



Эволюция решений защиты филиальной ИТ инфраструктуры

Алексей Мальцев

системный инженер 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.**

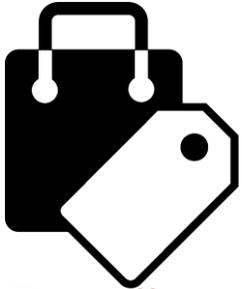
- ✓ Протоколы и сервисы
- ✓ База интернет-ресурсов (ISDB)
- ✓ Видимость и управления на уровне приложений L7 (Application awareness)

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

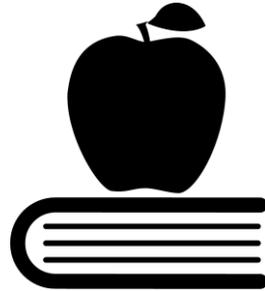
- ✓ Функции безопасности NGFW от FortiGate
- ✓ Инспекция SSL (включая TLS 1.3)

- ✓ Очереди, приоритезация и шейпирование
- ✓ Гарантирование полосы

Организации с **распределённой** структурой



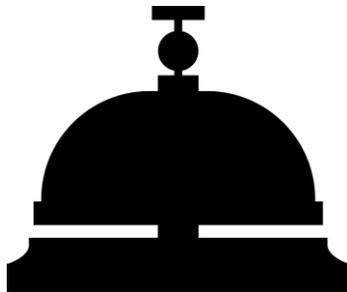
Ритейл



**Образовательные
учреждения**



Финансовый сектор



Сфера обслуживания



**Организации
здравоохранения**

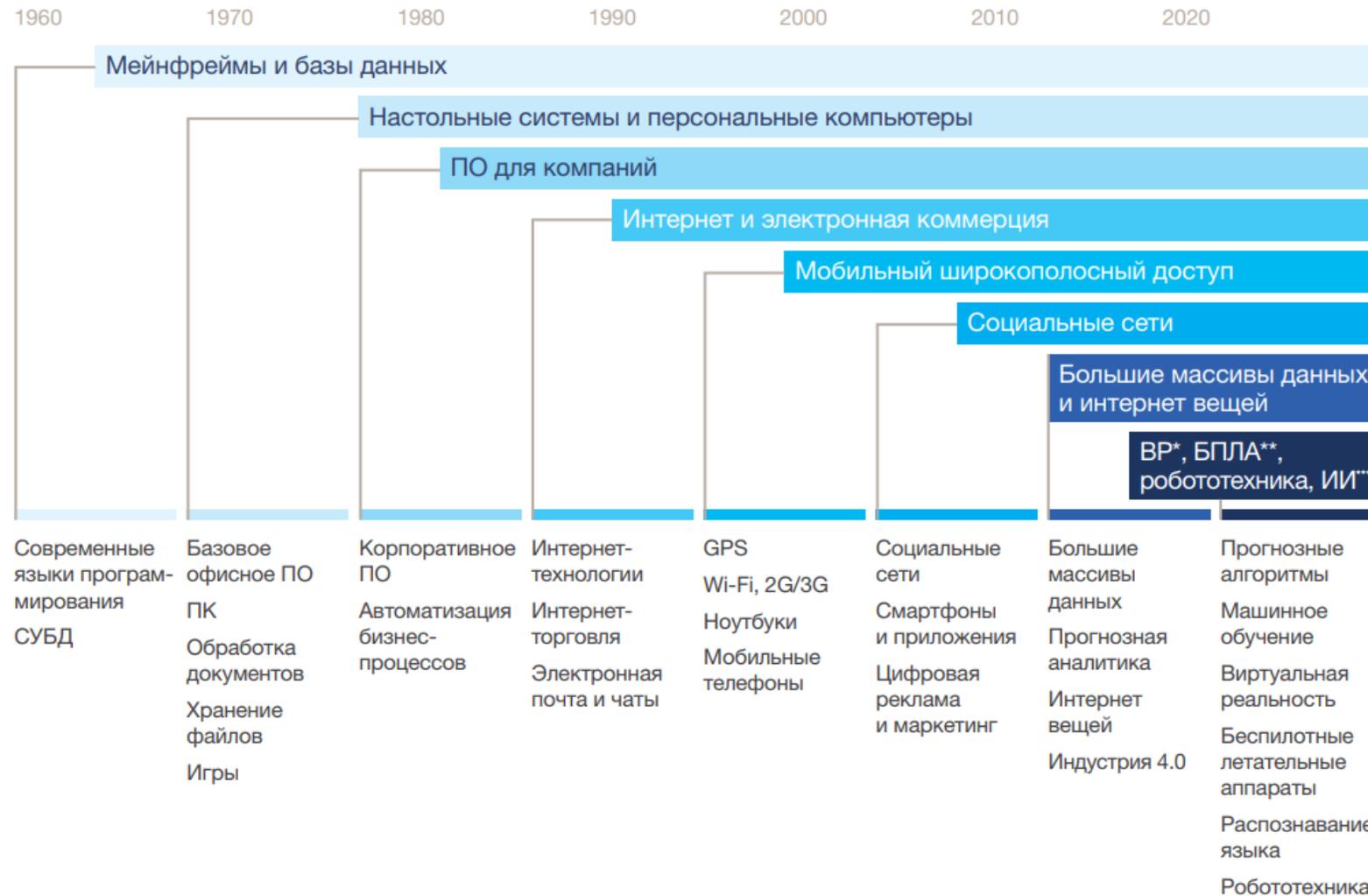


Сети ресторанов

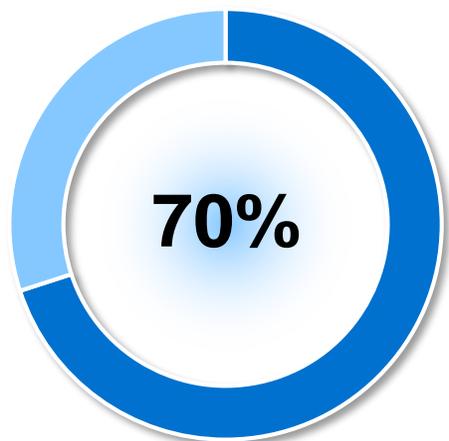


**Государственные
организации**

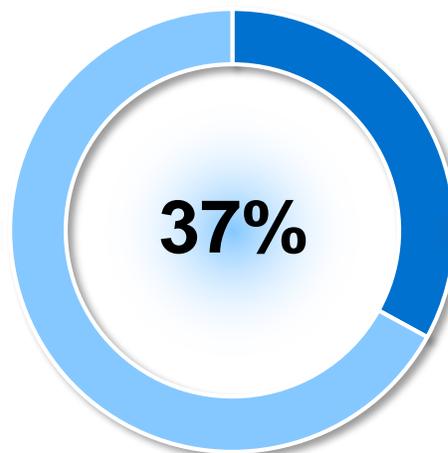
Цифровая экономика формируется под влиянием ускоряющихся волн инноваций



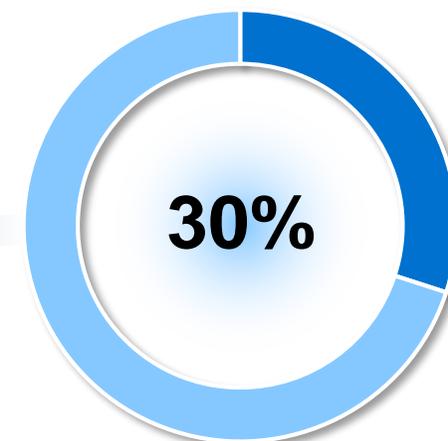
Облака и приложения SaaS



Процент приложений уже доступны в облаках



Считают, что SaaS удобнее в развёртывании и использовании по сравнению с локальными сервисами



Активно используют приложения SaaS

Влияние цифровой трансформации на SD-WAN



>50%

Организаций планируют использовать технологии SD-WAN в ближайшее время¹



62[↑]

Среднее количество облачных приложений. Значительный рост использования приложений SaaS и IaaS²



\$8 млрд.

