SD-WAN (опционально)

© Fortinet Inc. All Rights Reserved.

FortiAnalyzer

FortiAnalyzer

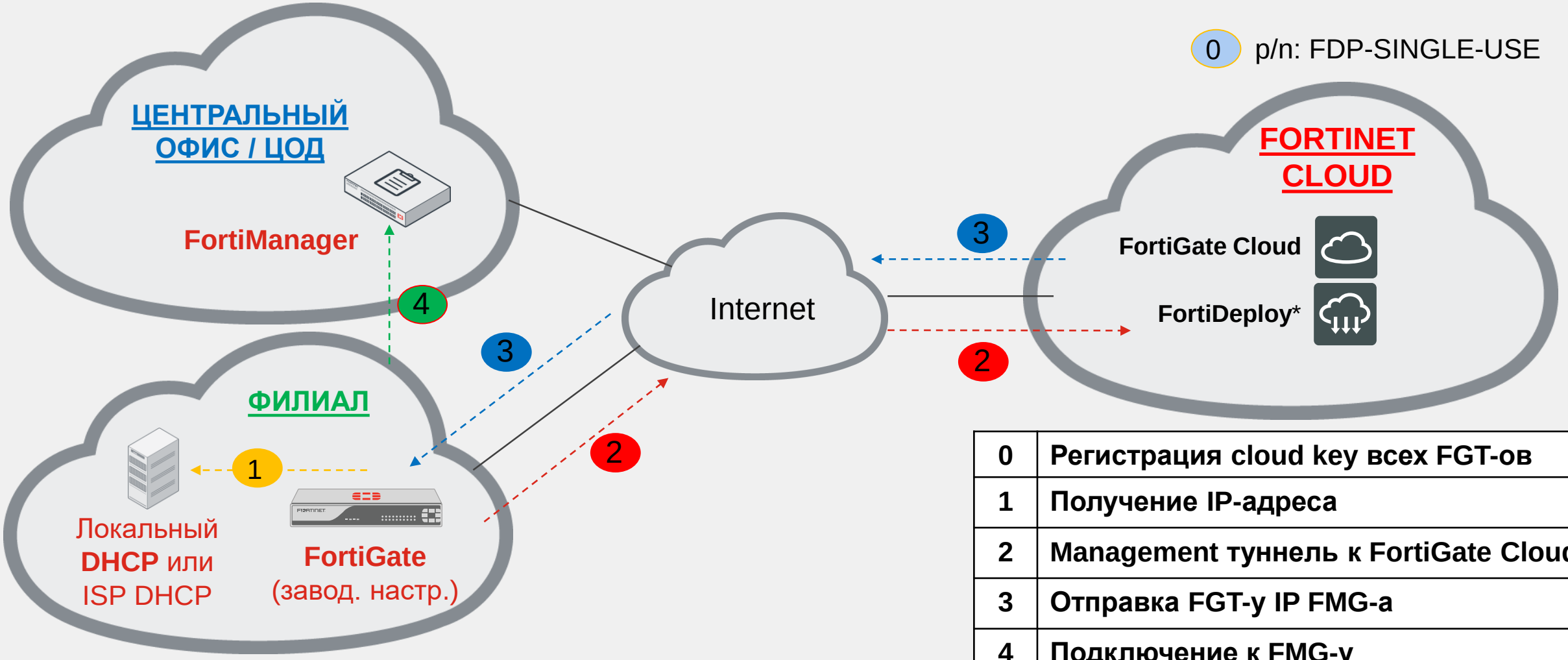
1 Сбор и корреляция логов	• Централизованная система сбора, корреляции и анализа журнальных файлов (логов)
2 Анализ логов и отчетность	• Анализ логов и построение всесторонних отчетов для понимания ситуации в сети
3 Генерация уведомлений	• Генерация уведомлений (events) в FAZ/email/SNMP/syslog, на основе определенных событий в логах (обработчики событий) для приоритизации и фокусировки на важных событиях
4 Выявление IOC и автоматизация	• Выявление в логах индикаторов компрометации и автоматизация реакции на выявленные угрозы (опционально)

© Fortinet Inc. All Rights Reserved.

