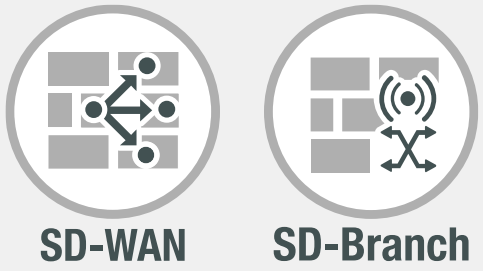
Защищённый SD-WAN и SD-Branch от Fortinet

Максим Порицкий
системный инженер

cis_se@fortinet.com (инженерная команда)



Содержание

Традиционная WAN vs Secure SD-WAN

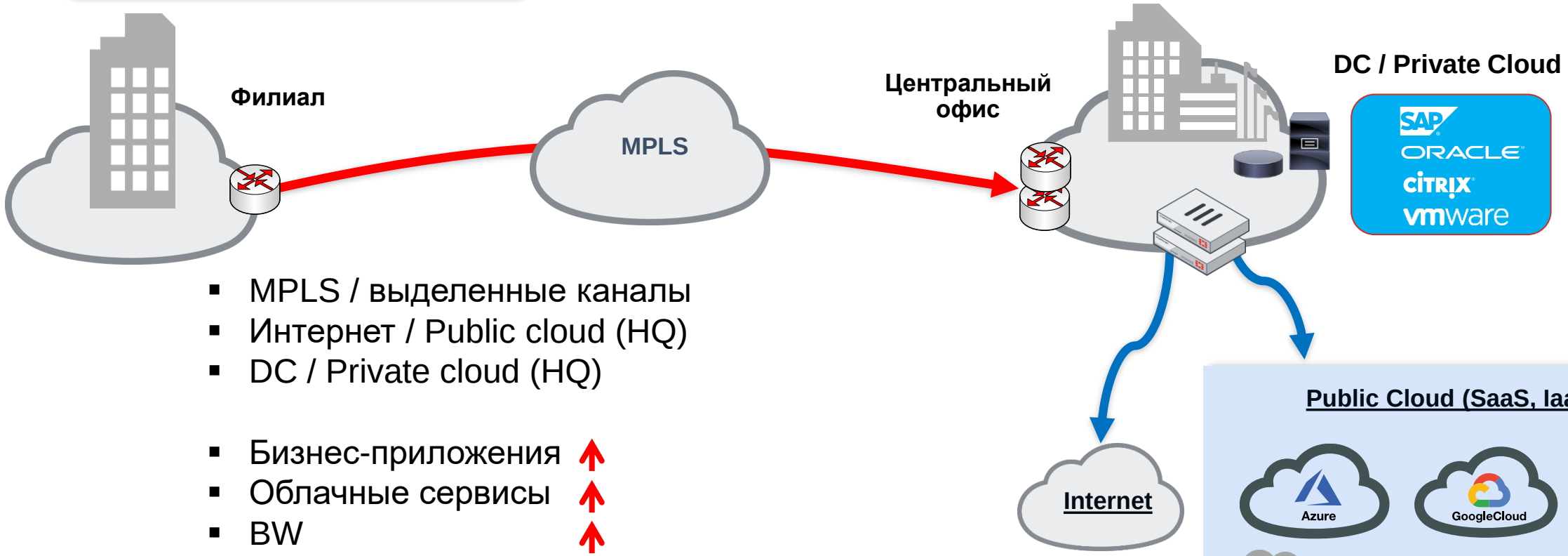
Традиционная WAN

Какие проблемы заставляют задуматься о модернизации WAN

1. MPLS / выделенные каналы - дорогие каналы связи

2. Загрузка каналов связи - весь трафик маршрутизируется в HQ и инспектируется в HQ

3. Маршрутизация / балансировка 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 ↑

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 Insp.) при доступе в Internet и Public Cloud из филиала / центрального офиса (backup)

3 **Упрощение дизайна WAN**

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

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**

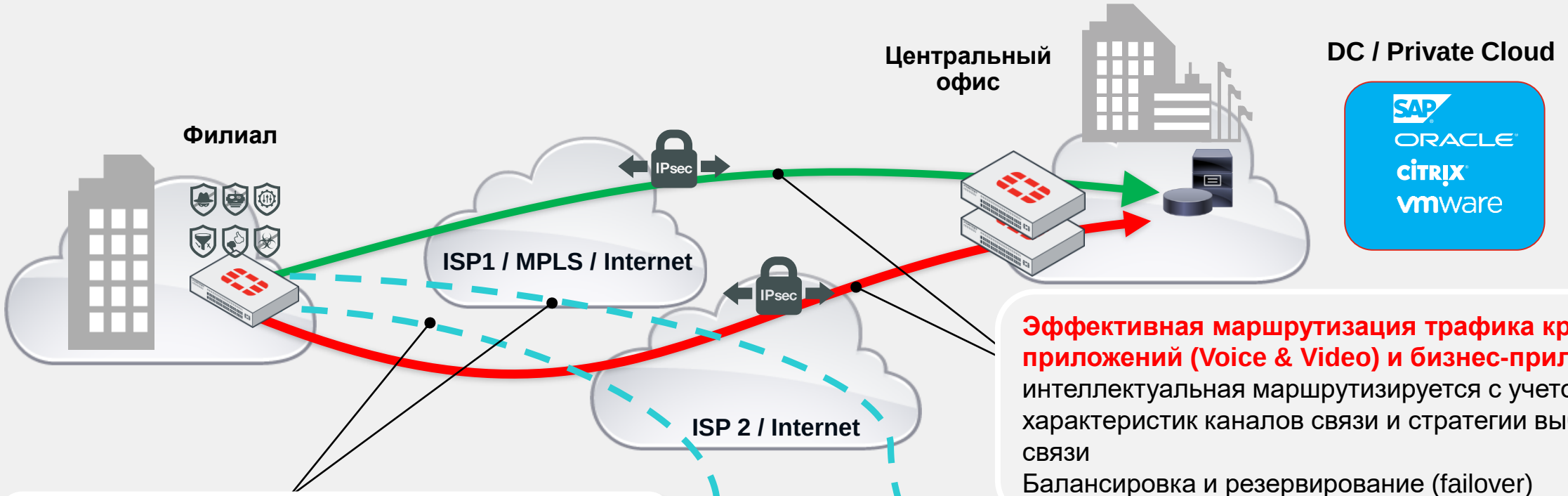
5 **Экономия затрат (OpEx, CapEx) и гибкость подключения**

- **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)**

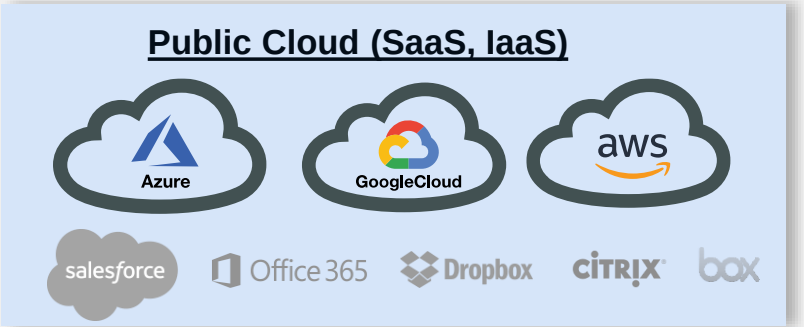
- Интегрированный **контроллер коммутаторов и ТД** (управление, конфигурация и мониторинг), FOS NAC
- **Интеграция** с другими продуктами - FNAC, FSA, FAC
- **Безопасность пользовательских устройств** (FCL-EMS)
- **2FA**

Реализация WAN с использованием Secure SD-WAN



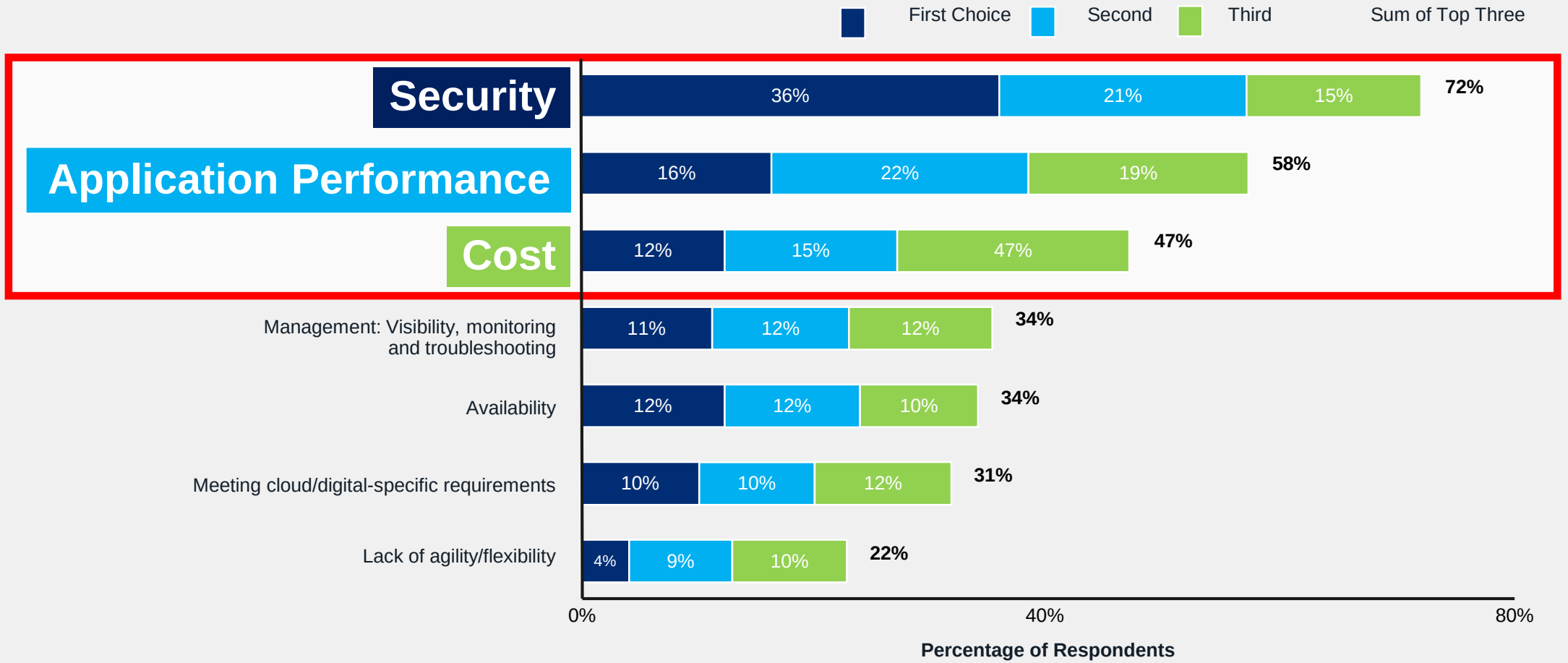
Эффективная маршрутизация трафика критичных приложений (Voice & Video) и бизнес-приложений
интеллектуальная маршрутизируется с учетом характеристик каналов связи и стратегии выбора каналов связи
Балансировка и резервирование (failover)