Оценка роста рынка SD-WAN решений к 2022 году. 83% роста за 2017 год³



70%[↑]

Заказчиков отмечают, что существующие WAN-сети медленные, дорогие и неэффективны для облачных приложений⁴

Пример миграции из MPLS в SD-WAN

Традиционные WAN



Пример миграции из MPLS в SD-WAN

Пример 1. Резервирование MPLS

Критичные приложения (Voice & Video) Лучший маршрут выбирается в зависимости от задержки, джиттера и потери пакетов.



ORACLE®

Microsoft Azure

SAP®

CITRIX®

vmware

Критичные приложения (Voice & Video) Перенаправляются в новые туннель в случае ухудшения качества в основном WAN.

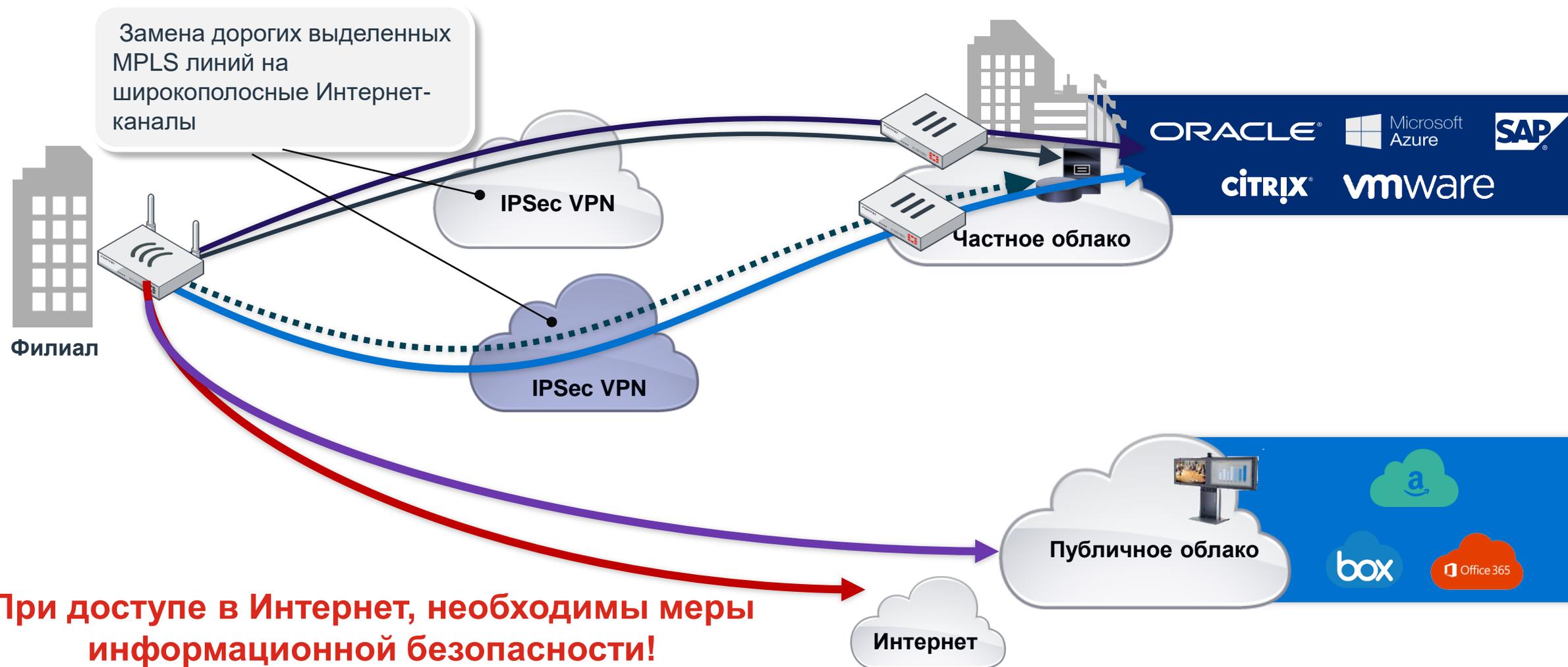
Бизнес-приложения Балансируются через различные линии, таким образом полоса оптимизирована.

Широкополосный доступ в сеть Интернет (SaaS и IaaS приложения) Балансировка, если требуется.

При доступе в Интернет, необходимы меры информационной безопасности!

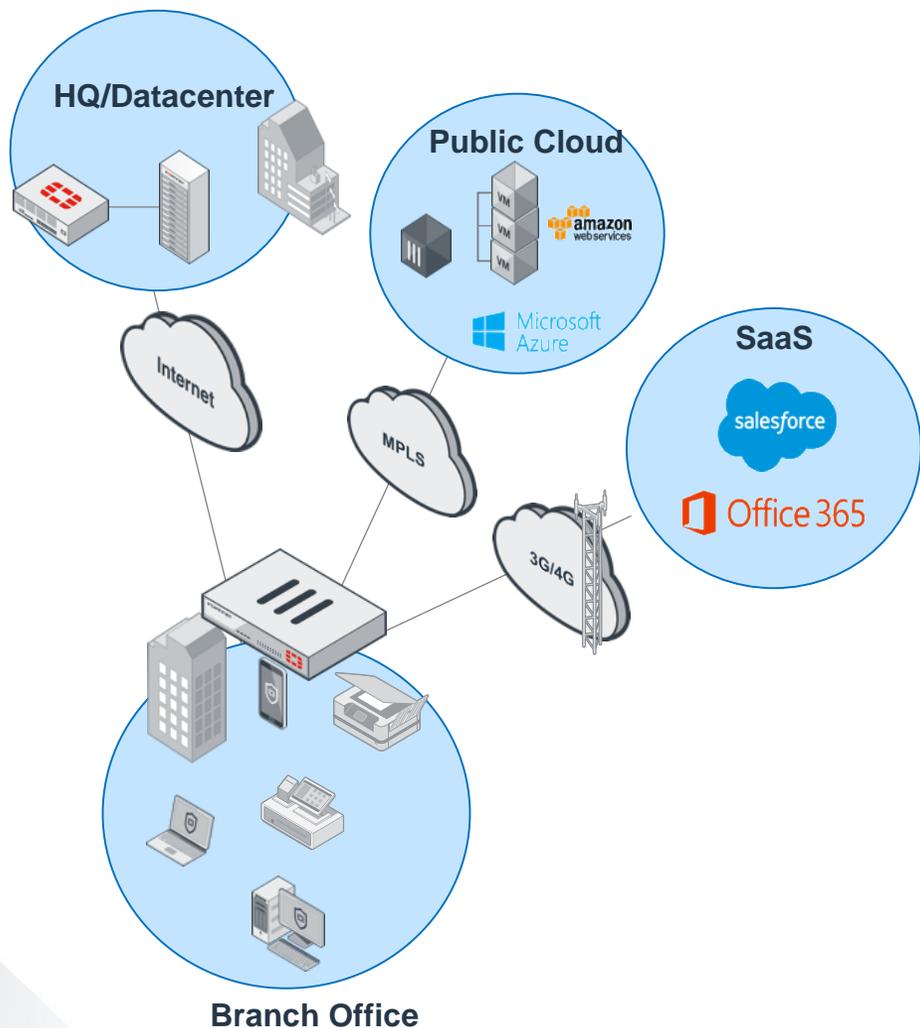
Пример миграции из MPLS в SD-WAN

Пример 2. Замена MPLS



При доступе в Интернет, необходимы меры информационной безопасности!