Автоматическое развёртывание и начальное конфигурирование (ZTP)

Общая схема реализации Zero Touch Provisioning (ZTP)

Автоматическое развёртывание и начальное конфигурирование



0	Регистрация cloud key всех FGT-ов
1	Получение IP-адреса
2	Management туннель к FortiGate Cloud
3	Отправка FGT-у IP FMG-а
4	Подключение к FMG-у

*https://www.forticloud.com; https://europe.forticloud.com

* Вкл. FG-200

Независимые оценки

Лидер в области Network Firewall и Wan Edge

2020 Magic Quadrant for Network Firewalls

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)

2020 Magic Quadrant for WAN Edge Infrastructure

Figure 1. Magic Quadrant for WAN Edge Infrastructure

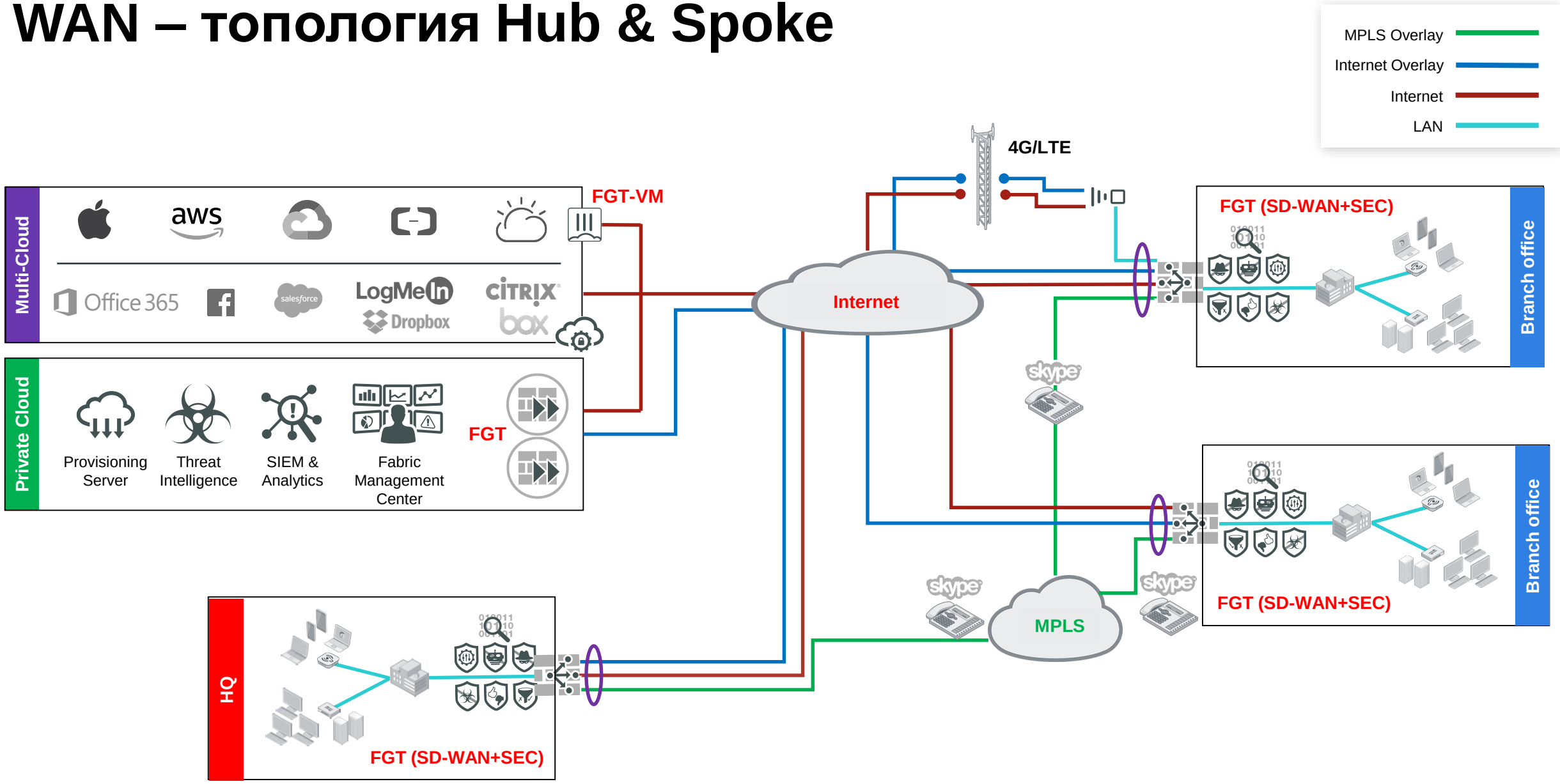


Source: Gartner (September 2020)

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.

