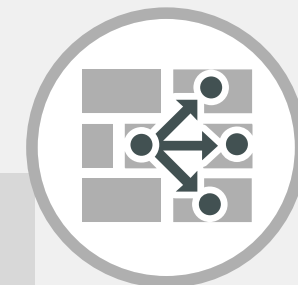




ПРИНЦИПЫ ПОСТРОЕНИЯ И АРХИТЕКТУРА SECURE SD-WAN (V7.0)

Программа мероприятия



SD WAN

Содержание

- 10-00 /10-05 MSK **Вводная информация для участников**
- 10-05 /10-50 MSK
 - Предпосылки к появлению SD-WAN (тренды и вызовы)
 - Обзор решения Fortinet Secure SD-WAN
 - Примеры использования Secure SD-WAN
 - SD-Branch - расширение Secure SD-WAN для филиальных сетей
 - Базовые шаги настройки Secure SD-WAN
- 10-50 /11-00 MSK **Вопросы и ответы**
- 11-00 /15-00 MSK **Лабораторная работа**

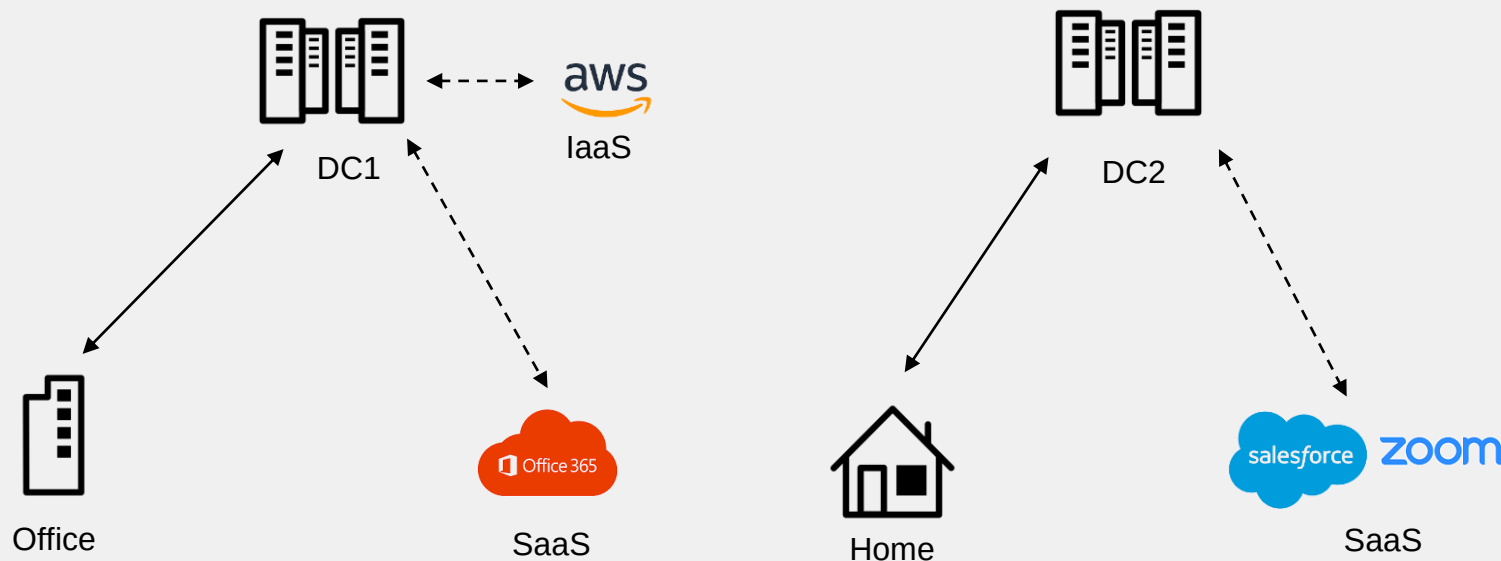




Тренды и вызовы в организации WAN-подключений



Традиционный подход к организации WAN влияет на продуктивность работы пользователей



Гибридная модель работы пользователей (офис / дом / мобильные пользователи)

и отсутствие современной инфраструктуры

Вызовы

- Плохой пользовательский опыт
- Высокие затраты на WAN
- Сложное сопровождение

Тренды в трансформации сетевой инфраструктуры



Управление трафиком на основе IP

Управление трафиком на основе приложений



Реактивные действия

Предиктивная аналитика



Ручное управление

Автоматизированное управление



Работа из офиса

Работа откуда угодно





Обзор решения Fortinet Secure SD-WAN



(Gartner) Что такое SD-WAN ?