WAN vs. SD-WAN



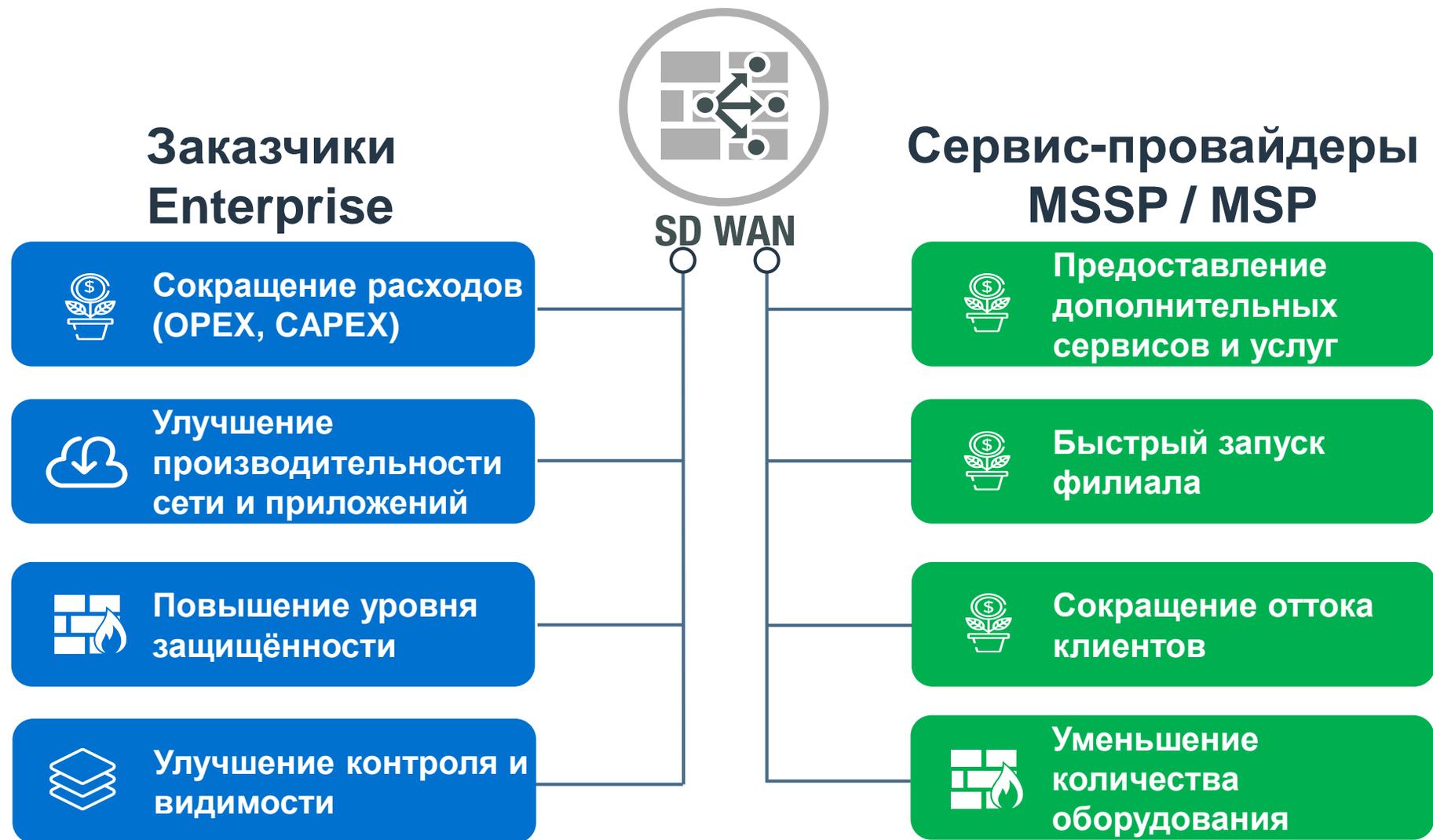
■ WAN (Wide Area Network)

- » Традиционно используются для подключения удалённых площадок, филиалов и ЦОД
- » На основе дорогих выделенных каналов MPLS
- » Фиксированные скорости и сложности при росте скоростей
- » Выделенное оборудование

■ SD-WAN (Software-Defined WAN)

- » Создают оверлей (overlay)
- » Не зависят от вида транспорта
- » Отделяют Management, Data, Control Plane
- » Позволяет строить эффективные WAN-соединения через каналы Интернет
- » Ориентируются на бизнес-приложения

