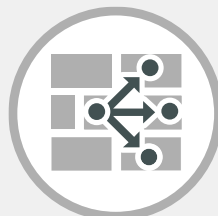




Защищённый SD-WAN и SD-Branch от Fortinet

Максим Порицкий
системный инженер

cis_se@fortinet.com (инженерная команда)



SD-WAN



SD-Branch

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

6

Базовые настройки SD-WAN



Традиционная WAN vs Secure SD-WAN



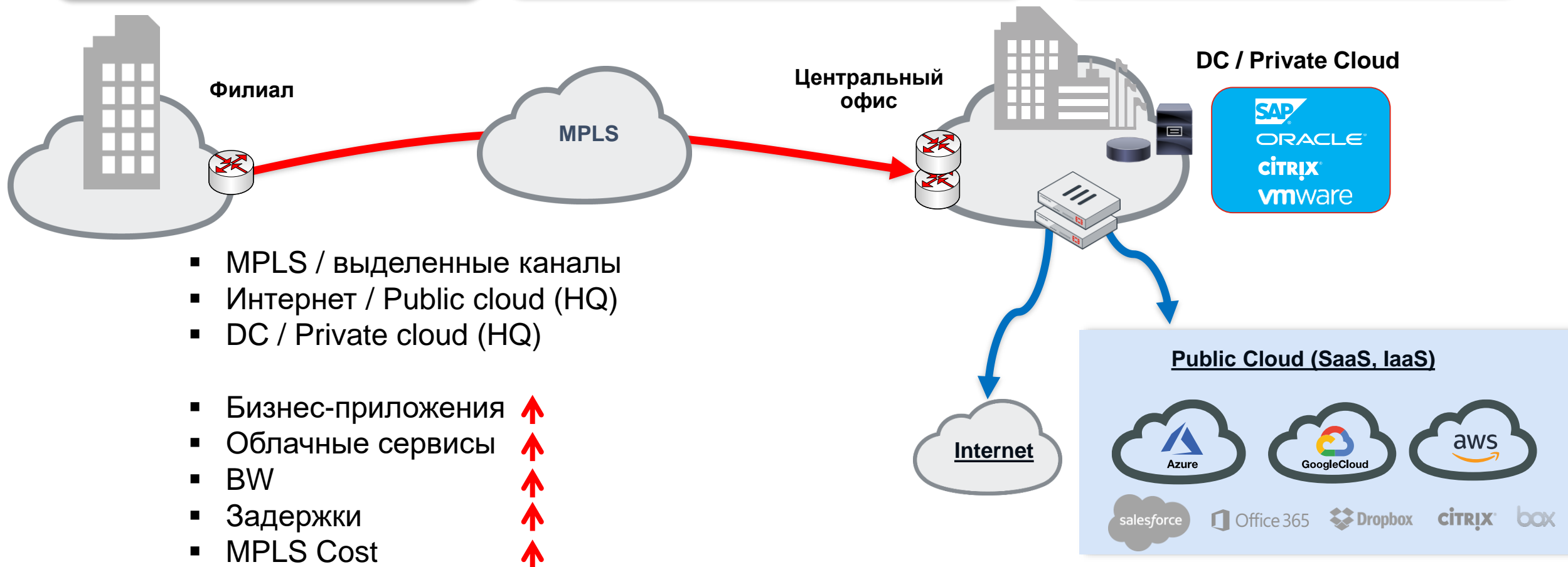
Традиционная WAN

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



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

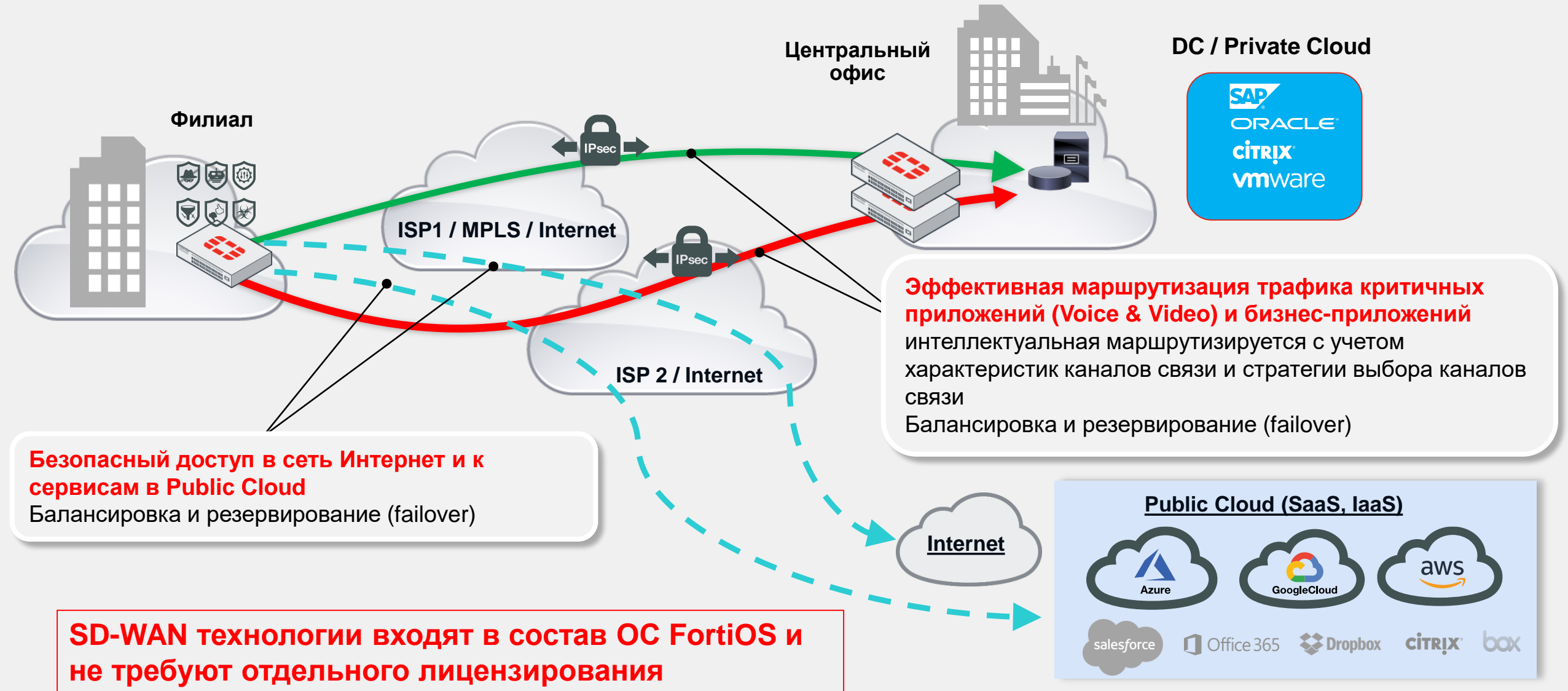
6

Интеграция с LAN инфраструктурой (Secure SD-Branch)