Software-Defined WAN (SD-WAN)

Решение **SD-WAN** обеспечивает динамический, определяемый политиками, выбор сетевого пути для приложений среди множества **WAN**-подключений, поддерживающий связывание с дополнительными сервисами, такими как **WAN**-оптимизация и межсетевое экранирование.

SD-WAN provides dynamic, policy-based, application path selection across multiple **WAN** connections and supports service chaining for additional services such as **WAN** optimization and firewalls.

[Definition of Software-Defined WAN - IT Glossary | Gartner](#)



Преимущества использования SD-WAN для бизнеса

01 Улучшение
пользовательского
опыта



Прямой доступ в Internet для бизнес приложений вместо направления трафика через HQ

02 Быстрый возврат
инвестиций (ROI)



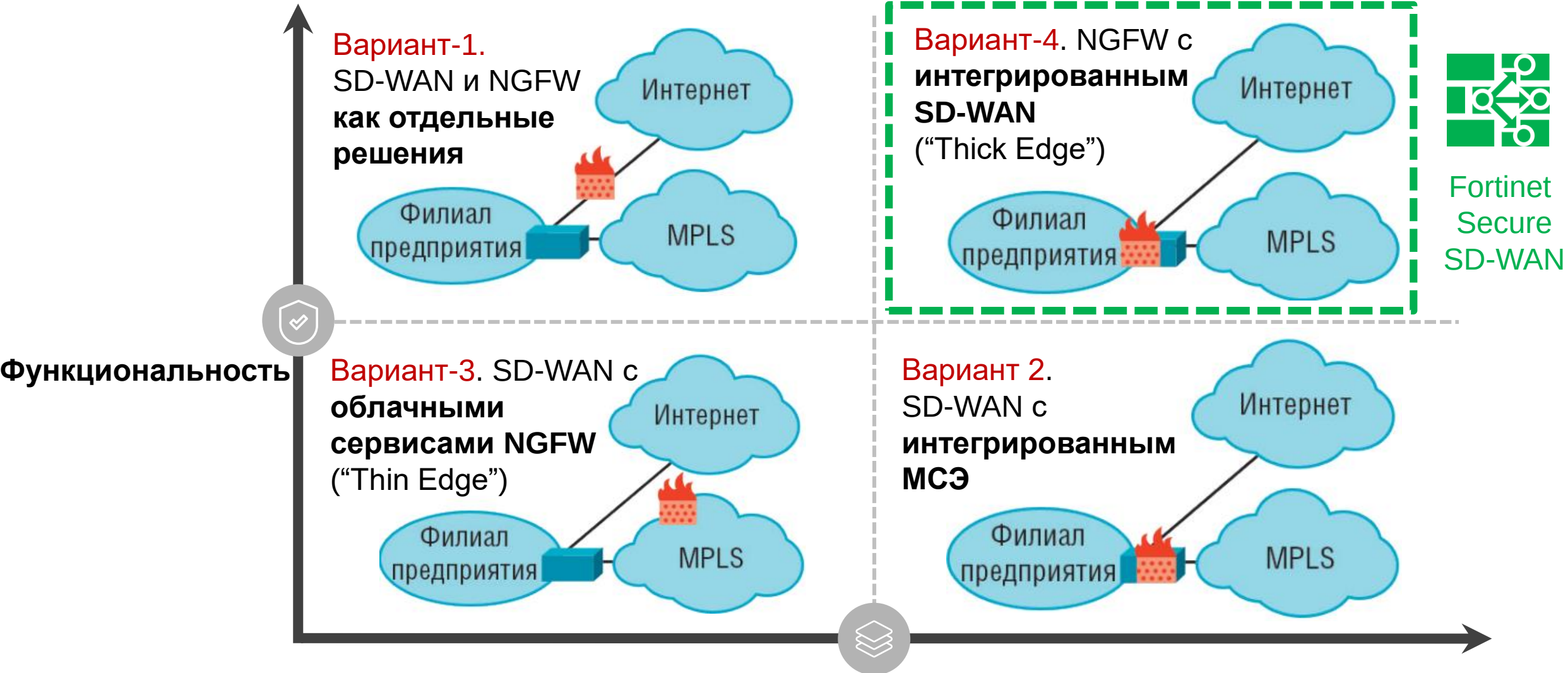
Больше пропускной способности для пользователей, объединение сетевых продуктов и продуктов ИБ