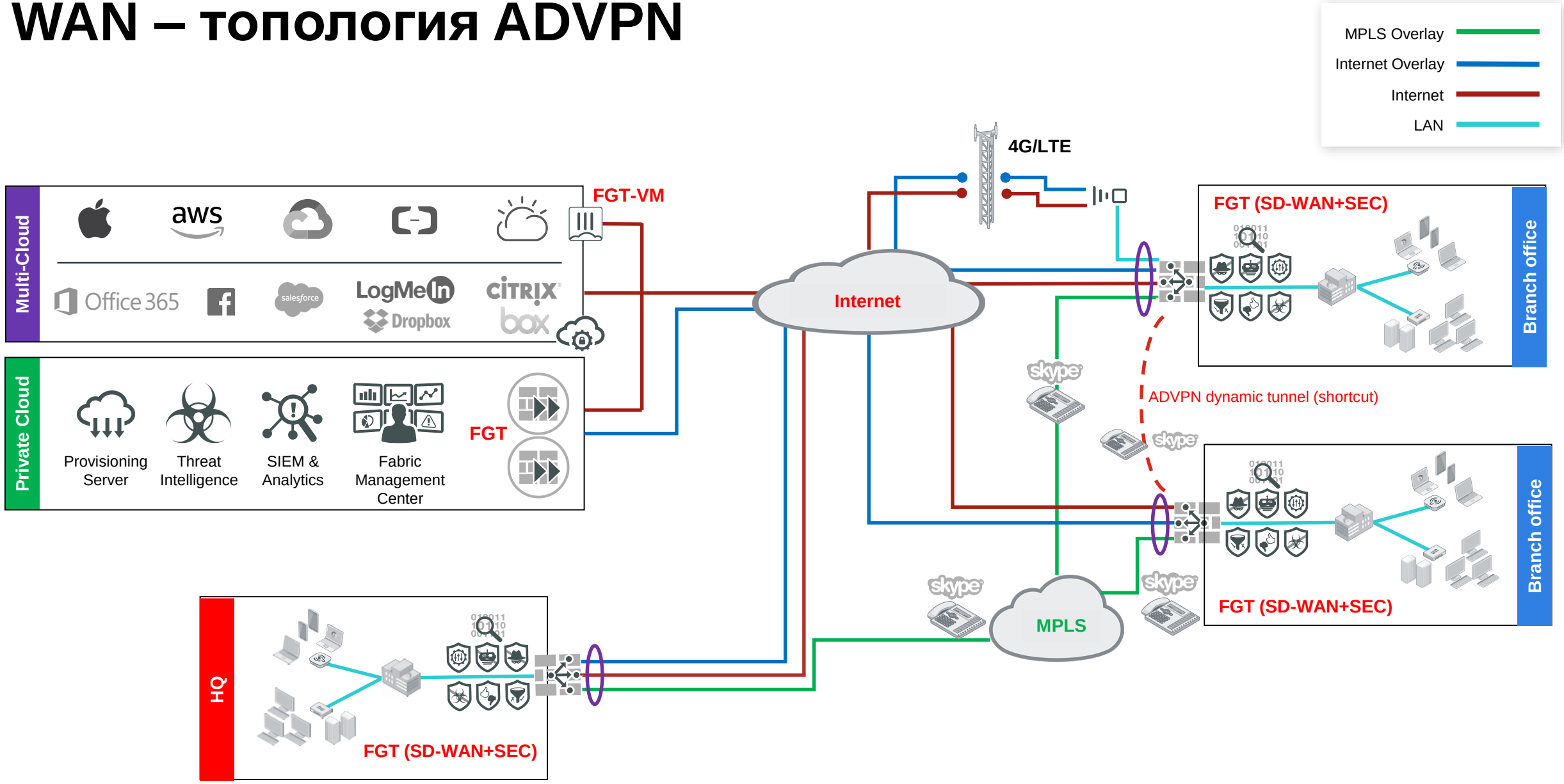
Варианты использования Secure SD-WAN

WAN – топология Hub & Spoke