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

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)

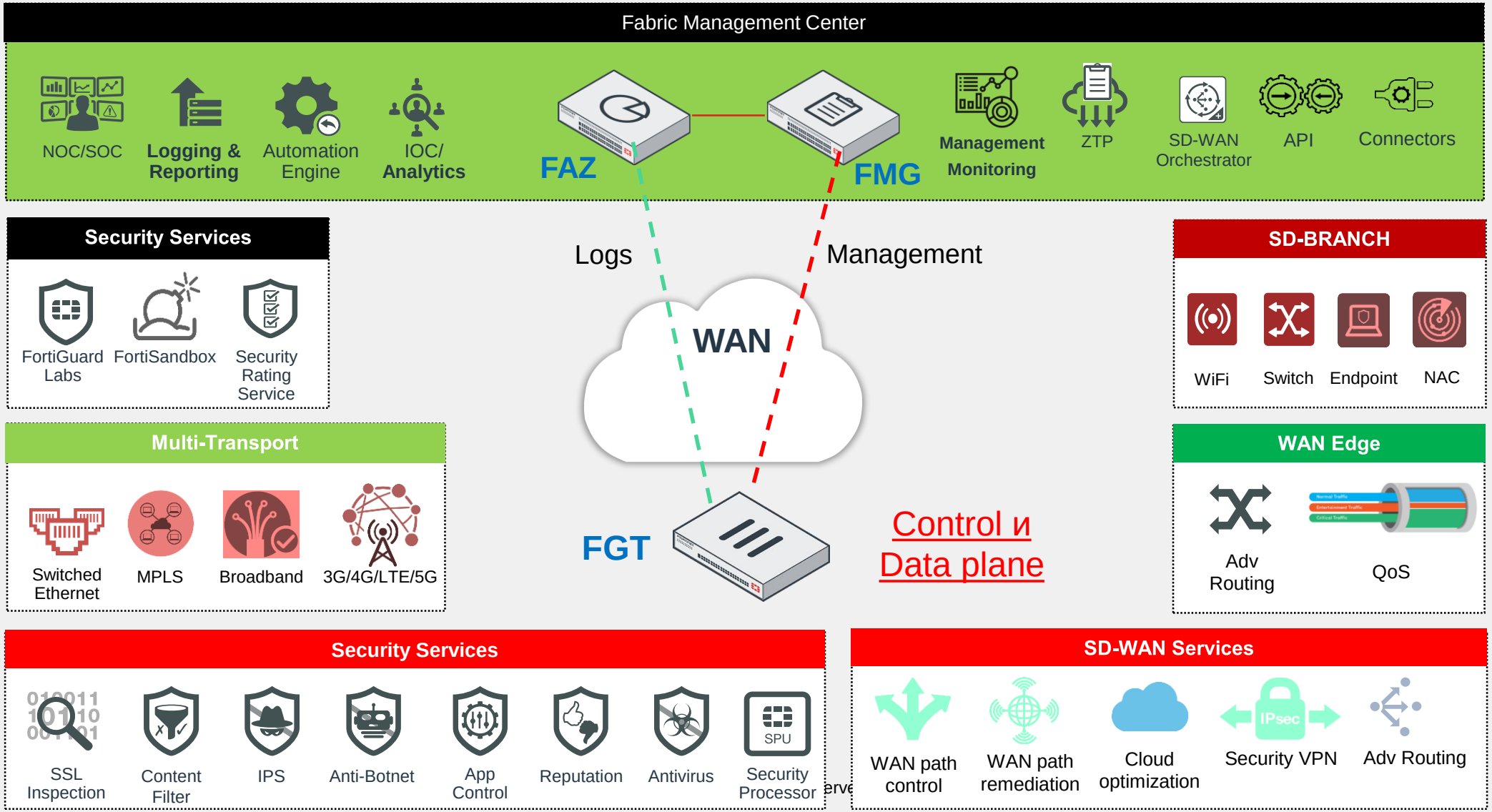
4  **FortiGate Cloud** – облачная централизованная система управления и мониторинга

FortiDeploy – компонент ZTP в составе FortiGateCloud

Архитектура Secure SD-WAN

Архитектура Fortinet Secure SD-WAN (Controllerless)