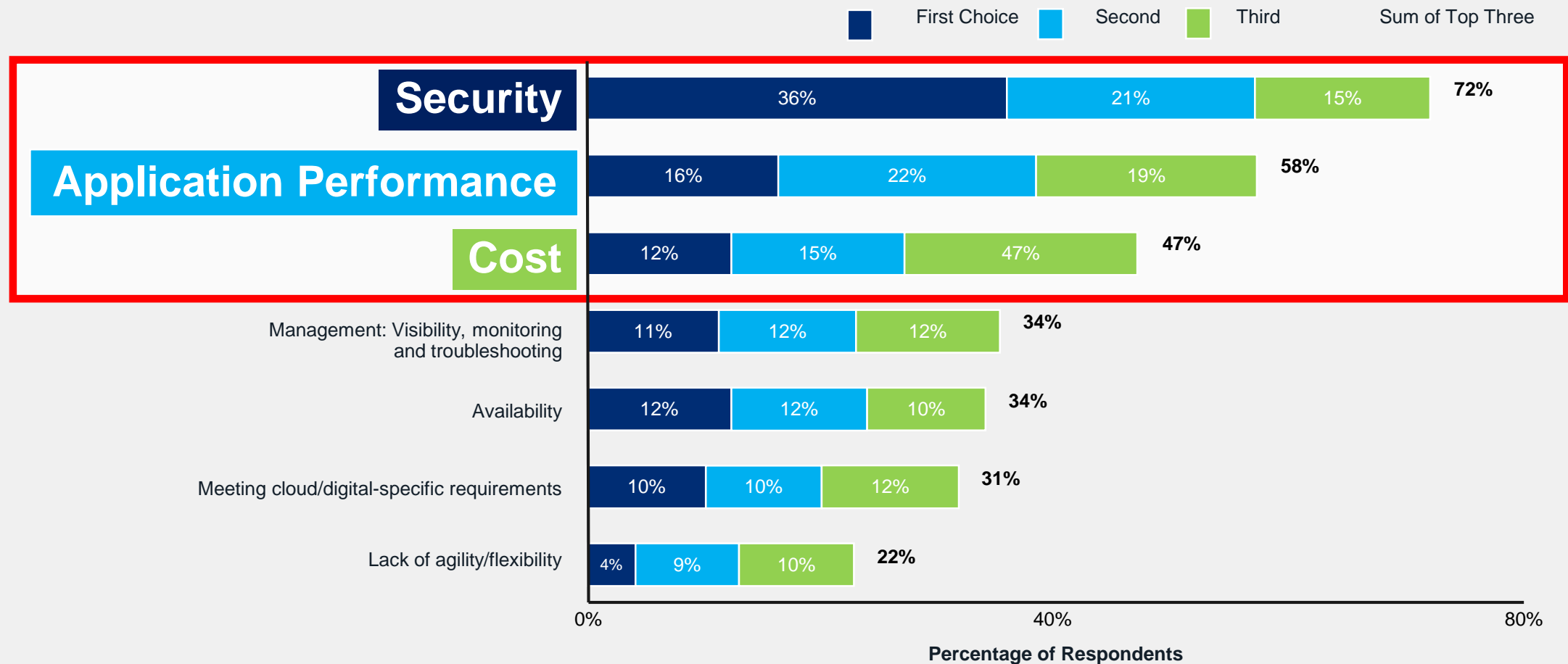
- Интегрированный контроллер коммутаторов и ТД (управление, конфигурация и мониторинг), FOS NAC
- Интеграция с другими продуктами - FNAC, FSA, FAC
- Безопасность пользовательских устройств (FCL-EMS)
- **2FA**



Реализация WAN с использованием Secure SD-WAN



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



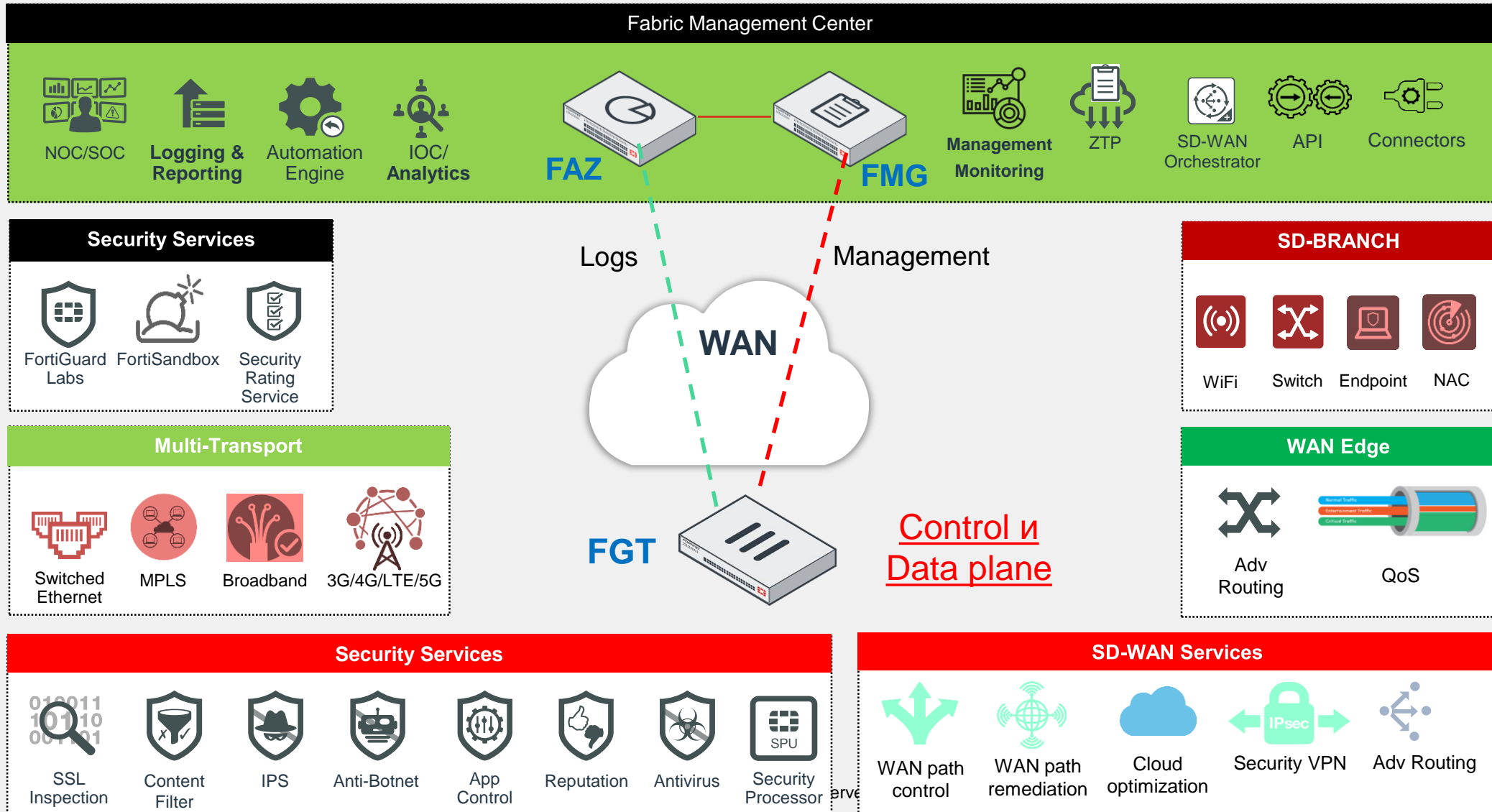


Архитектура Secure SD-WAN



Архитектура Fortinet Secure SD-WAN (Controllerless)