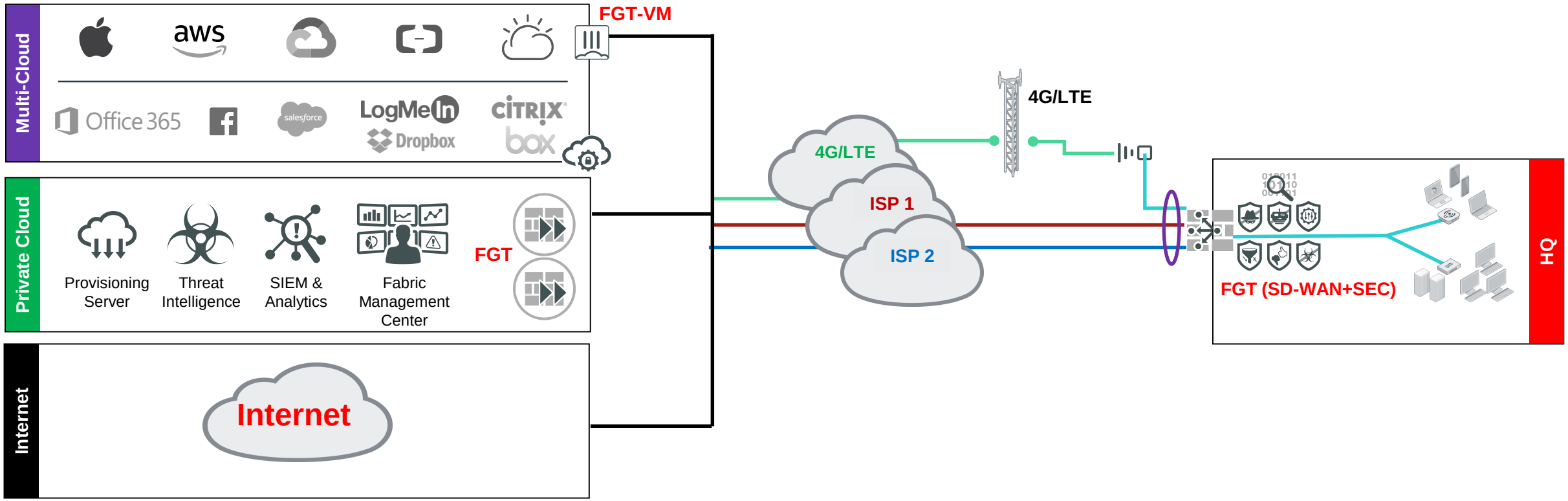
© Fortinet Inc. All Rights Reserved.

WAN – топология ADVPN



© Fortinet Inc. All Rights Reserved.