Orchestration и Management plane

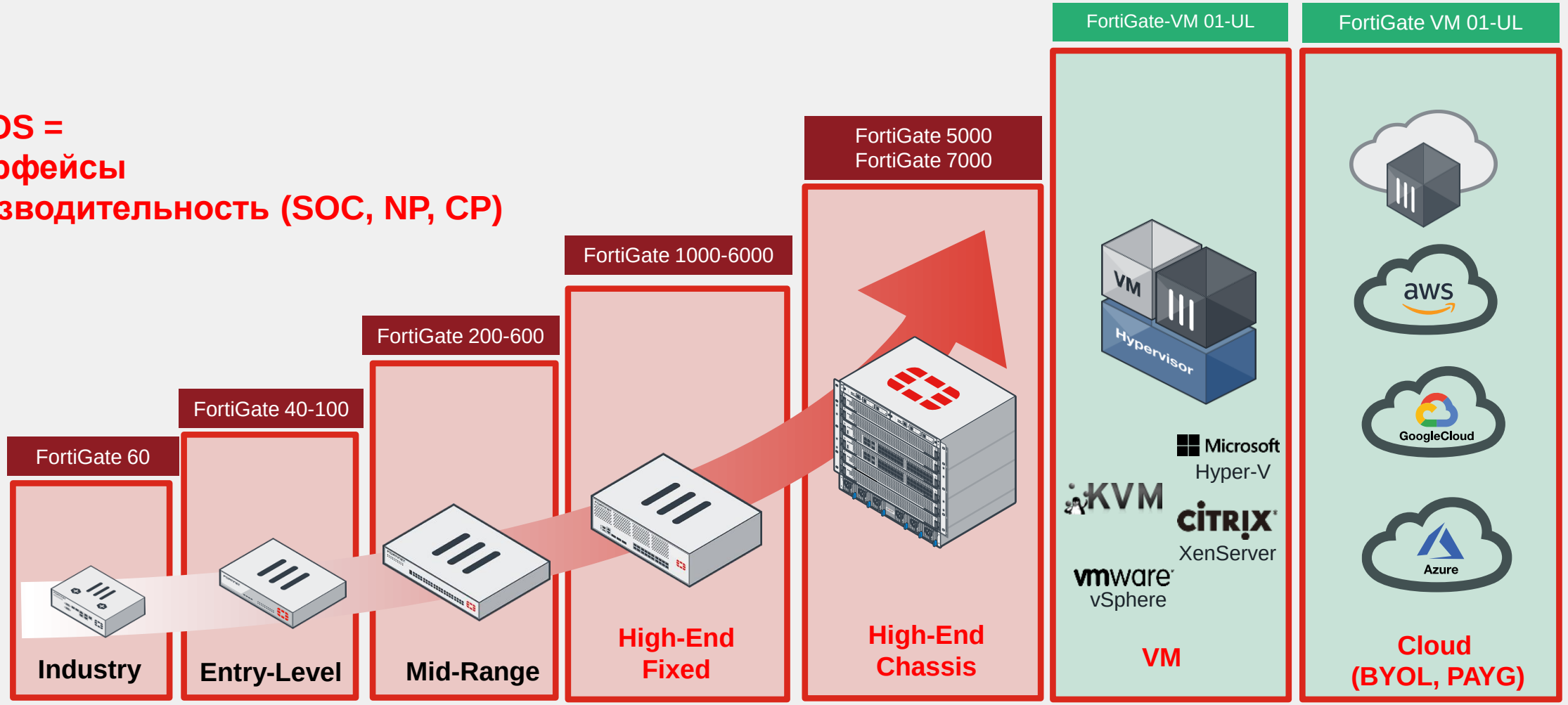


FortiGate

FortiGate – модельный ряд*

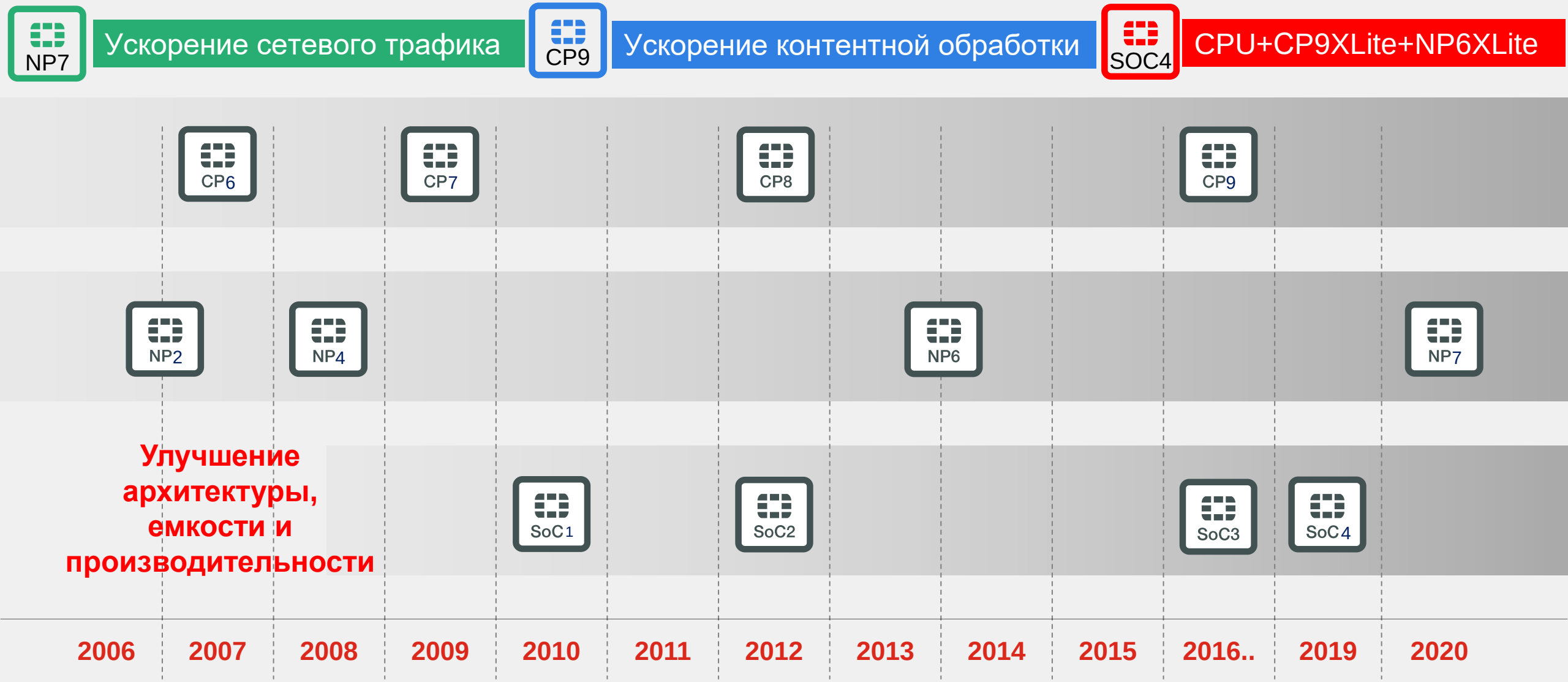
От небольших филиалов до крупных ЦОД

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)

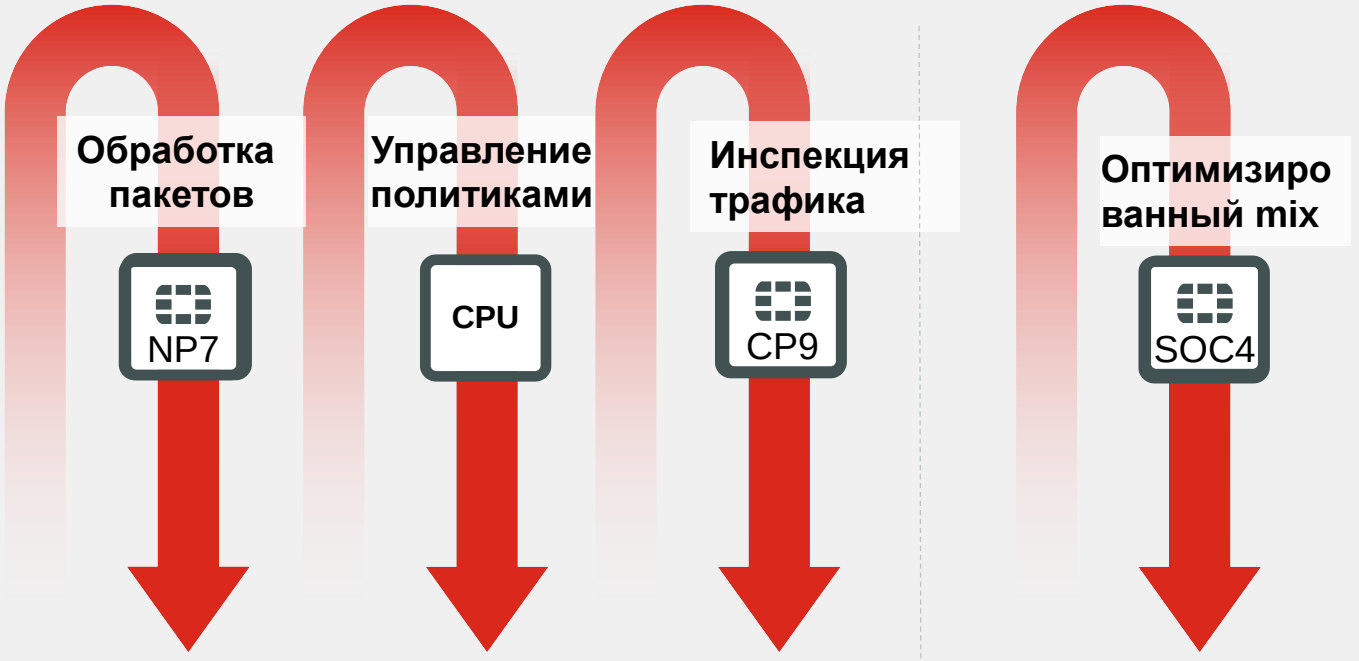


Преимущества использования SPU

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

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

Функционал SD-WAN FGT

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

- Идентификация приложений (FortiGuard, 5000+)
- Мониторинг характеристик каналов связи + SLA targets
- Динамический выбор канала на основе правил и стратегий
- 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 (на основе)**

- Пользовательских групп (User Identity Based)
- Подсетей, протоколов, портов
- Типов приложений / ISDB
- Custom application / ISDB

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**

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

FortiAnalyzer

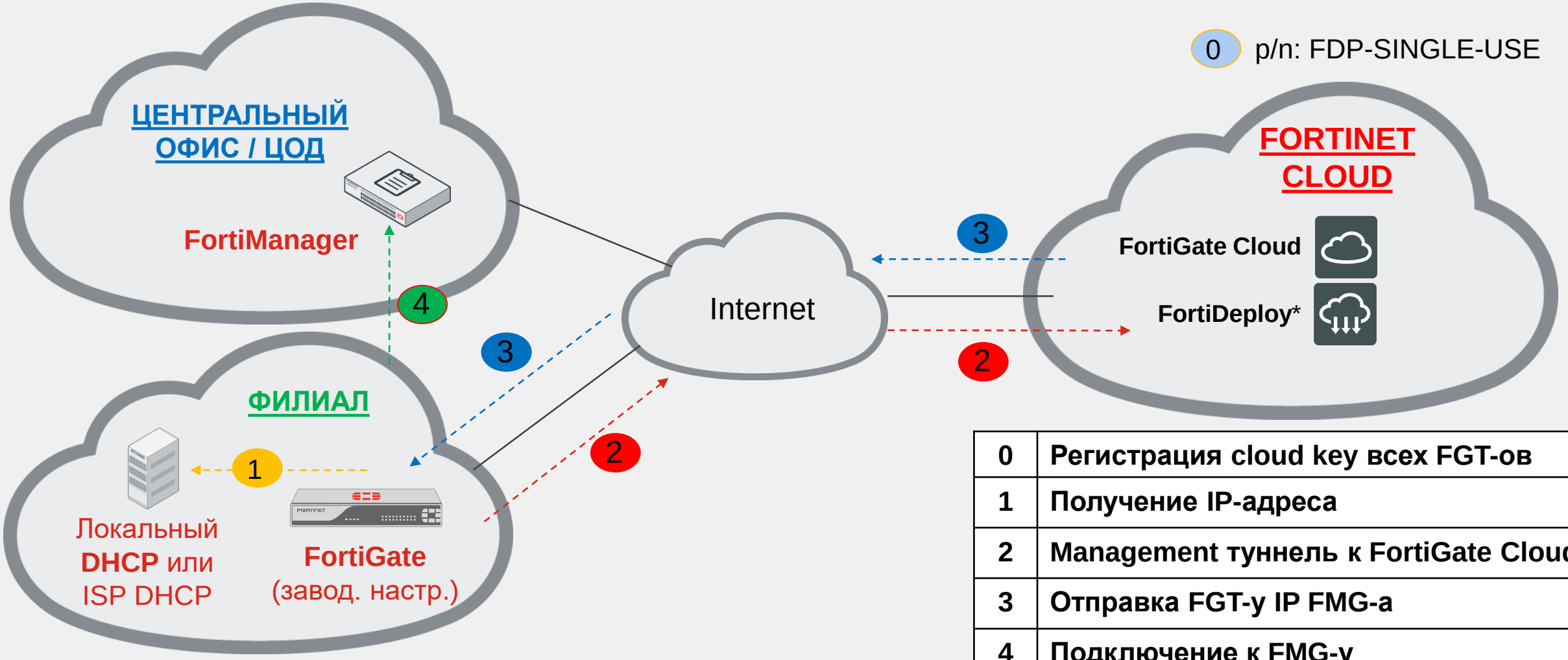
FortiAnalyzer

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)