Мотиваторы развития технологии SD-WAN



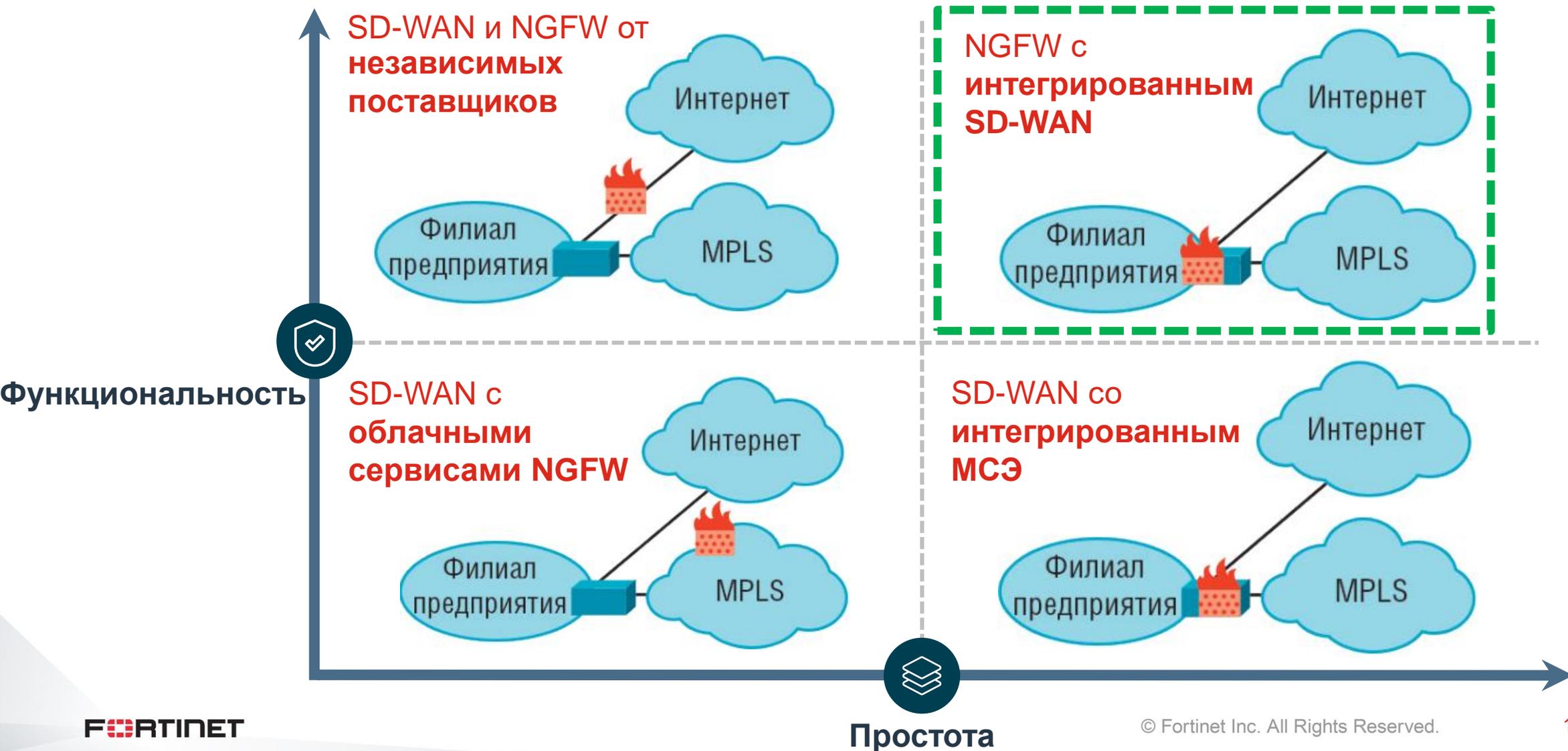
Безопасность – основное препятствие для SD-WAN



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 в проектах SD-WAN, наряду с производительностью и стоимостью

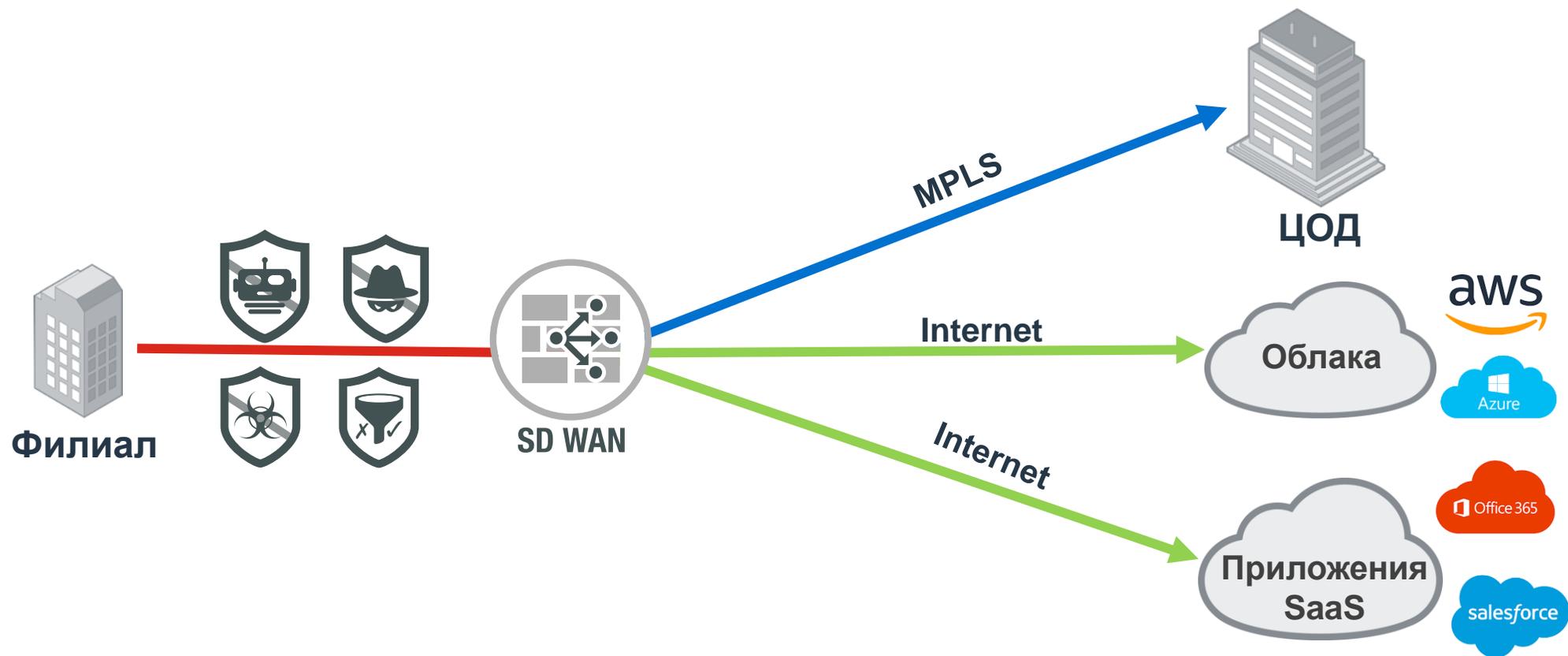
Архитектуры безопасности для SD-WAN



#1. FortiGate - это NGFW с интегрированным SD-WAN

Функциональные возможности и безопасность
от FortiOS

#1. FortiGate NGFW с интегрированным SD-WAN



SD-WAN – это встроенный функционал FortiGate

#1. FortiGate – лидерство и инновации NGFW

“Leader” - Magic Quadrant от Gartner (Enterprise Firewall и UTM)



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



#1 – по количеству устройств безопасности (согласно IDC)

Защищённый SD-WAN



FORTINET

SD-WAN



SD-WAN



Routing and Traffic Shaping

+



VPN

+



App Control

+



Intrusion Prevention

+



Antivirus

+



URL Filtering

+



Sandboxing

+



SSL Inspection

NGFW

Высокая производительность и масштабируемость

Тесная интеграция решений и расширенная видимость

#1. Примеры реализации Fortinet Secure SD-WAN

Аналитика и решения для MSSP



FortiPortal



FortiAnalyzer

Инструменты управления и автоматизации



FortiManager



FortiDeploy



Сторонний оркестратор (SDWAN контроллер)

Fortinet Secure SD-WAN

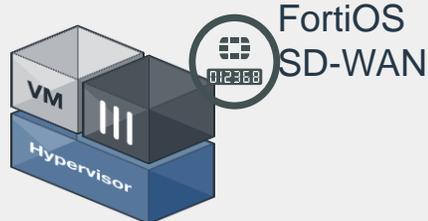


FortiExtender



FortiGate

Выделенный шлюз (ПАК)



FortiGate-VM (ESXi, KVM, etc)
3rd Party VMs

Виртуальная машина (ESXi, KVM)

Сторонняя платформа (vCPE/uCPE)