03 Упрощение
управления



Легкость в возможностях масштабируемого управления, автоматизации, видимости и аналитики

(Gartner) Архитектуры безопасности для SD-WAN



Преимущества решения Fortinet Secure SD-WAN

01

Фокус на приложения



Широчайшие возможности идентификации и направления трафика приложений для улучшения пользовательского опыта

02

Высокопроизводительная конвергенция сетевых функций и функций сетевой безопасности



Уникальные в индустрии периметровые устройства, имеющие SD-WAN ASIC с поддержкой расширенной маршрутизации, SD-WAN и NGFW

03

Эффективное управление



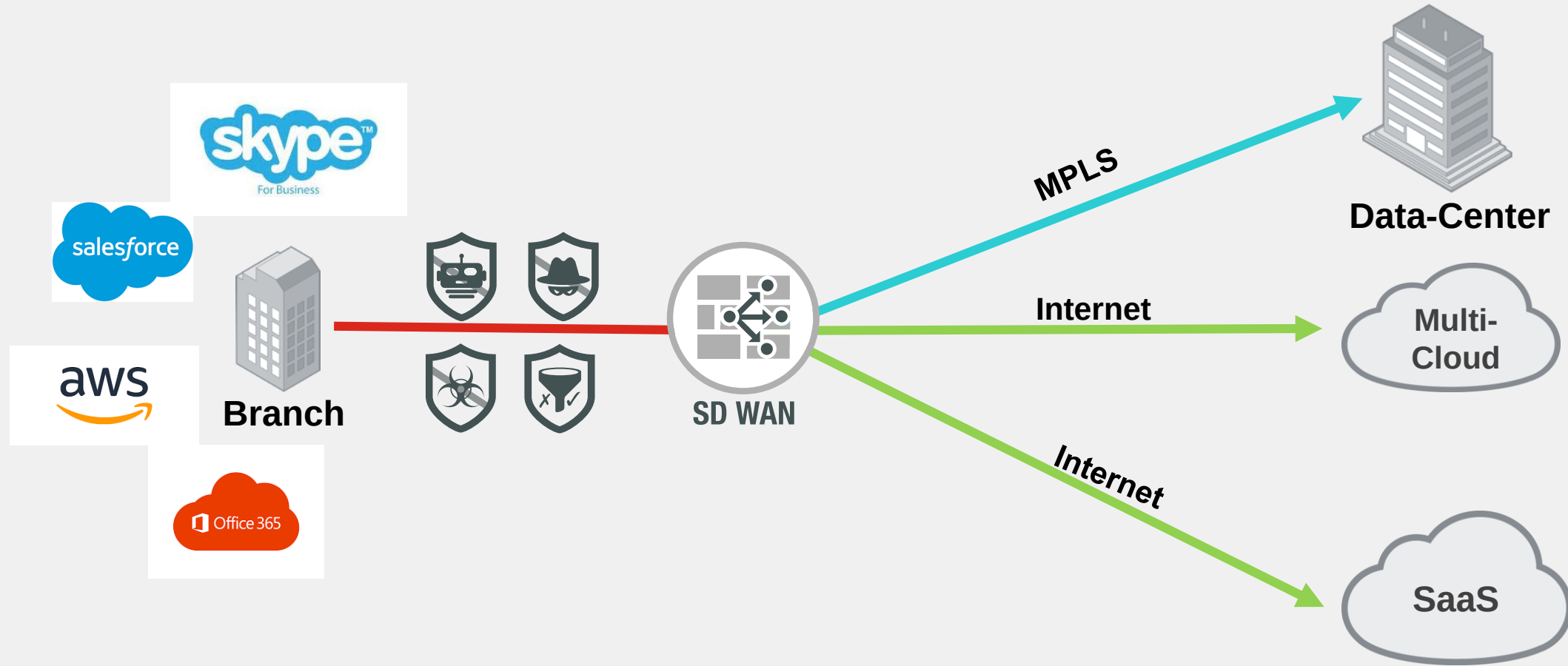
Централизованная оркестрация и аналитика для масштабируемых развертываний SD-WAN и SD-Branch с минимальным участием человека (ZTP)