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

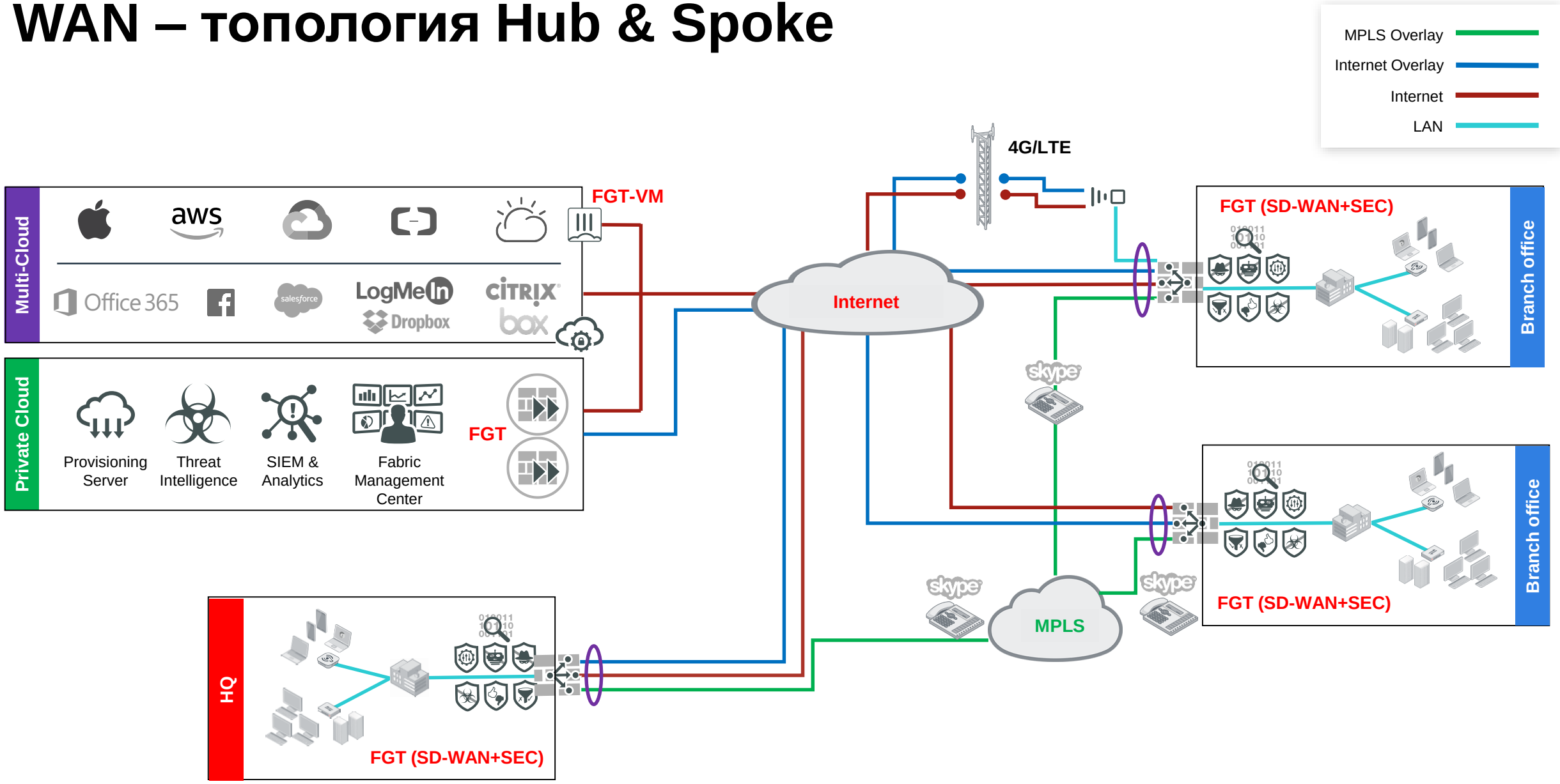
Source: Gartner (November 2020)

2021 Magic Quadrant for WAN Edge Infrastructure

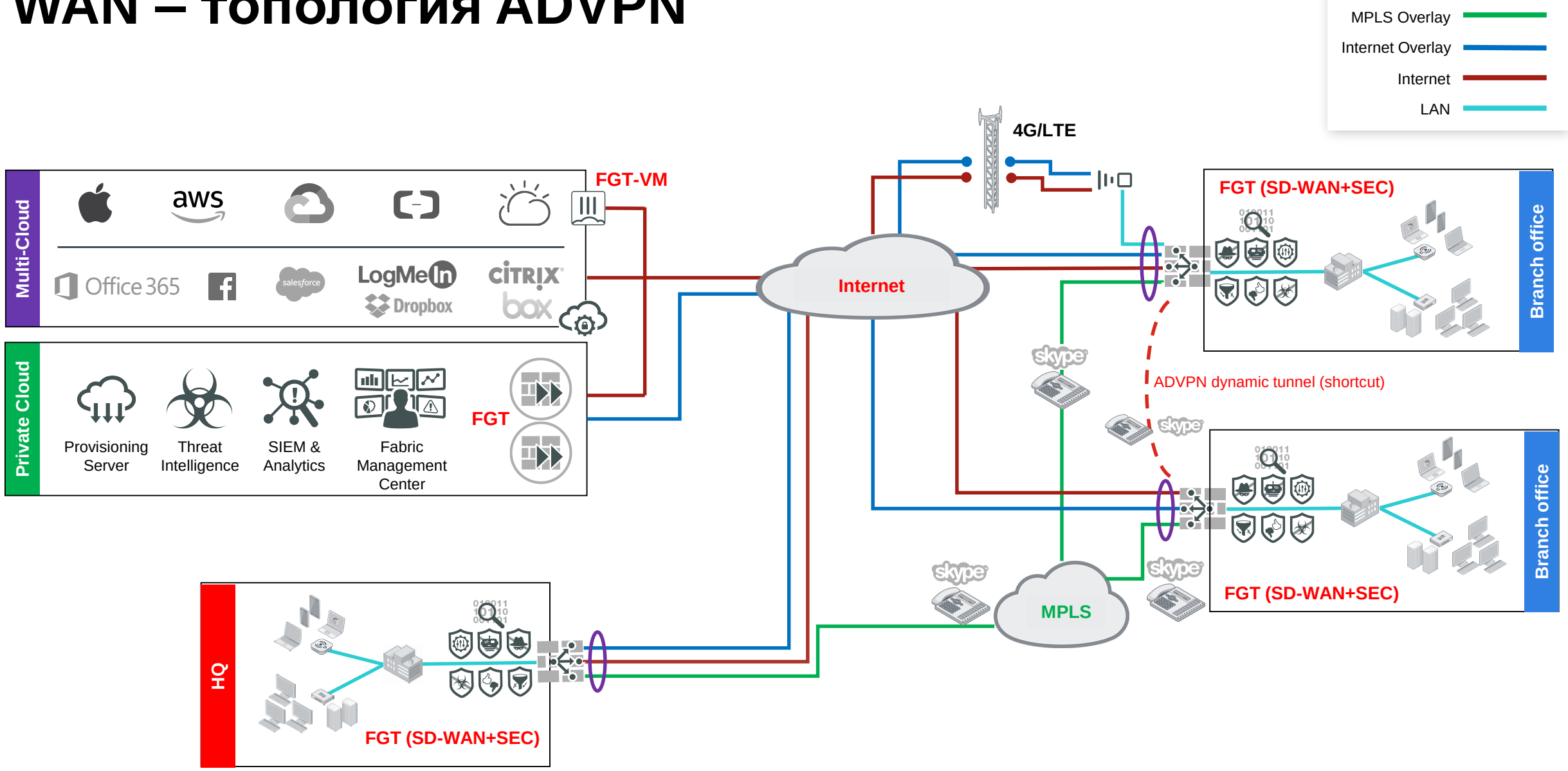
Figure 1: Magic Quadrant for WAN Edge Infrastructure