Fortinet или Partner SD-WAN
+ FortiGate-VM security

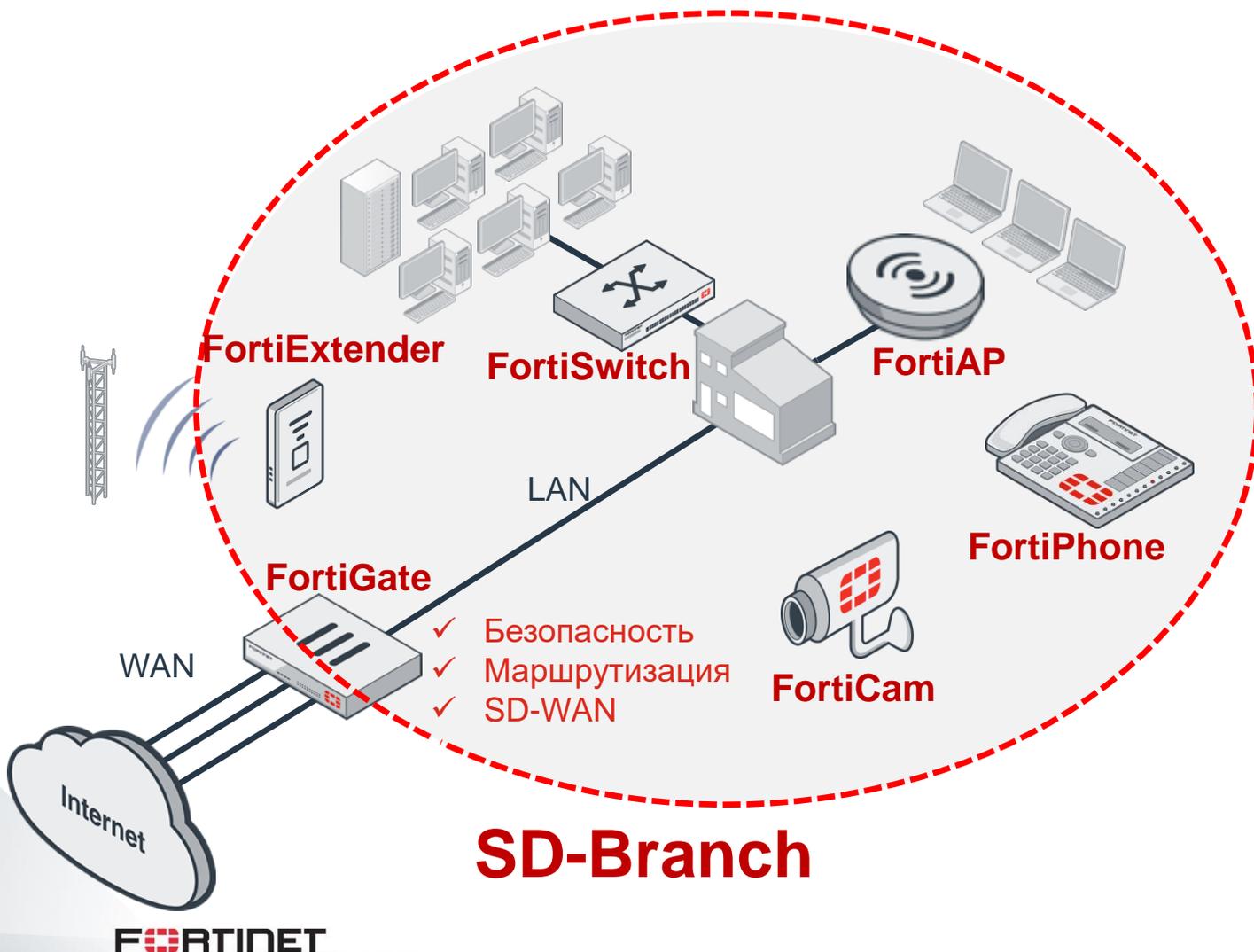
Технологические партнёры

#2. От SD-WAN к SD-Branch

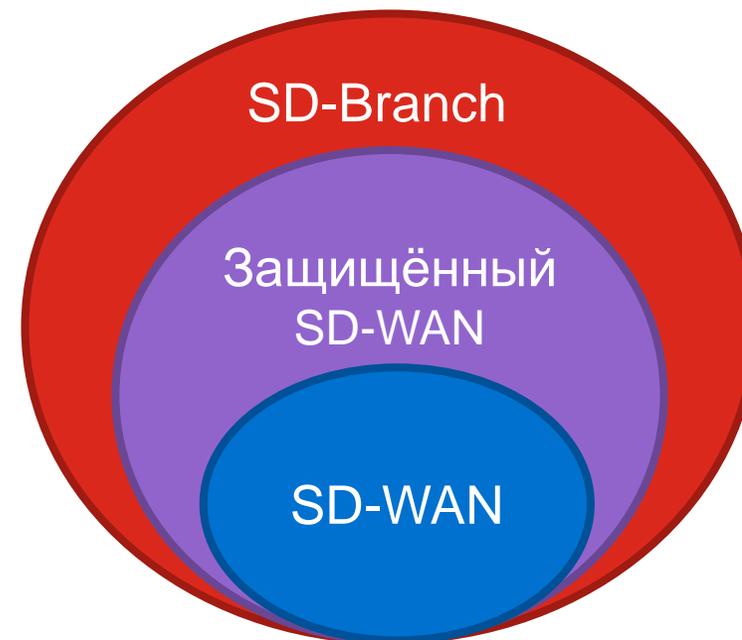
Расширение сервисов в филиале

#2. Консолидация сервисов в SD-Branch

Единая консоль управления безопасностью LAN и WAN



- Fortinet единственный вендор с интегрированными возможностями по управлению коммутаторами и точками доступа (Wireless & Switching)
- Не требует лицензирования в FortiOS



#2. FortiGate и решения Fortinet Security Fabric

Тесная интеграция решений и расширение возможностей филиала



FortiSwitch

Встроенный в CPE контроллер управления коммутаторами



FortiAuthenticator
Radius / 2FA / AAA



FortiPresence

WiFi-аналитика и поведение клиентов



FortiAP

Встроенный в CPE FortiGate WiFi-контроллер



FortiCAM/Voice

Видеонаблюдение и телефония



FortiExtender

Расширитель сигнала 4G
(важен для проектов SD-WAN)



Модемы

Резервный канал 4G/LTE



Sandbox Cloud

Уникальная для рынка SD-WAN интеграция с ATP-решением (защита от продвинутых угроз)!