Orchestration и Management plane





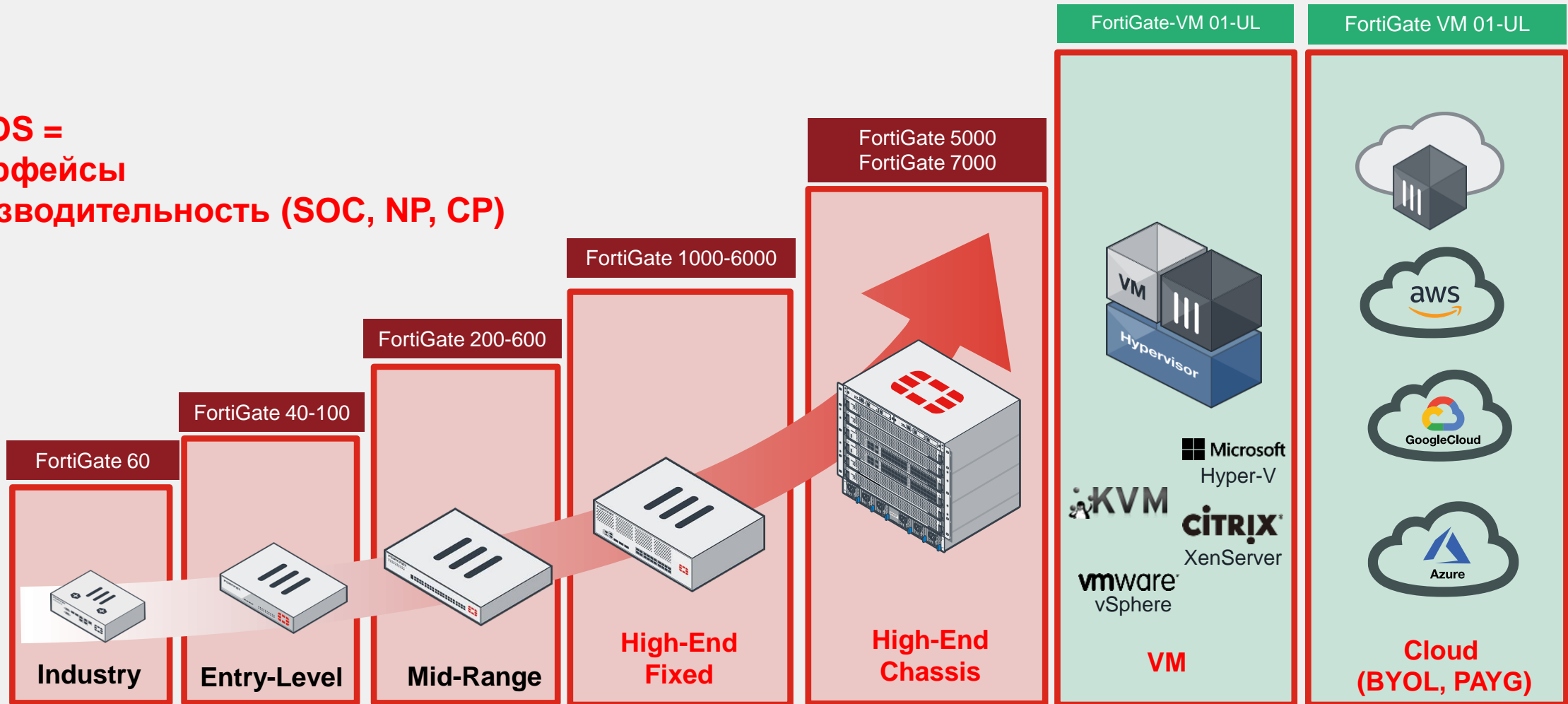
FortiGate



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)



Ускорение сетевого трафика



Ускорение контентной обработки



CPU+CP9XLite+NP6XLite

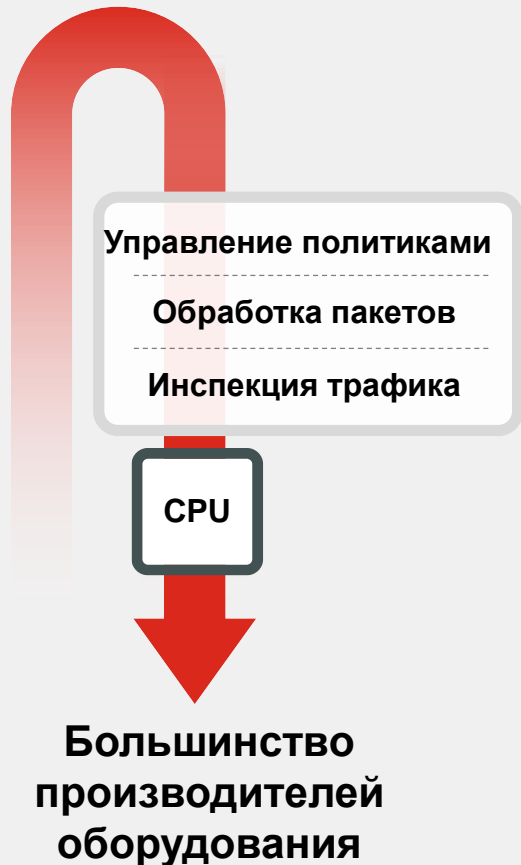
Улучшение архитектуры, емкости и производительности