Варианты использования Secure SD-WAN

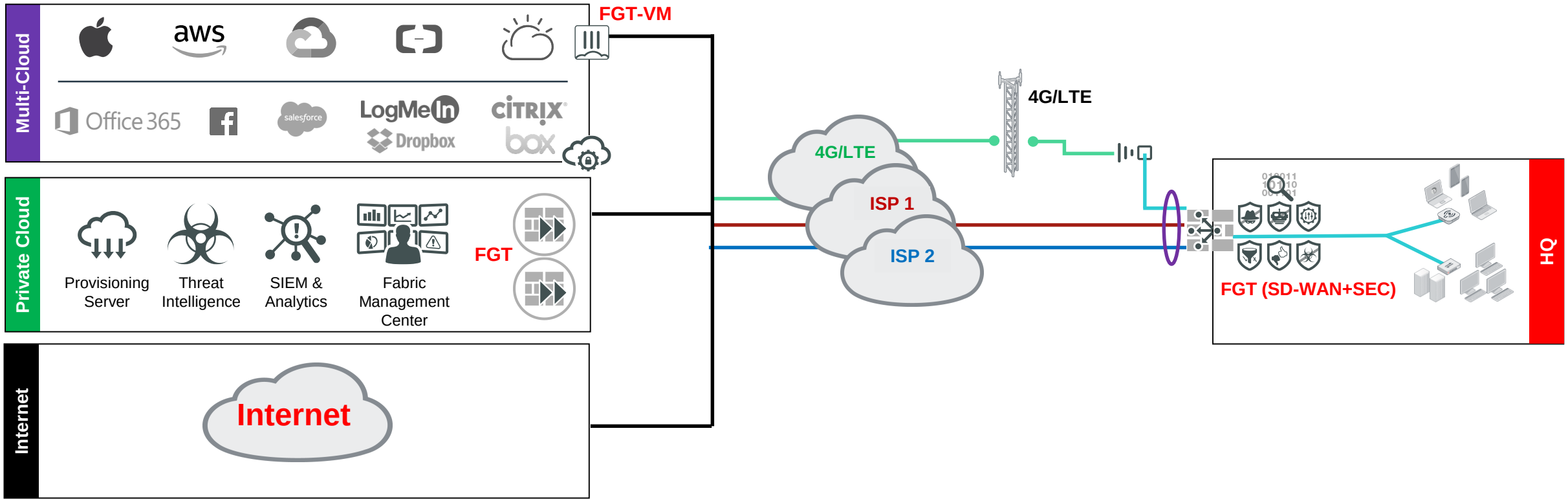
WAN – топология Hub & Spoke



WAN – топология ADVPN

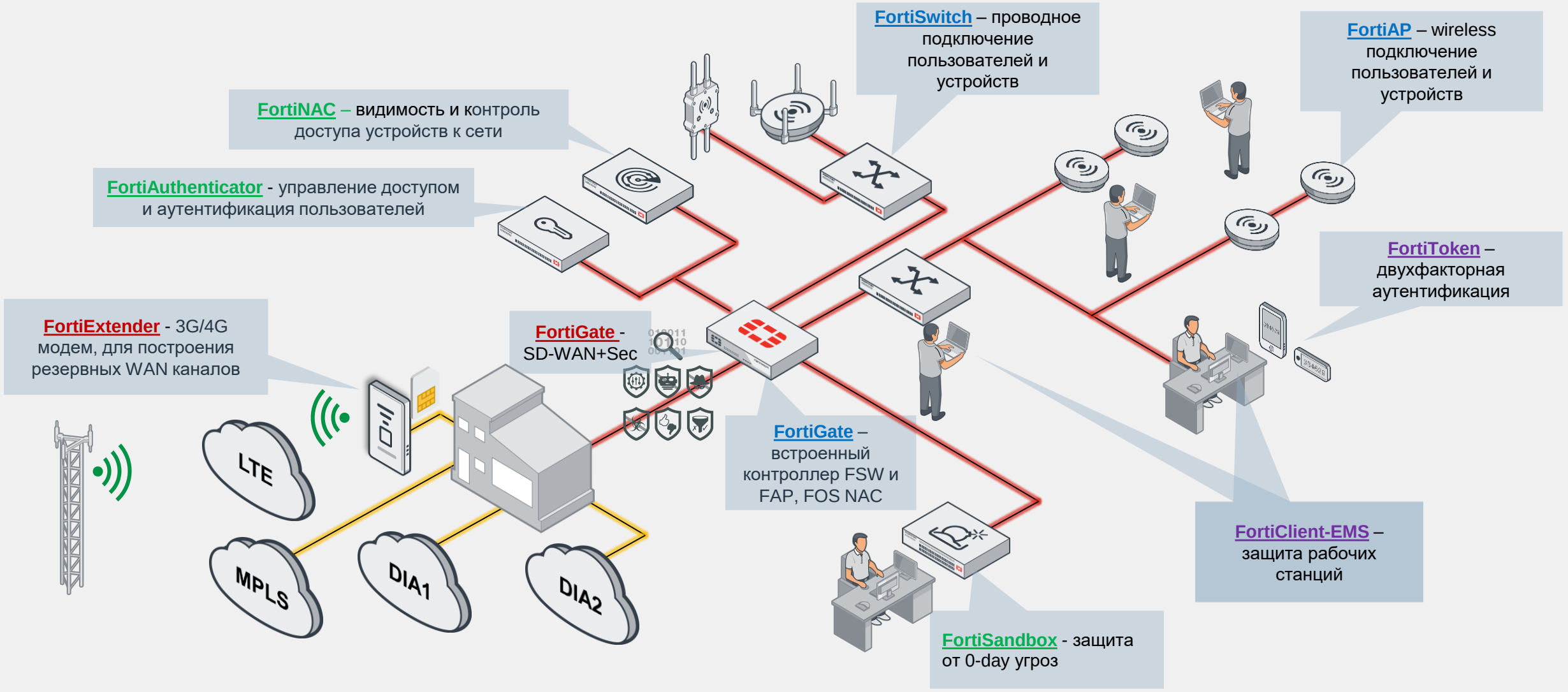


Центральный офис



Secure SD-Branch

Решение Secure SD-Branch



Преимущества Secure SD-Branch

1 **Безопасность**

- Интегрированная всесторонняя безопасность от WAN Edge до рабочей станции

2 **Простота и функциональность**

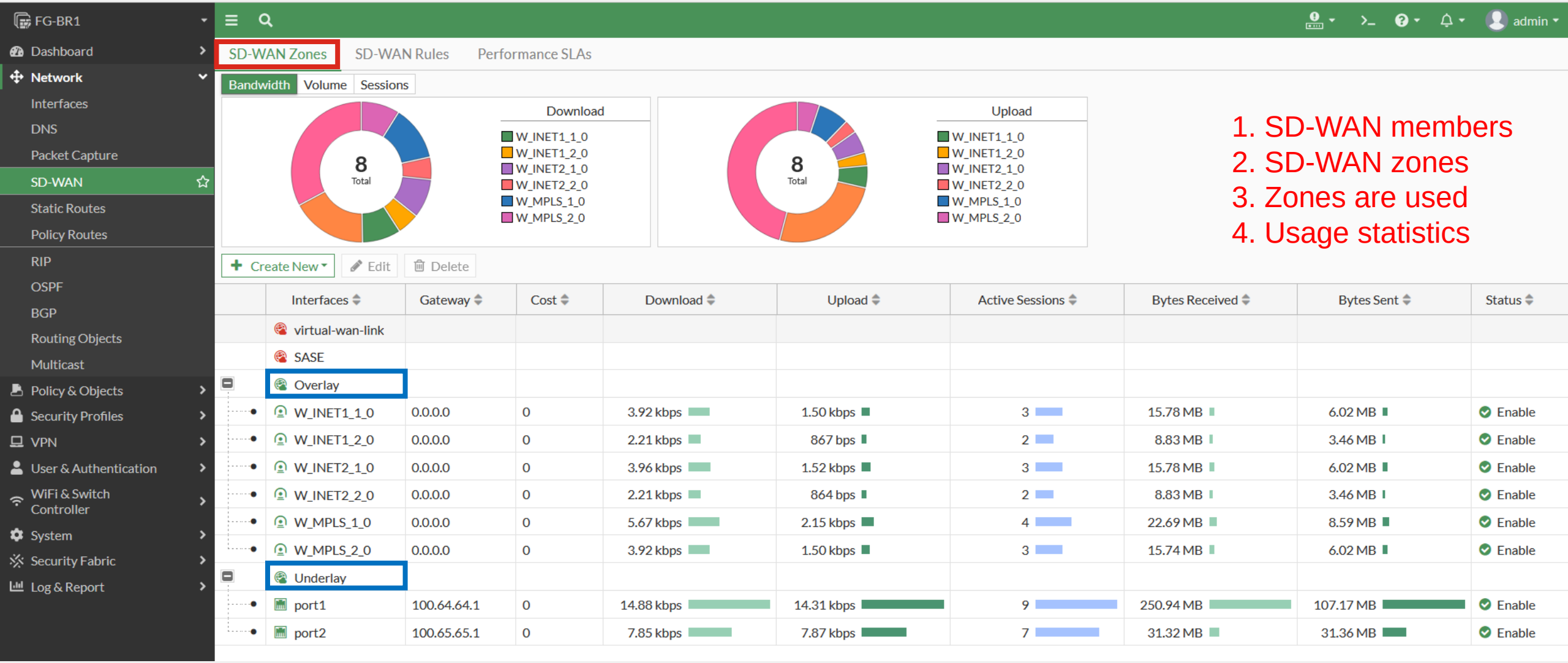
- Гибкая **интеграции** Sec, WAN, LAN + доп. системы (видимость, автоматизация)
- **Единая система управления** FMC (FMG+FAZ) для Sec, WAN, LAN
- Широкий функционал
- Масштабируемая архитектура