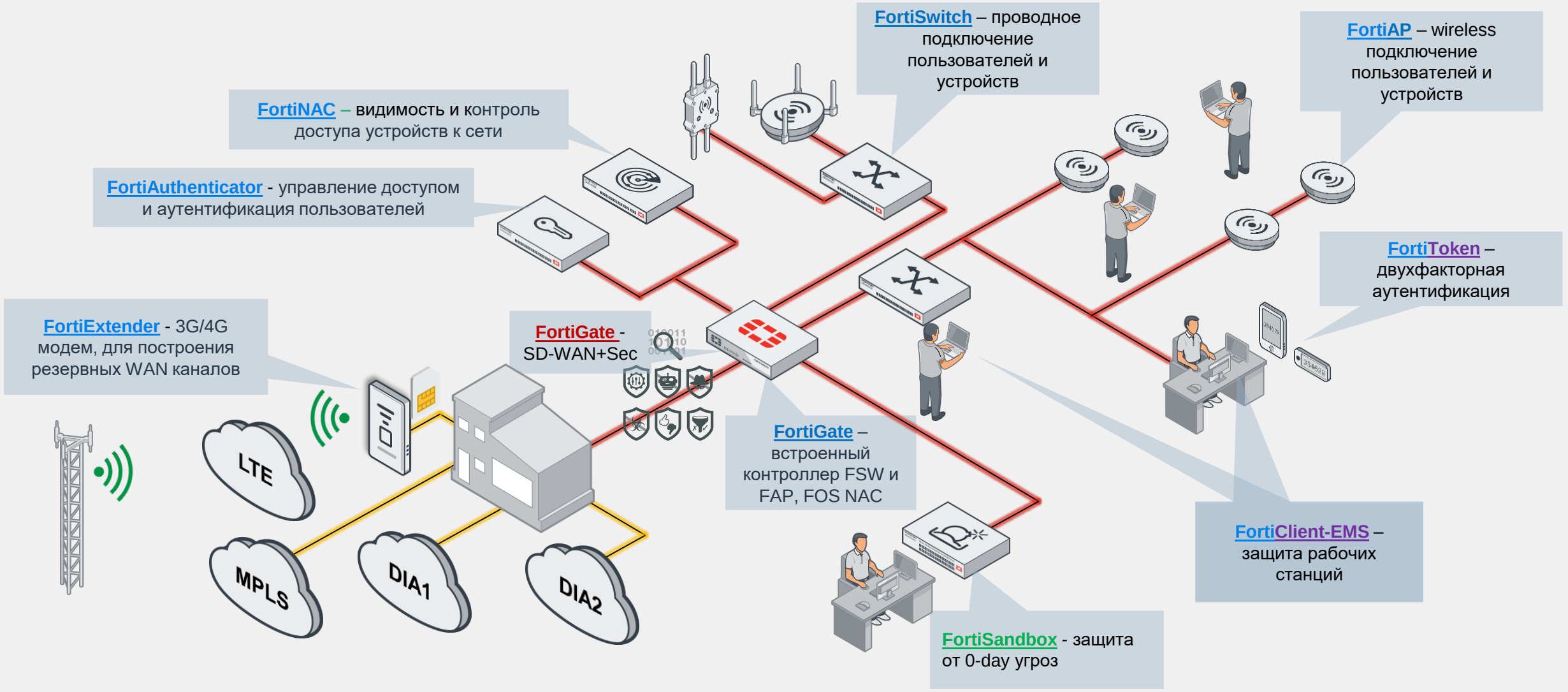
Центральный офис



© Fortinet Inc. All Rights Reserved.

Secure SD-Branch

Решение Secure SD-Branch



© Fortinet Inc. All Rights Reserved.

Преимущества Secure SD-Branch

1 **Безопасность**

- Интегрированная всесторонняя безопасность от WAN Edge до рабочей станции

2 **Простота и функциональность**

- Гибкая **интеграции** Sec, WAN, LAN + доп. системы (видимость, автоматизация)
- **Единая система управления** FMC (FMG+FAZ) для Sec, WAN, LAN
- Широкий функционал
- Масштабируемая архитектура

3 **Снижение совокупной стоимости владения**

- Меньше устройств, лицензий, сервисов тех. поддержки
- Простое внедрение (ztp распространяется и на FSW, FAP)

© Fortinet Inc. All Rights Reserved.

Заключение

Защищённый SD-WAN и SD-Branch от Fortinet

Преимущества для Вас

1. **Улучшение производительности приложений (повышение удовлетворенности пользователей)**
2. **Обеспечение безопасного доступа в Internet / Public Cloud**
3. **Упрощение дизайна WAN**
4. **Упрощение управления и внедрения**
5. **Экономия затрат (OpEx, CapEx) и гибкость подключения**
6. **Интеграция с LAN инфраструктурой (Secure SD-Branch)**

© Fortinet Inc. All Rights Reserved.


FORTINET