FortiNAC !NEW

Контроль доступа устройств к сети



#3. SD-WAN и приложения

Продвинутые возможности по балансировке приложений и отслеживанию качества обслуживания

#3. 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



#3. Отслеживание качества SLA



 **Office 365** Latency < 100ms
Packet Loss < 1%
 **Skype for Business** Jitter < 30ms

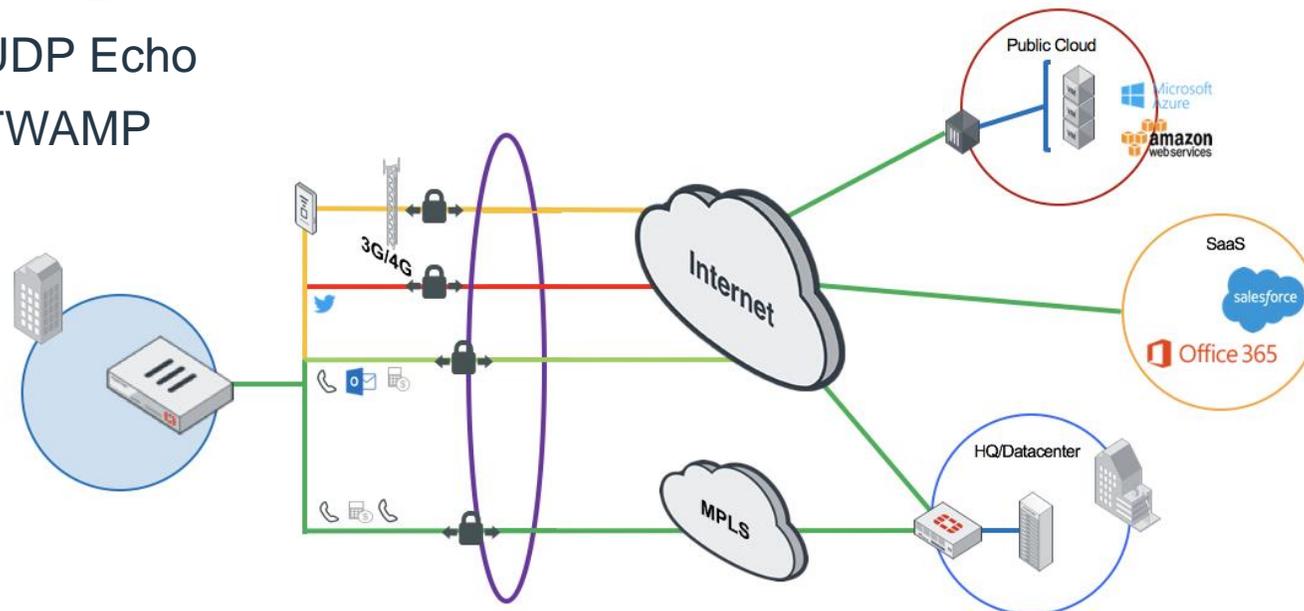
- Ping
- HTTP
- TCP Echo
- UDP Echo
- TWAMP

- Настройка интервалов
- Исключение flapping

Traffic Shaper

Параметры QoS

Динамическое переключение

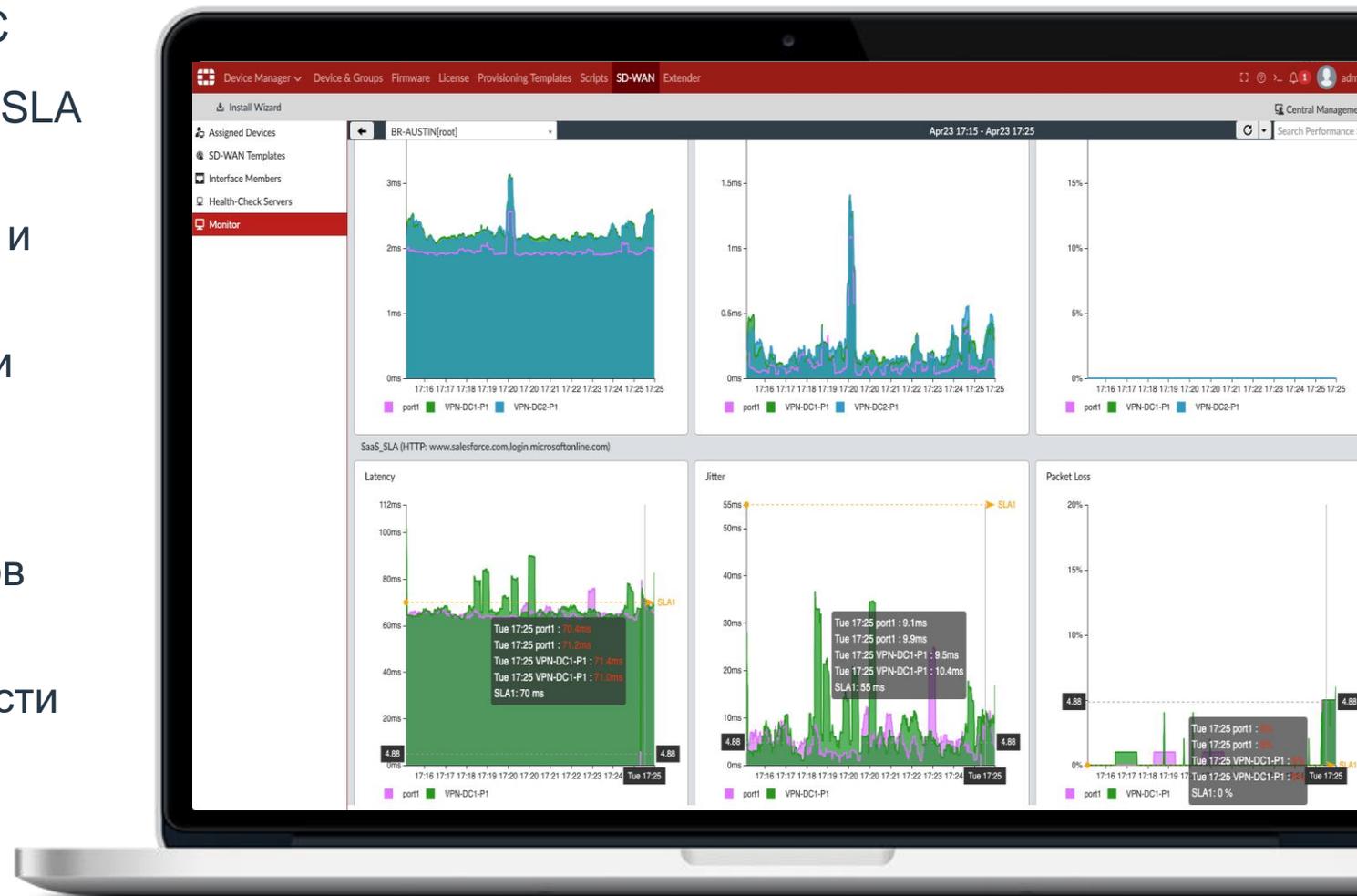


#4. FortiManager и ZTP

Централизованное управление SD-Branch и
Zero-Touch Provisioning

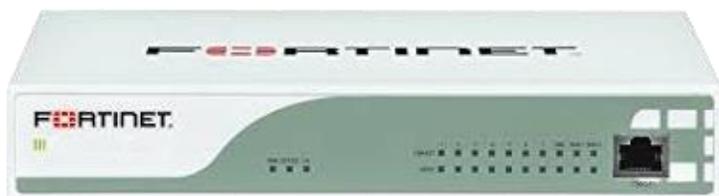
#4. FortiManager для SD-WAN – централизованное управление и видимость

- ✓ SD-WAN шаблоны и виджеты для NOC
- ✓ Продвинутое мониторинг параметров SLA SD-WAN-соединений, VPN-туннелей
- ✓ Управление политиками безопасности и мониторинг SOC
- ✓ Управление SD-Branch (коммутаторы и точки доступа)
- ✓ Автоматизация API
- ✓ Гибкость при использовании контекстов (ADOM)
- ✓ Упрощение и повышение эффективности администрирования



#4. SDWAN и Zero Touch Provisioning (ZTP)