2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016.. 2019 2020

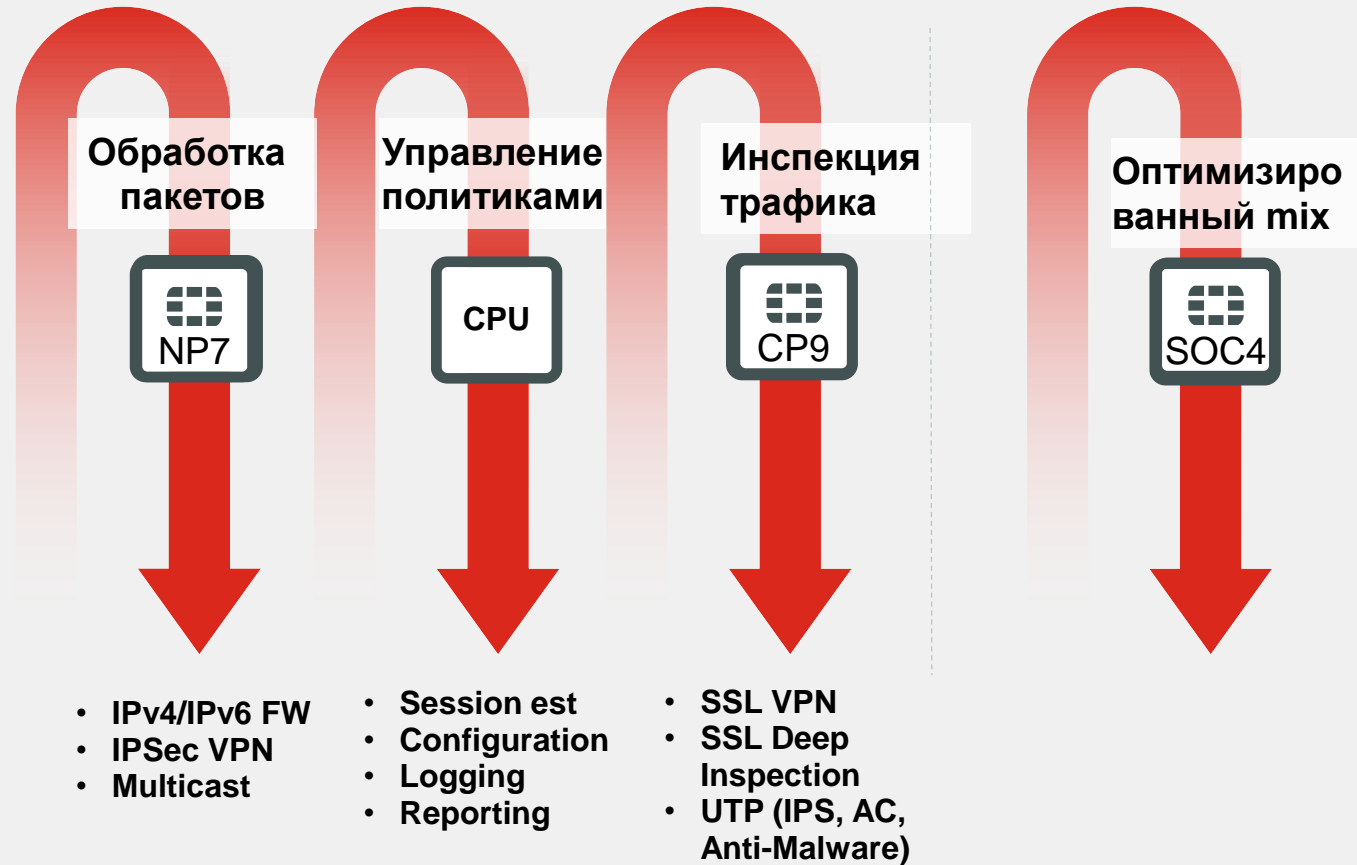


Преимущества использования SPU

CPU Only «классический подход»



Архитектура Fortinet Parallel Path Processing (PPP)



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





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




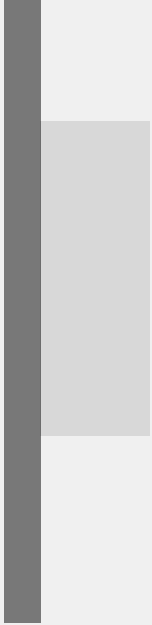



- 1 Сбор и корреляция логов**
 - Централизованная система сбора, корреляции и анализа журнальных файлов (логов)
- 2 Анализ логов и отчетность**
 - Анализ логов и построение всесторонних отчетов для понимания ситуации в сети
- 3 Генерация уведомлений**
 - Генерация уведомлений (events) в FAZ/email/SNMP/syslog,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



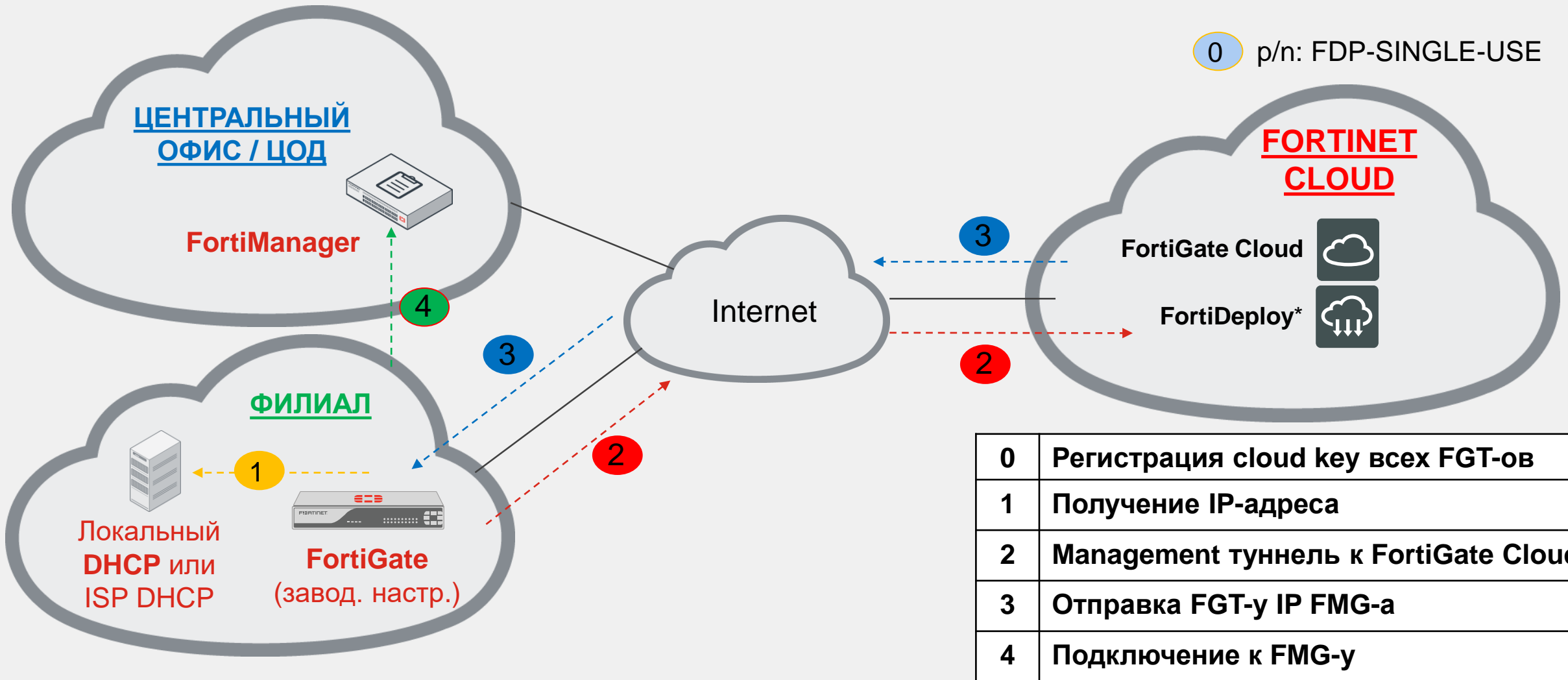


**Автоматическое
развёртывание и начальное
конфигурирование (ZTP)**



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





Независимые оценки



Лидер в области Network Firewall и Wan Edge



2020 Magic Quadrant for Network Firewalls

2021 Magic Quadrant for WAN Edge Infrastructure

Figure 1. Magic Quadrant for Network Firewalls

Figure 1: Magic Quadrant for WAN Edge Infrastructure



Source: Gartner (November 2020)