3 **Снижение совокупной стоимости владения**

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

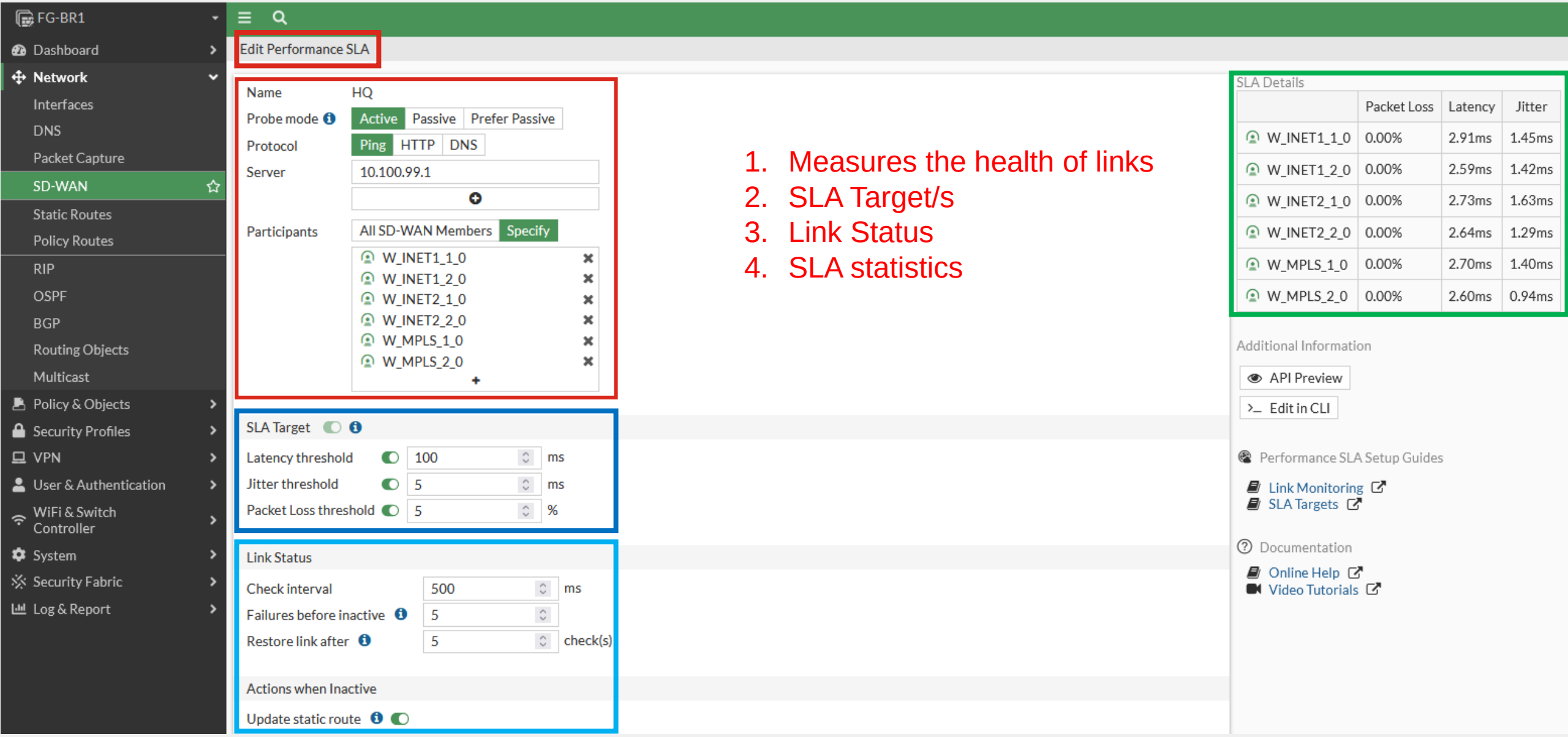
Базовые настройки SD-WAN

SD-WAN Zones



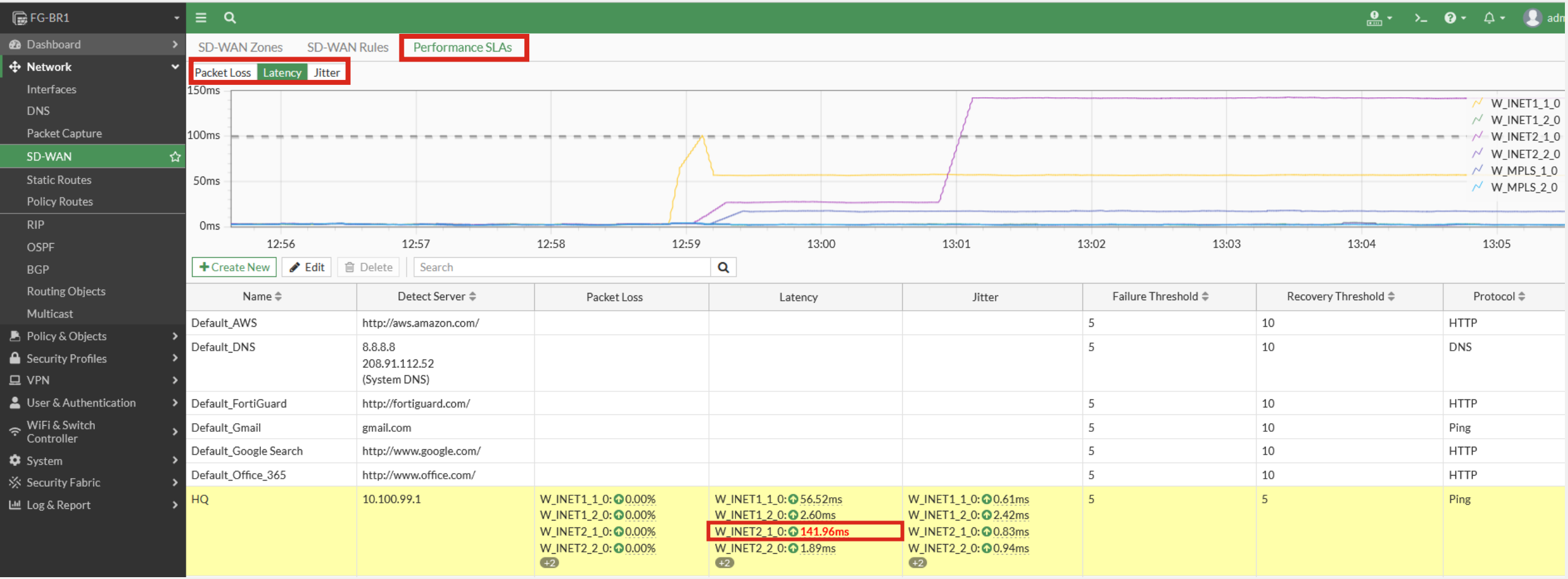
1. SD-WAN members
2. SD-WAN zones
3. Zones are used
4. Usage statistics

SD-WAN Performance SLA - link health monitoring

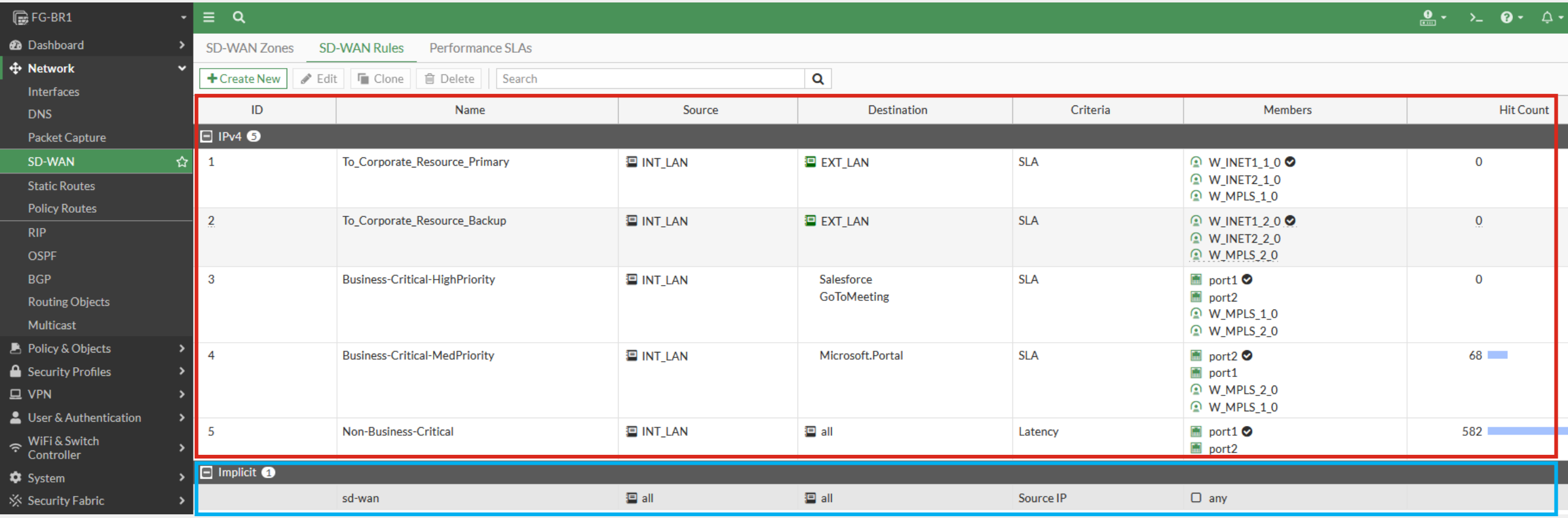


SD-WAN Performance SLA - link health monitoring

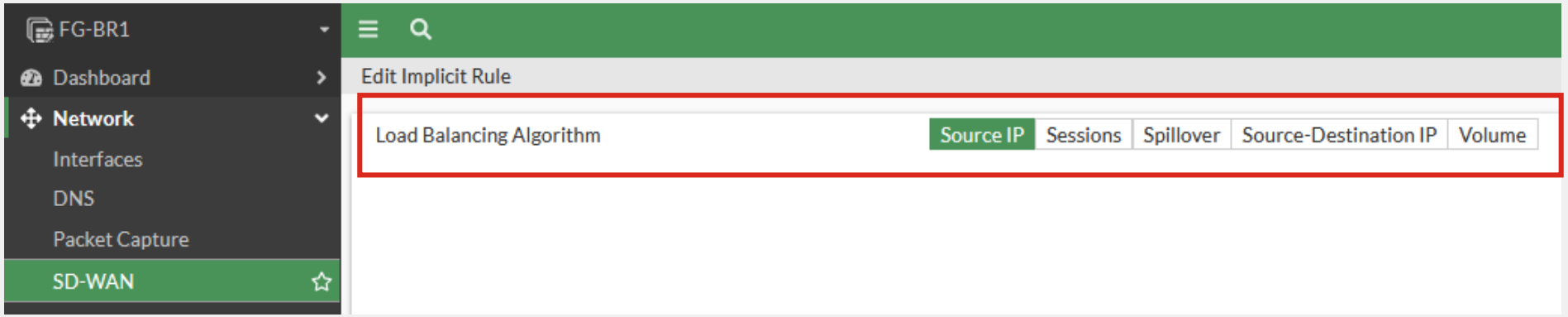
1. Визуальное и табличное отображение характеристик
2. DSCP в тестовых пакетах (CLI)
3. SNMP, RESP API
4. Logs (local), FAZ