Варианты реализации задачи ZTP



Опция DHCP



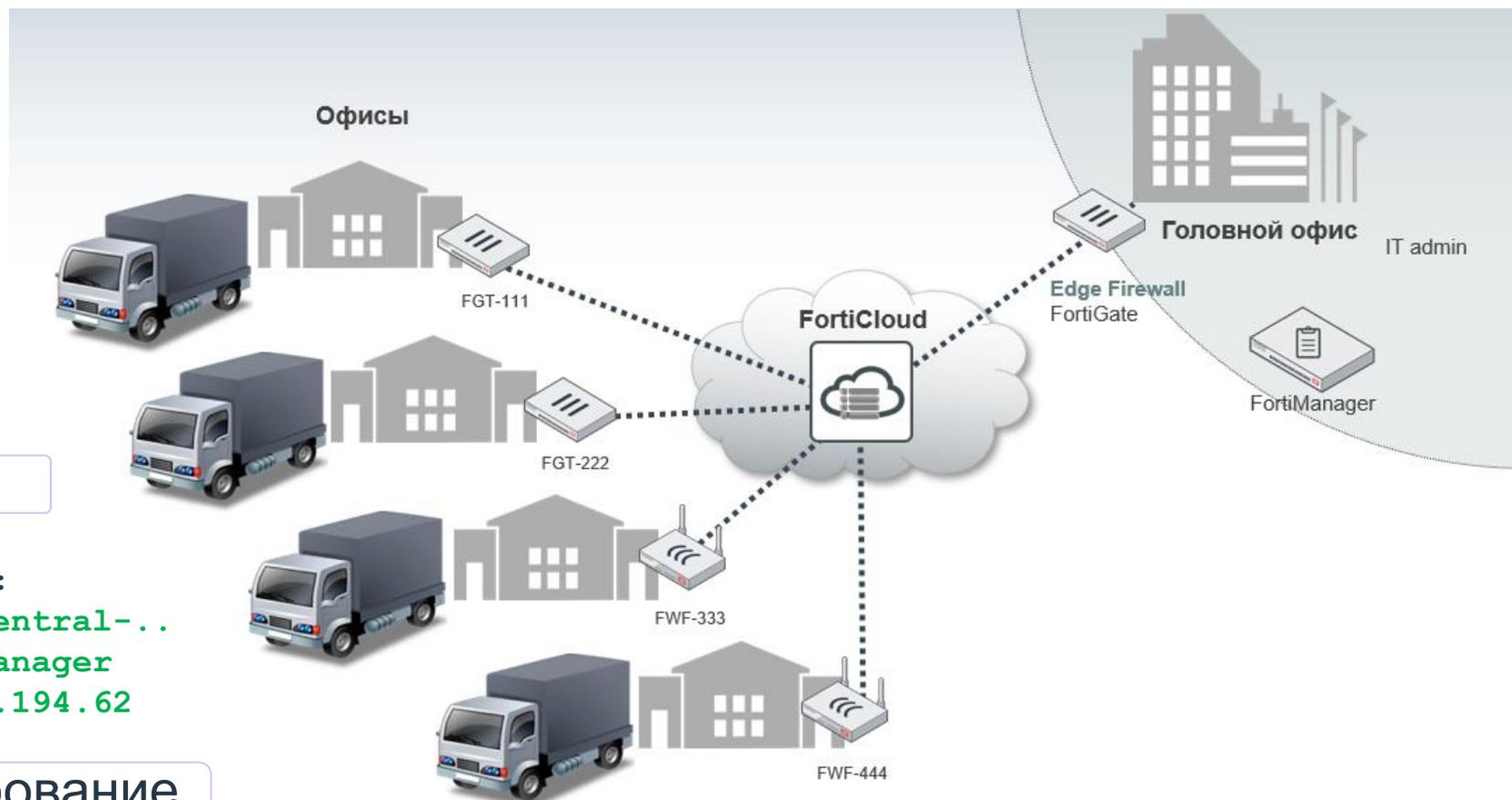
FortiDeploy



USB-накопитель

```
fgt_system.conf:  
config system central-...  
set type fortimanager  
set fmg 192.168.194.62  
set mode normal
```

Конфигурирование параметров



#5. Независимые оценки и СТОИМОСТЬ владения (ТСО)

Отчёты, аналитика, рейтинги

#5. Выбор решений SDWAN

Традиционные производители
(Pure-play игроки)



Производители решений
безопасности

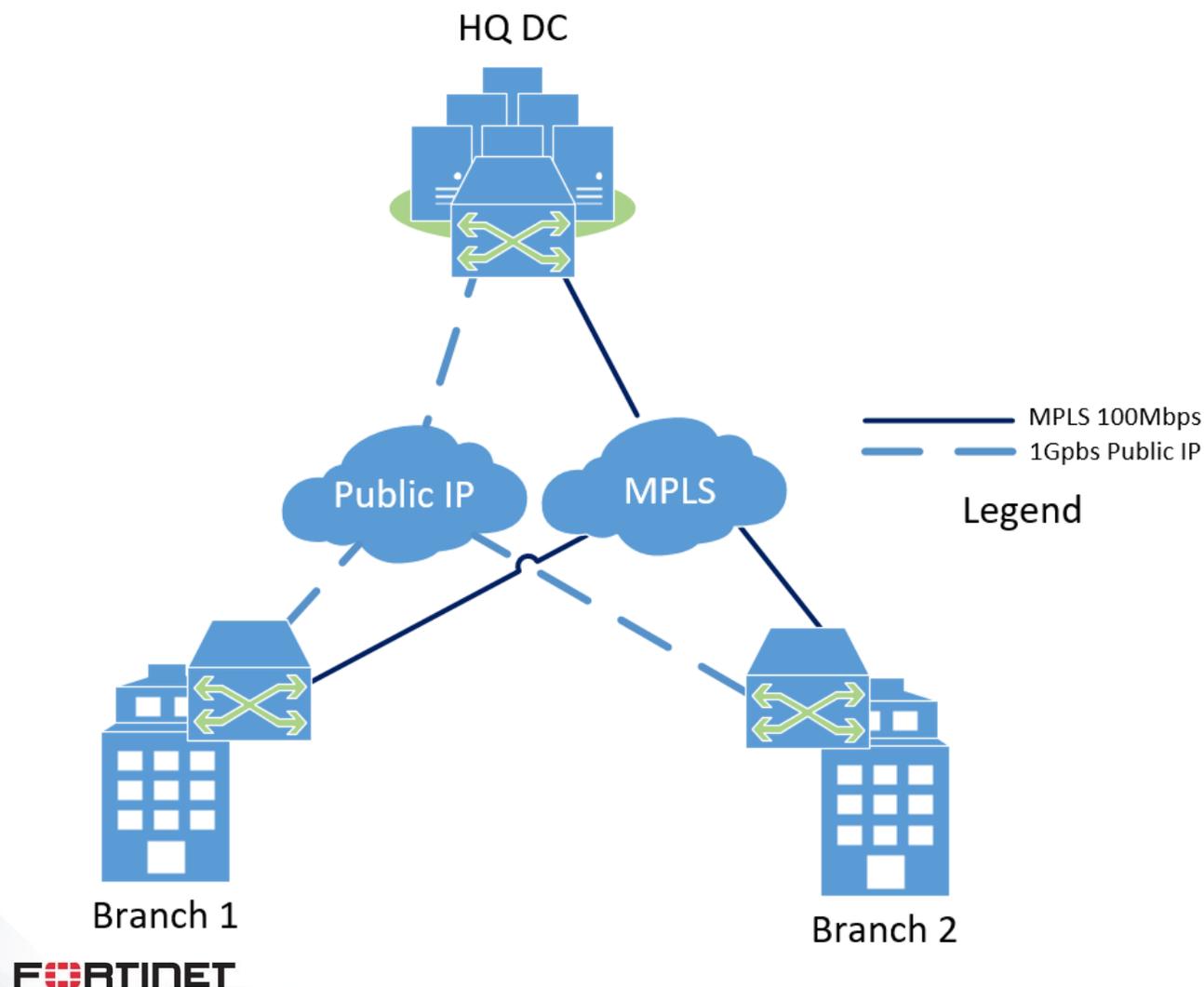


Производители беспроводных
решений (Wireless)