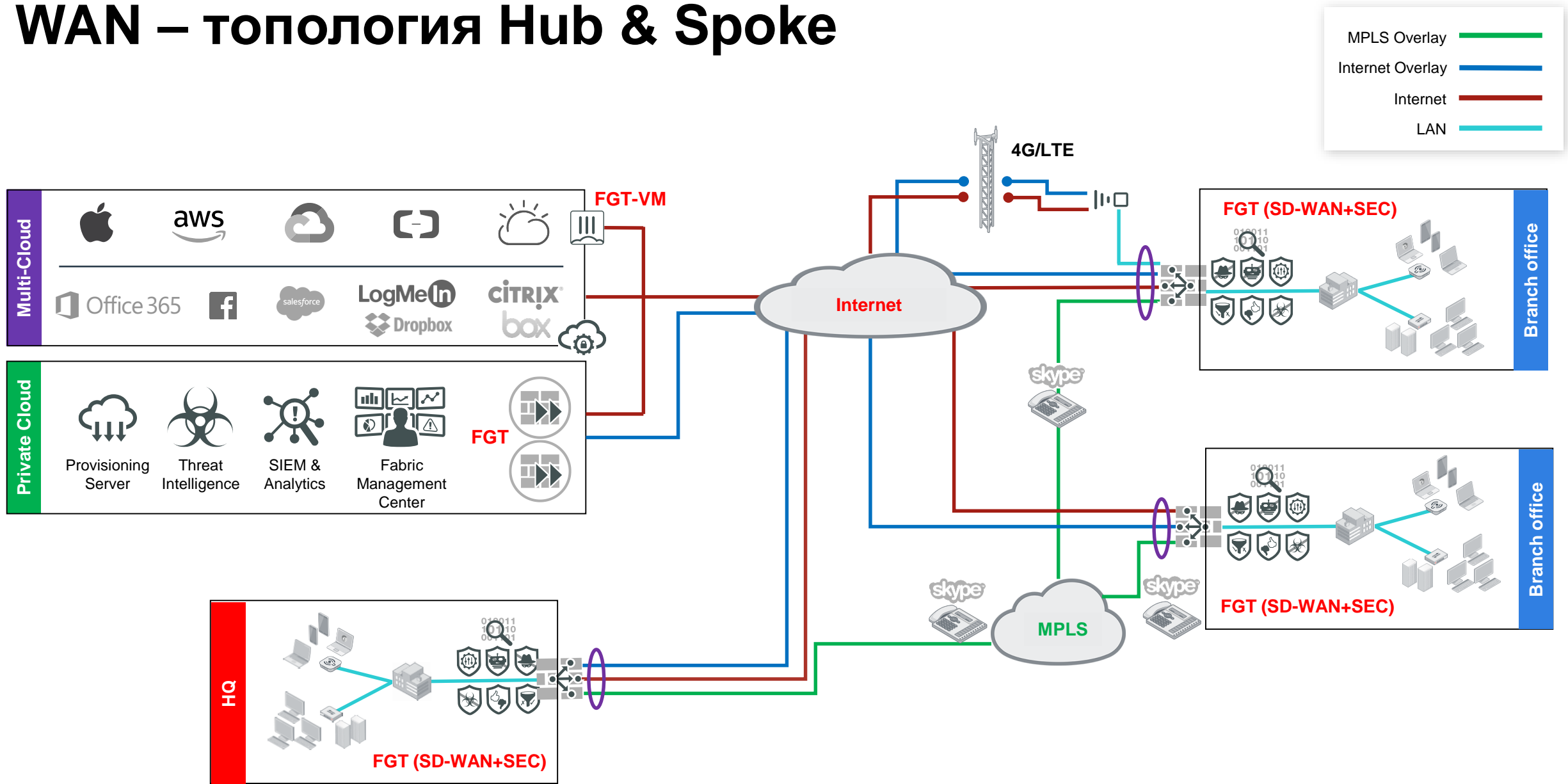
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet. Gartner does not endorse any vendor, product or service depicted in its research publications, 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.



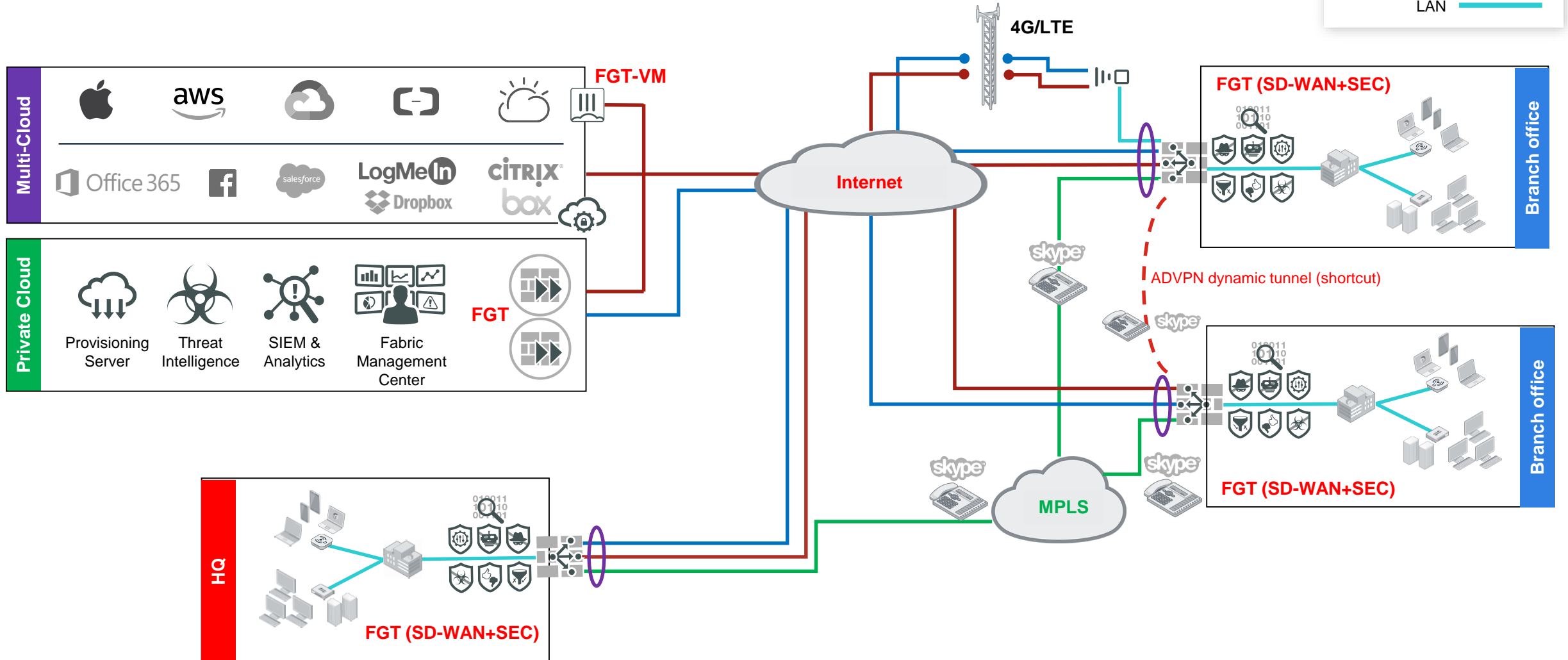
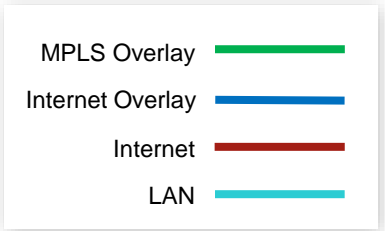
**Варианты
использования
Secure SD-WAN**