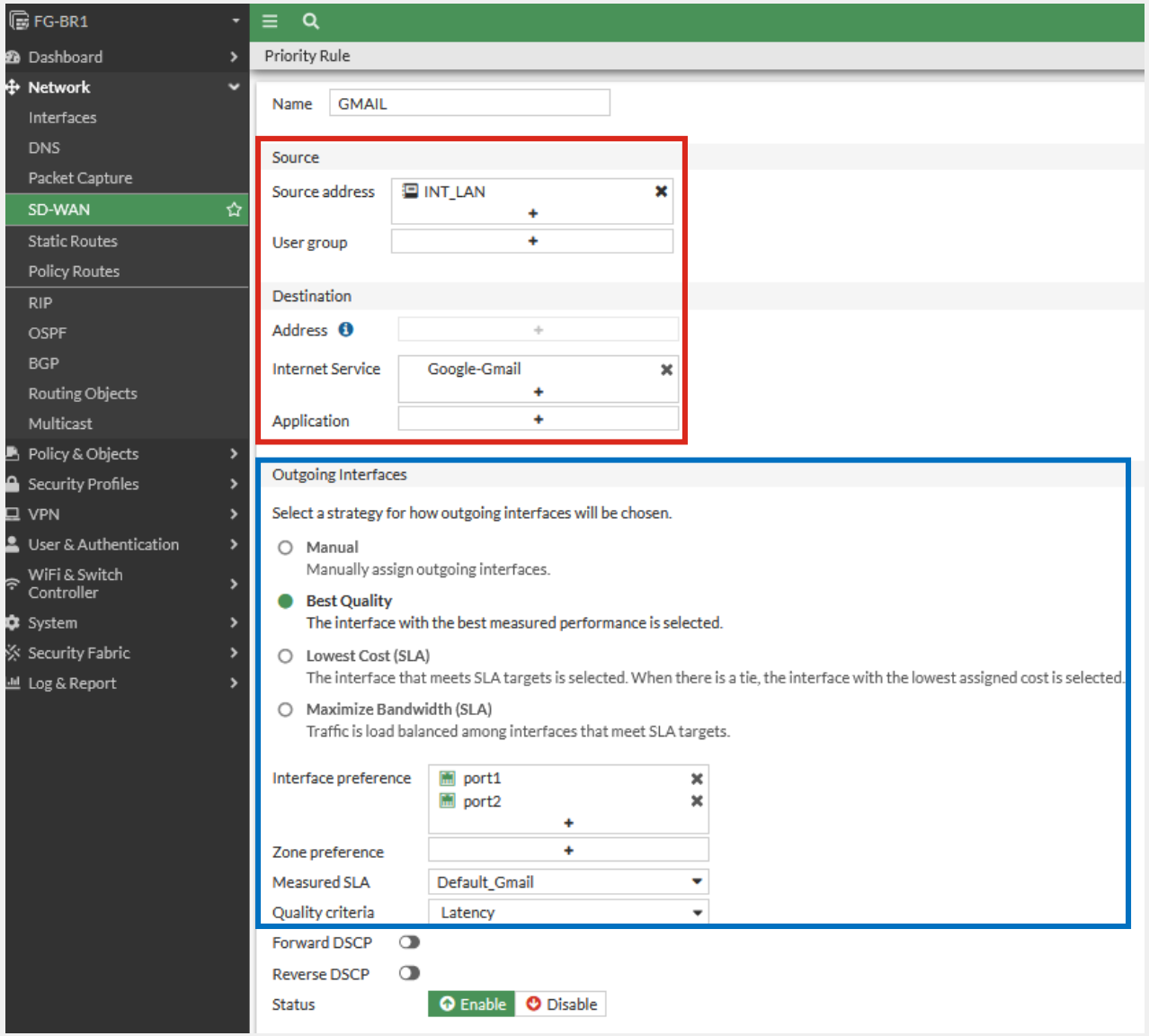
SD-WAN Rules


FG-BR1
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
SD-WAN Zones
SD-WAN Rules
Performance SLAs
Create New
Edit
Clone
Delete
Search
ID
Name
Source
Destination
Criteria
Members
Hit Count
IPv4 5
1
To_Corporate_Resource_Primary
INT_LAN
EXT_LAN
SLA
W_INET1_1_0
W_INET2_1_0
W_MPLS_1_0
0
2
To_Corporate_Resource_Backup
INT_LAN
EXT_LAN
SLA
W_INET1_2_0
W_INET2_2_0
W_MPLS_2_0
0
3
Business-Critical-HighPriority
INT_LAN
Salesforce
GoToMeeting
SLA
port1
port2
W_MPLS_1_0
W_MPLS_2_0
0
4
Business-Critical-MedPriority
INT_LAN
Microsoft.Portal
SLA
port2
port1
W_MPLS_2_0
W_MPLS_1_0
68
5
Non-Business-Critical
INT_LAN
all
Latency
port1
port2
582
Implicit 1
sd-wan
all
all
Source IP
any