Компоненты решения Secure SD-WAN



#1. FortiGate NGFW с интегрированным SD-WAN



SD-WAN – это встроенный функционал FortiGate NGFW

#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)

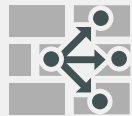


#1 – по количеству устройств безопасности (согласно IDC)

Безопасный SD-WAN

SD-WAN

NGFW



SD-WAN



Traffic Shaping



VPN



App Control



Intrusion Prevention



Antivirus



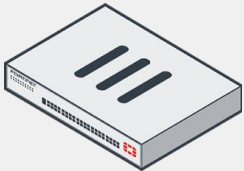
URL Filtering



Sandboxing



SSL Inspection

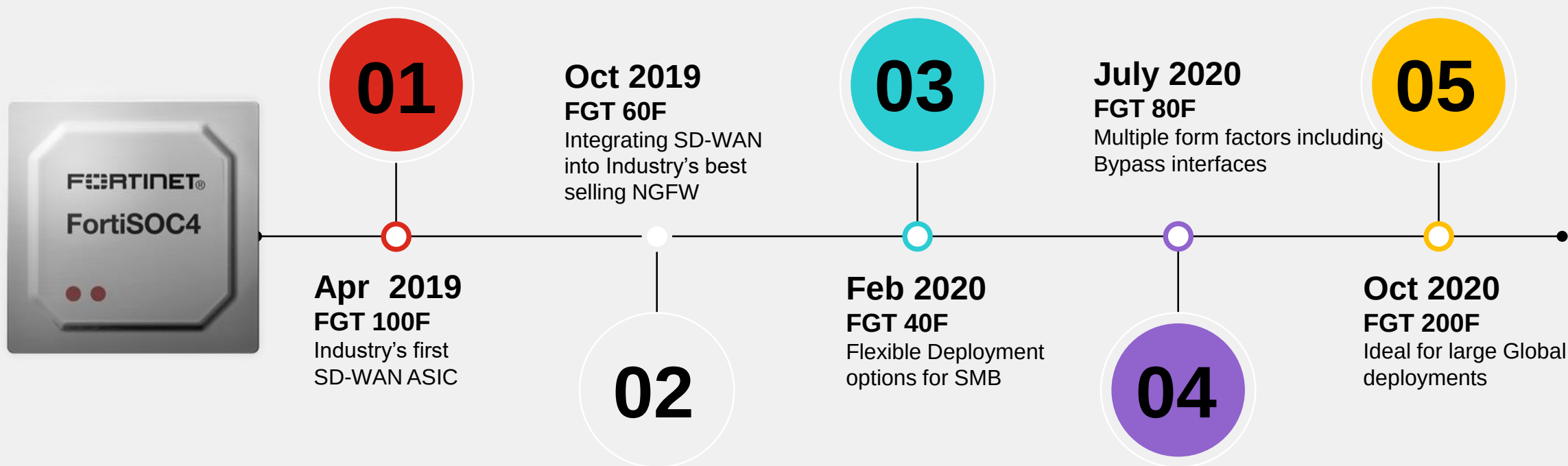


Высокая производительность и масштабируемость

Тесная интеграция решений и расширенная видимость



#1 FortiGate – широкий выбор устройств (SD-WAN ASIC)