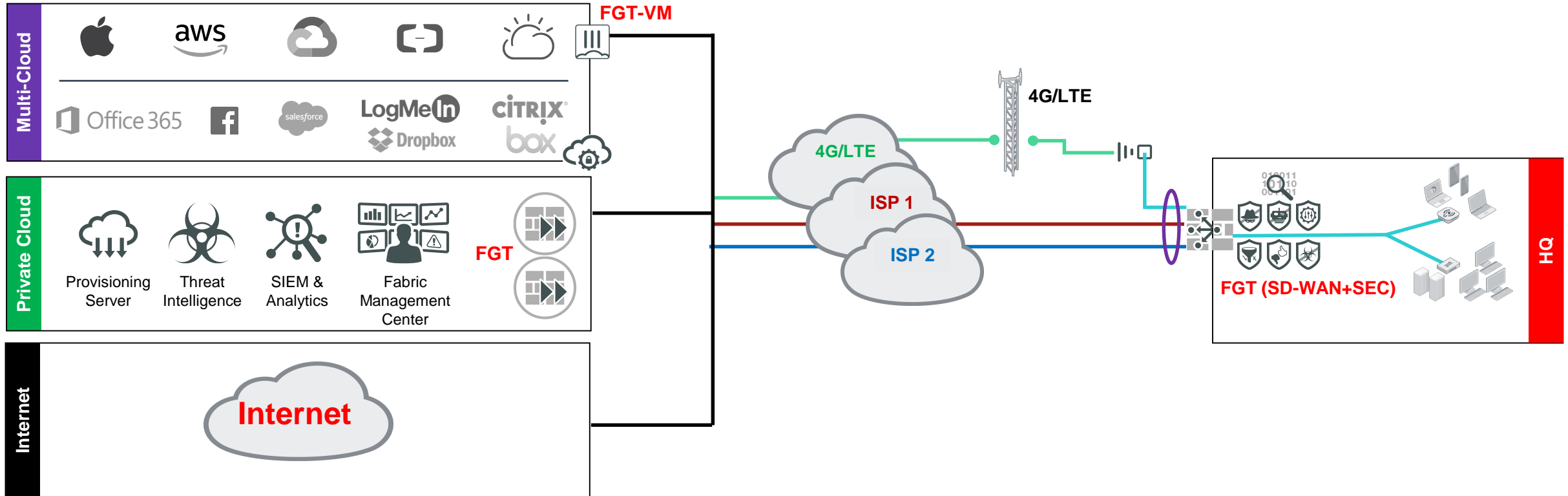
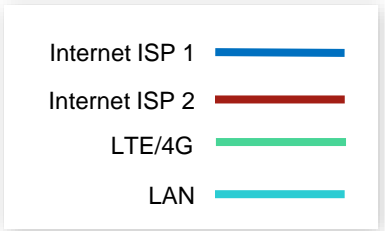
WAN – топология Hub & Spoke