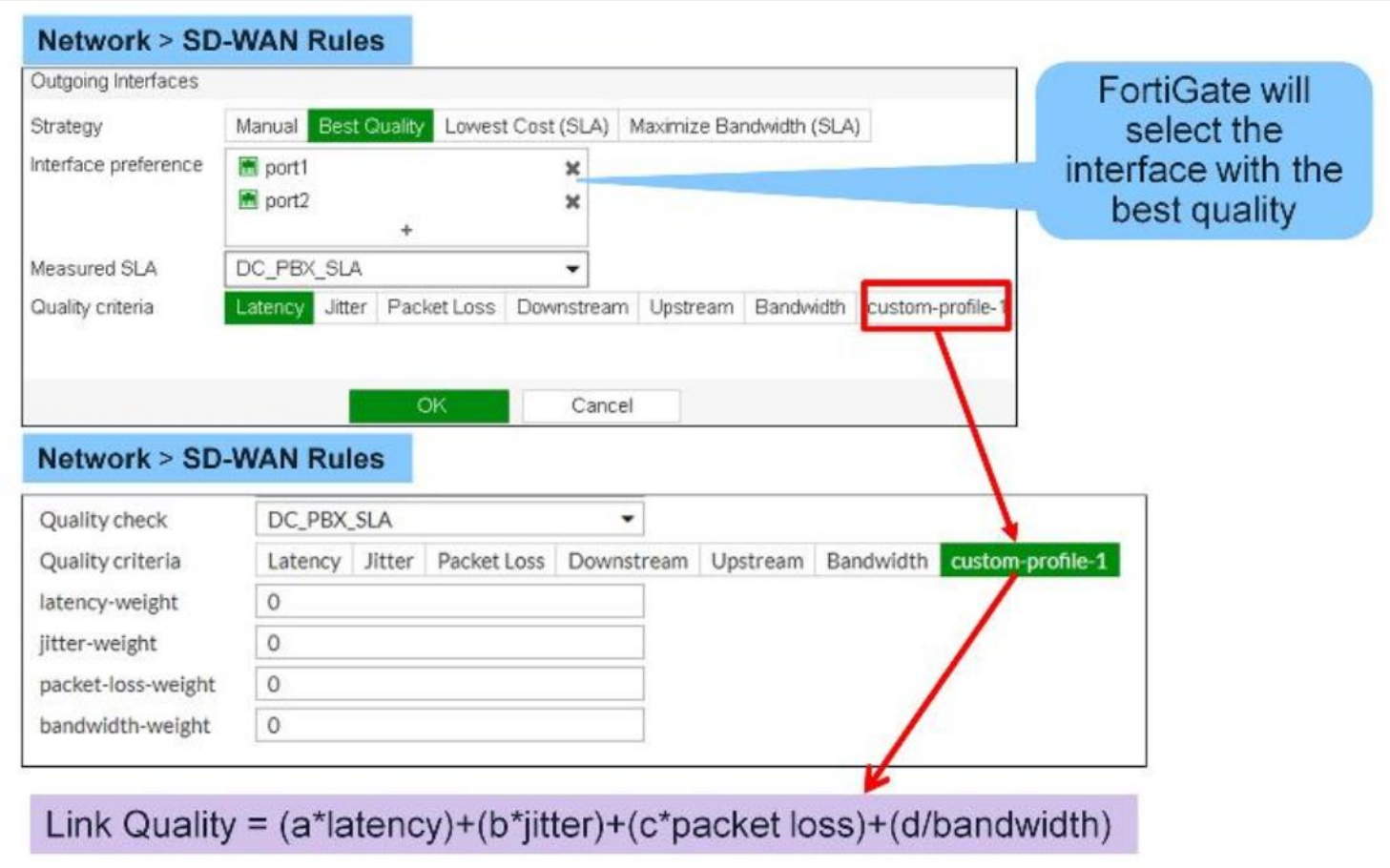
SD-WAN Rules – Implicit Rule



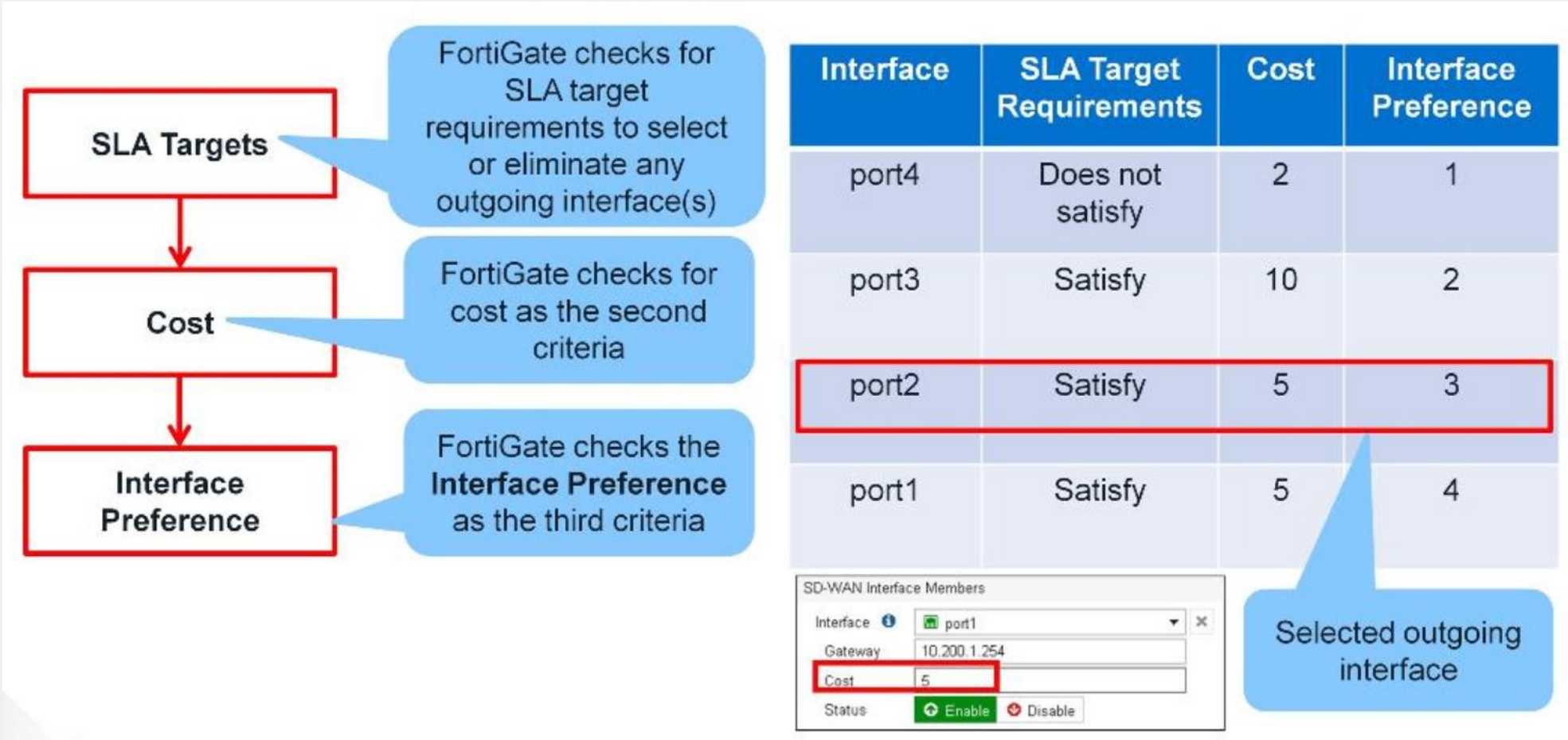
SD-WAN Rules


FG-BR1
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
Priority Rule
Name
GMAIL
Source
Source address
INT_LAN
User group
Destination
Address
Internet Service
Google-Gmail
Application
Outgoing Interfaces
Select a strategy for how outgoing interfaces will be chosen.
Manual
Manually assign outgoing interfaces.
Best Quality
The interface with the best measured performance is selected.
Lowest Cost (SLA)
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.
Maximize Bandwidth (SLA)
Traffic is load balanced among interfaces that meet SLA targets.
Interface preference
port1
port2
Zone preference
Measured SLA
Default_Gmail
Quality criteria
Latency
Forward DSCP
Reverse DSCP
Status
Enable
Disable

Стратегия Best Quality

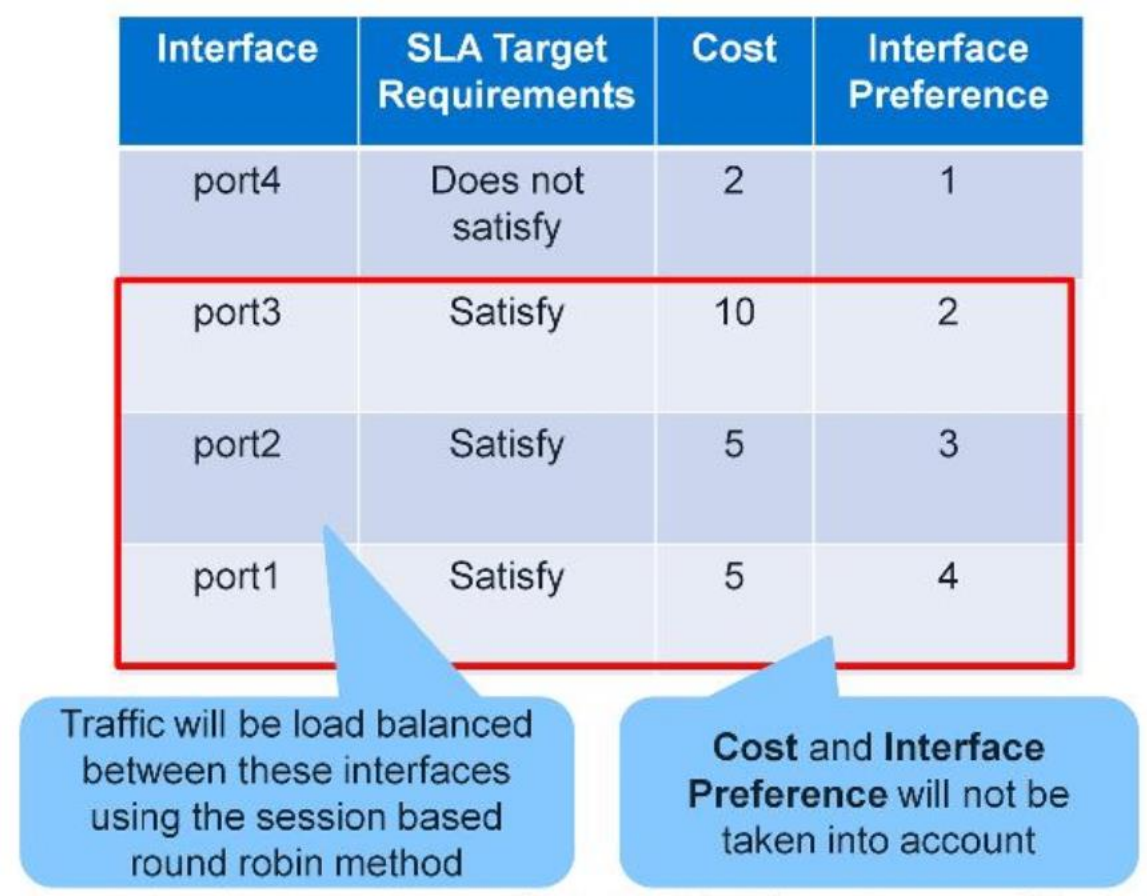


Стратегия Lowest cost

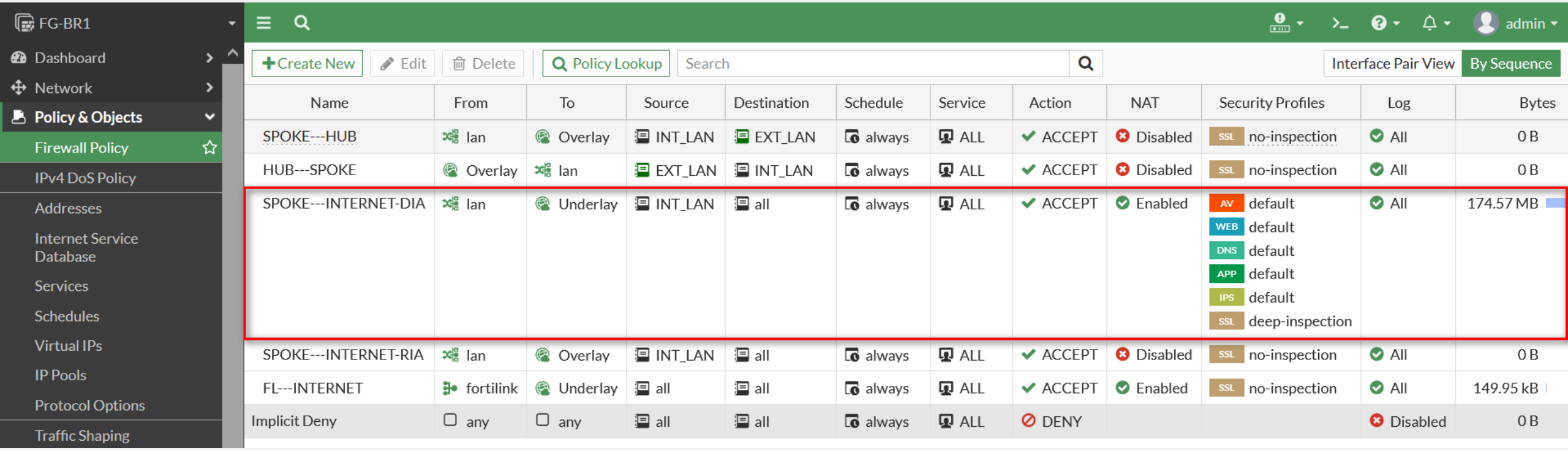


Interface	SLA Target Requirements	Cost	Interface Preference
port4	Does not satisfy	2	1
port3	Satisfy	10	2
port2	Satisfy	5	3
port1	Satisfy	5	4

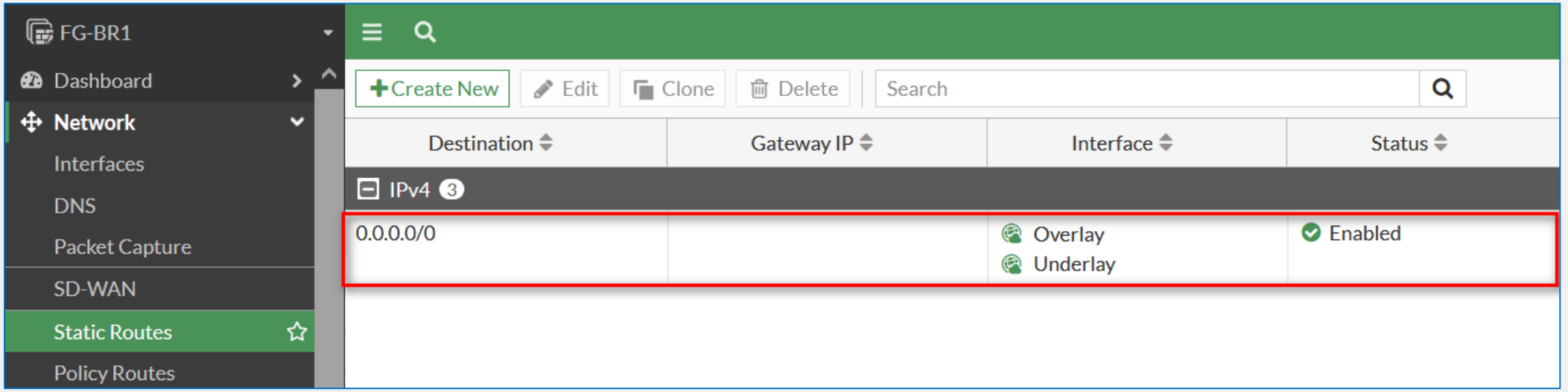
Стратегия Maximize Bandwidth



Firewall Policy



Routing



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