Поставщики решений WAN-
оптимизации трафика

#5. NSS Labs и SD-WAN

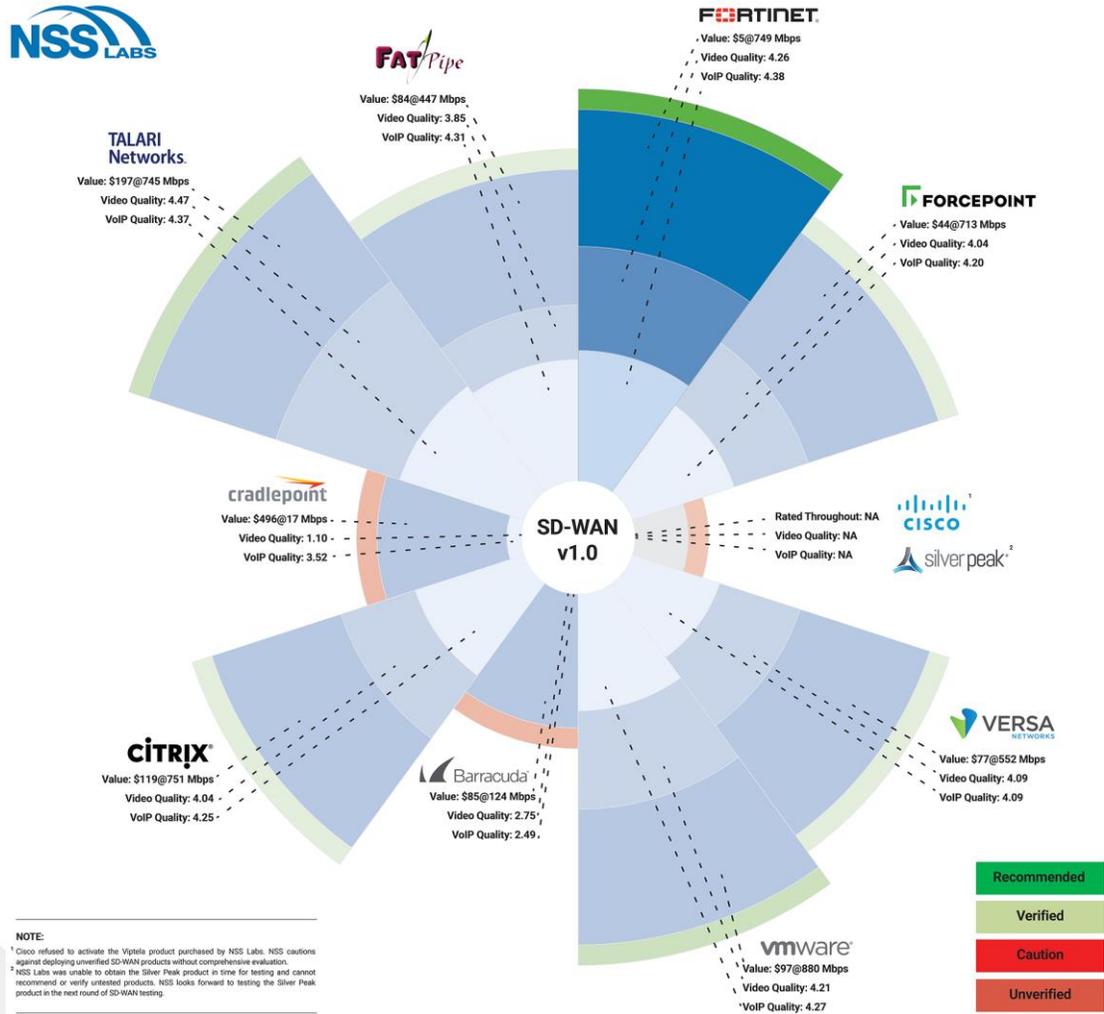
Первое в индустрии групповое тестирование решений SD-WAN



- **Первый** групповой тест лидирующих решений SD-WAN
- **Условия** испытаний:
 - ✓ Популярная топология подключения
 - ✓ Трафик Business Critical
 - ✓ Различные сценарии с плохим качеством сетевых соединений
 - ✓ Оценка ZTP



#5. Fortinet SD-WAN – Рекомендовано NSS Labs



NOTE
 1 Cisco refused to activate the Viptela product purchased by NSS Labs. NSS cautions against deploying unverified SD-WAN products without comprehensive evaluation.
 2 NSS Labs was unable to obtain the Silver Peak product in time for testing and cannot recommend or verify untested products. NSS looks forward to testing the Silver Peak product in the next round of SD-WAN testing.



Наивысшая оценка QoE для VoIP
4.38 из 4.41

Лучшая оценка стоимости владения
\$5@749 Mbps

Единственный вендор безопасности со статусом Recommended
Заблокировано 100% атак

Vendor	QoE for VoIP		QoE for Video		TCO per Mbps	Overall Rating
Barracuda Networks	2.49	Below Use Case	2.75	Below Use Case	\$85	Caution
Citrix Systems	4.25	Above Use Case	4.04	Above Use Case	\$119	Verified
Cradlepoint	3.52	Above Use Case	1.10	Below Use Case	\$496	Caution
FatPipe Networks	4.31	Above Use Case	3.85	Above Use Case	\$84	Verified
Forcepoint	4.20	Above Use Case	4.04	Above Use Case	\$44	Verified
Fortinet	4.38	Above Use Case	4.26	Above Use Case	\$5	Recommended
Talari Networks	4.37	Above Use Case	4.47	Above Use Case	\$197	Recommended
Versa Networks	4.09	Above Use Case	4.09	Above Use Case	\$77	Verified
VMware	4.27	Above Use Case	4.21	Above Use Case	\$97	Recommended

#5. 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 возникающие потребности клиентов.
- Отмечен как “Challenger” с самым высоким рейтингом **“Completion of Vision”**

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.

Заключение: почему SD-WAN и SD-Branch от 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

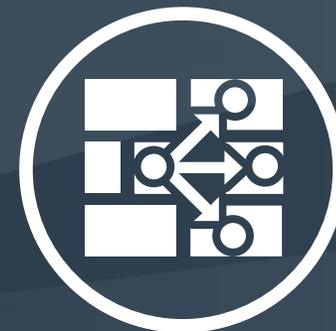


Входит в состав Fortinet Security Fabric: расширение сервисов в филиале



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

FORTINET[®]



SD-WAN



SD-Branch

Спасибо за внимание!