WAN – топология ADVPN



Центральный офис

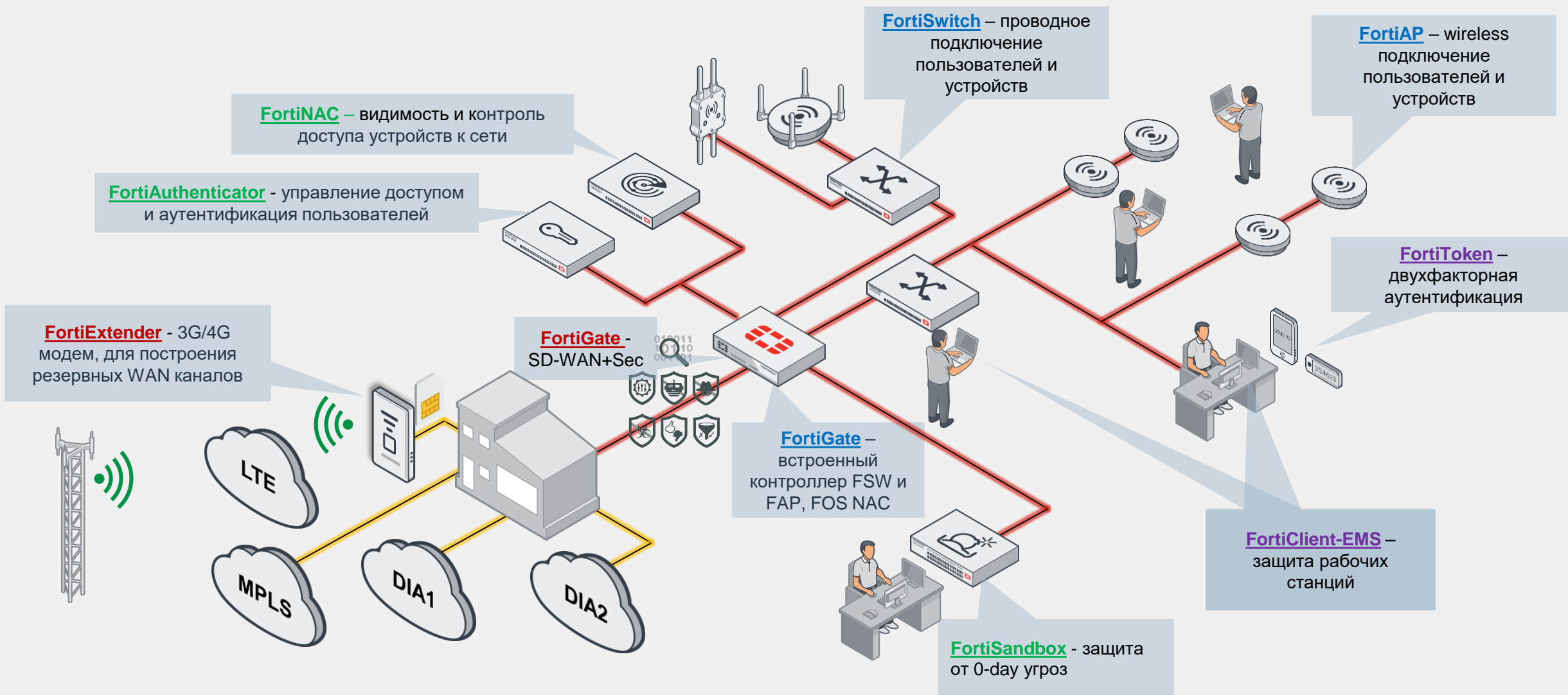




Secure SD-Branch



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

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

SD-WAN Zones

SD-WAN Rules

Performance SLAs

Bandwidth

Volume

Sessions

Download

Upload

8 Total

8 Total

W_INET1_1_0

W_INET1_2_0

W_INET2_1_0

W_INET2_2_0

W_MPLS_1_0

W_MPLS_2_0

W_INET1_1_0

W_INET1_2_0

W_INET2_1_0

W_INET2_2_0

W_MPLS_1_0

W_MPLS_2_0

Create New

Edit

Delete

	Interfaces	Gateway	Cost	Download	Upload	Active Sessions	Bytes Received	Bytes Sent	Status
	virtual-wan-link								
	SASE								
	Overlay								
	W_INET1_1_0	0.0.0.0	0	3.92 kbps	1.50 kbps	3	15.78 MB	6.02 MB	Enable
	W_INET1_2_0	0.0.0.0	0	2.21 kbps	867 bps	2	8.83 MB	3.46 MB	Enable
	W_INET2_1_0	0.0.0.0	0	3.96 kbps	1.52 kbps	3	15.78 MB	6.02 MB	Enable
	W_INET2_2_0	0.0.0.0	0	2.21 kbps	864 bps	2	8.83 MB	3.46 MB	Enable
	W_MPLS_1_0	0.0.0.0	0	5.67 kbps	2.15 kbps	4	22.69 MB	8.59 MB	Enable
	W_MPLS_2_0	0.0.0.0	0	3.92 kbps	1.50 kbps	3	15.74 MB	6.02 MB	Enable
	Underlay								
	port1	100.64.64.1	0	14.88 kbps	14.31 kbps	9	250.94 MB	107.17 MB	Enable
	port2	100.65.65.1	0	7.85 kbps	7.87 kbps	7	31.32 MB	31.36 MB	Enable

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



SD-WAN Performance SLA - link health monitoring

- 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

Edit Performance SLA

Name: HQ

Probe mode: Active Passive Prefer Passive

Protocol: Ping HTTP DNS

Server: 10.100.99.1

Participants: All SD-WAN Members

- W_INET1_1_0
- W_INET1_2_0
- W_INET2_1_0
- W_INET2_2_0
- W_MPLS_1_0
- W_MPLS_2_0

SLA Target:

Latency threshold: 100 ms

Jitter threshold: 5 ms

Packet Loss threshold: 5 %

Link Status

Check interval: 500 ms

Failures before inactive: 5

Restore link after: 5 check(s)

Actions when Inactive

Update static route:

1. Measures the health of links
2. SLA Target/s
3. Link Status
4. SLA statistics

SLA Details			
	Packet Loss	Latency	Jitter
<input checked="" type="checkbox"/> W_INET1_1_0	0.00%	2.91ms	1.45ms
<input checked="" type="checkbox"/> W_INET1_2_0	0.00%	2.59ms	1.42ms
<input checked="" type="checkbox"/> W_INET2_1_0	0.00%	2.73ms	1.63ms
<input checked="" type="checkbox"/> W_INET2_2_0	0.00%	2.64ms	1.29ms
<input checked="" type="checkbox"/> W_MPLS_1_0	0.00%	2.70ms	1.40ms
<input checked="" type="checkbox"/> W_MPLS_2_0	0.00%	2.60ms	0.94ms

Additional Information

Performance SLA Setup Guides

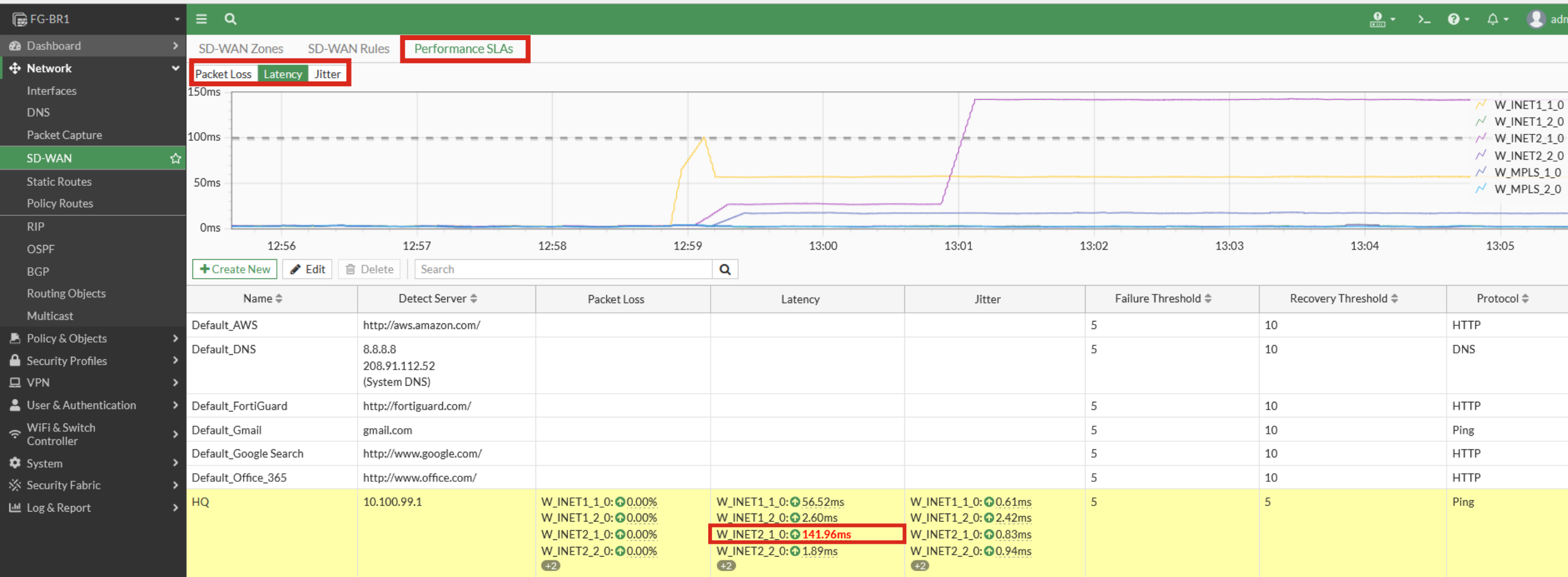
- [Link Monitoring](#)
- [SLA Targets](#)

Documentation

- [Online Help](#)
- [Video Tutorials](#)

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

The screenshot shows the Fortinet SD-WAN configuration interface. On the left is a dark sidebar with a menu: 'FG-BR1' (selected), 'Dashboard', 'Network' (expanded), 'Interfaces', 'DNS', 'Packet Capture', and 'SD-WAN' (highlighted in green). The main content area has a green header with a search icon and a grey sub-header 'Edit Implicit Rule'. Below this is a dropdown menu for 'Load Balancing Algorithm' with a red border. The dropdown options are: 'Source IP' (highlighted in green), 'Sessions', 'Spillover', 'Source-Destination IP', and 'Volume'.



SD-WAN Rules

The screenshot shows the configuration page for a Priority Rule named "GMAIL" on a device labeled "FG-BR1". The left sidebar contains a navigation menu with categories like Network, Policy & Objects, and System. The main content area is divided into several sections:

- Name:** GMAIL
- Source:** A red box highlights this section, which includes:
 - Source address: INT_LAN
 - User group: (empty)
- Destination:** Includes:
 - Address: (empty)
 - Internet Service: Google-Gmail
 - Application: (empty)
- Outgoing Interfaces:** A blue box highlights this section, which includes:
 - Strategy selection:
 - 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: (empty)
 - Measured SLA: Default_Gmail
 - Quality criteria: Latency
- Forward DSCP:** Disabled
- Reverse DSCP:** Disabled
- Status:** Enable (selected) / Disable

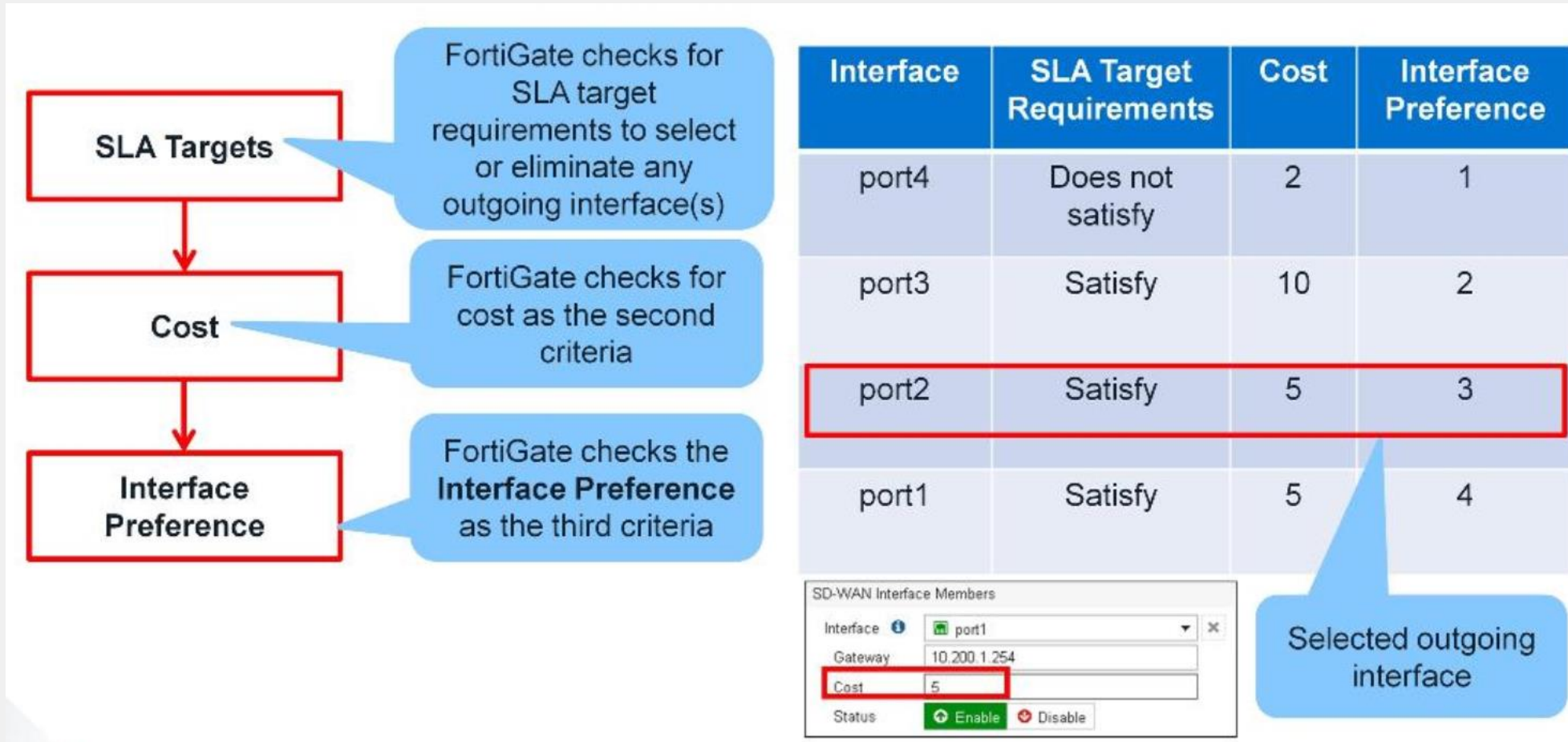


Стратегия Best Quality

The image shows two screenshots of the FortiGate SD-WAN Rules configuration interface. The top screenshot shows the 'Strategy' set to 'Best Quality' and 'Interface preference' with 'port1' and 'port2'. A blue callout box points to the interface preference list with the text: 'FortiGate will select the interface with the best quality'. The 'Quality criteria' section shows 'Latency' selected, and a red box highlights 'custom-profile-1' in the dropdown menu. The bottom screenshot shows the 'Quality check' section with 'DC_PBX_SLA' selected and 'custom-profile-1' selected in the 'Quality criteria' dropdown. Below this, there are input fields for 'latency-weight', 'jitter-weight', 'packet-loss-weight', and 'bandwidth-weight', all set to 0. A red arrow points from the 'custom-profile-1' dropdown in the top screenshot to the 'custom-profile-1' dropdown in the bottom screenshot. At the bottom of the image, a purple box contains the formula:
$$\text{Link Quality} = (a * \text{latency}) + (b * \text{jitter}) + (c * \text{packet loss}) + (d / \text{bandwidth})$$



Стратегия Lowest cost



Стратегия Maximize Bandwidth

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

Traffic will be load balanced between these interfaces using the session based round robin method

Cost and Interface Preference will not be taken into account



Firewall Policy

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
SPOKE---HUB	lan	Overlay	INT_LAN	EXT_LAN	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	0 B
HUB---SPOKE	Overlay	lan	EXT_LAN	INT_LAN	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	0 B
SPOKE---INTERNET-DIA	lan	Underlay	INT_LAN	all	always	ALL	ACCEPT	Enabled	AV default WEB default DNS default APP default IPS default SSL deep-inspection	All	174.57 MB
SPOKE---INTERNET-RIA	lan	Overlay	INT_LAN	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	0 B
FL---INTERNET	fortilink	Underlay	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	149.95 kB
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	0 B



Routing

The screenshot displays the configuration interface for Static Routes on a Fortinet device (FG-BR1). The left sidebar shows the navigation menu with 'Static Routes' selected. The main content area features a table of routes. A red box highlights the following entry:

Destination	Gateway IP	Interface	Status
0.0.0.0/0		Overlay Underlay	Enabled





Заключение



Защищённый SD-WAN и SD-Branch от Fortinet

Преимущества для Вас

1

Улучшение производительности приложений (повышение удовлетворенности пользователей)

4

Упрощение управления и внедрения

2

Обеспечение безопасного доступа в Internet / Public Cloud

5

Экономия затрат (OpEx, CapEx) и гибкость подключения

3

Упрощение дизайна WAN

6

Интеграция с LAN инфраструктурой (Secure SD-Branch)



FORTINET®