Множество
вариантов
исполнения



Встроенный
LTE



Встроенный
Wi-Fi



Встроенный
PoE/PoE+



Встроенный
Bypass



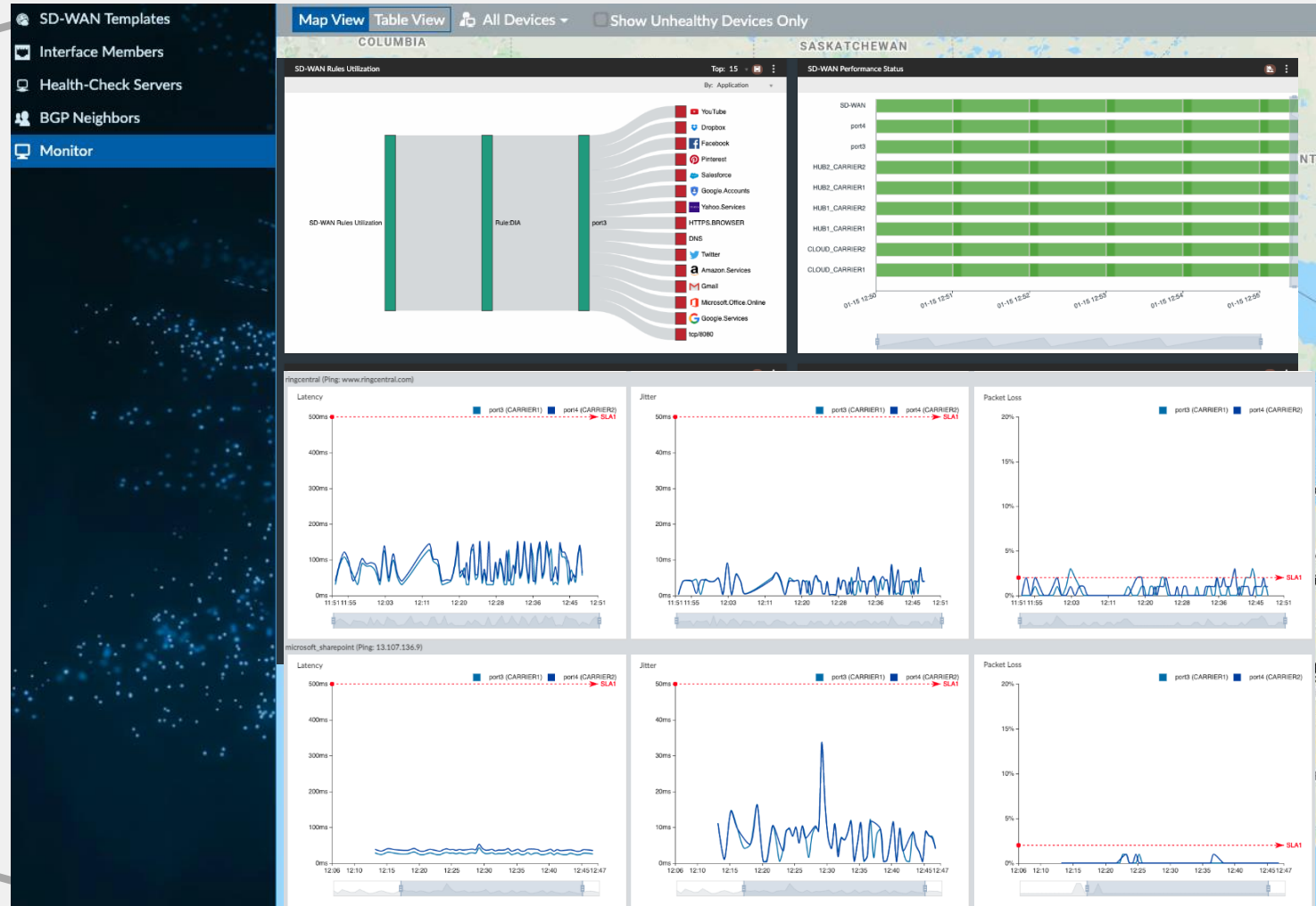
#2 Fabric Management Center (FortiManager, FortiAnalyzer, FortiDeploy)

Унификация NOC + SOC
Dashboard в одном
решении, автоматизация
реагирования

Визуализация и
мониторинг
производительности
сети,
централизованная
конфигурация
и развертывание (ZTP)

Визуализация и
мониторинг
производительности
приложений,
активности
пользователей и
устройств,
сетевой безопасности

Широкие возможности
отчетности и аналитики



SD-WAN от Fortinet (Secure SD-WAN)

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



Примеры использования Fortinet Secure SD-WAN

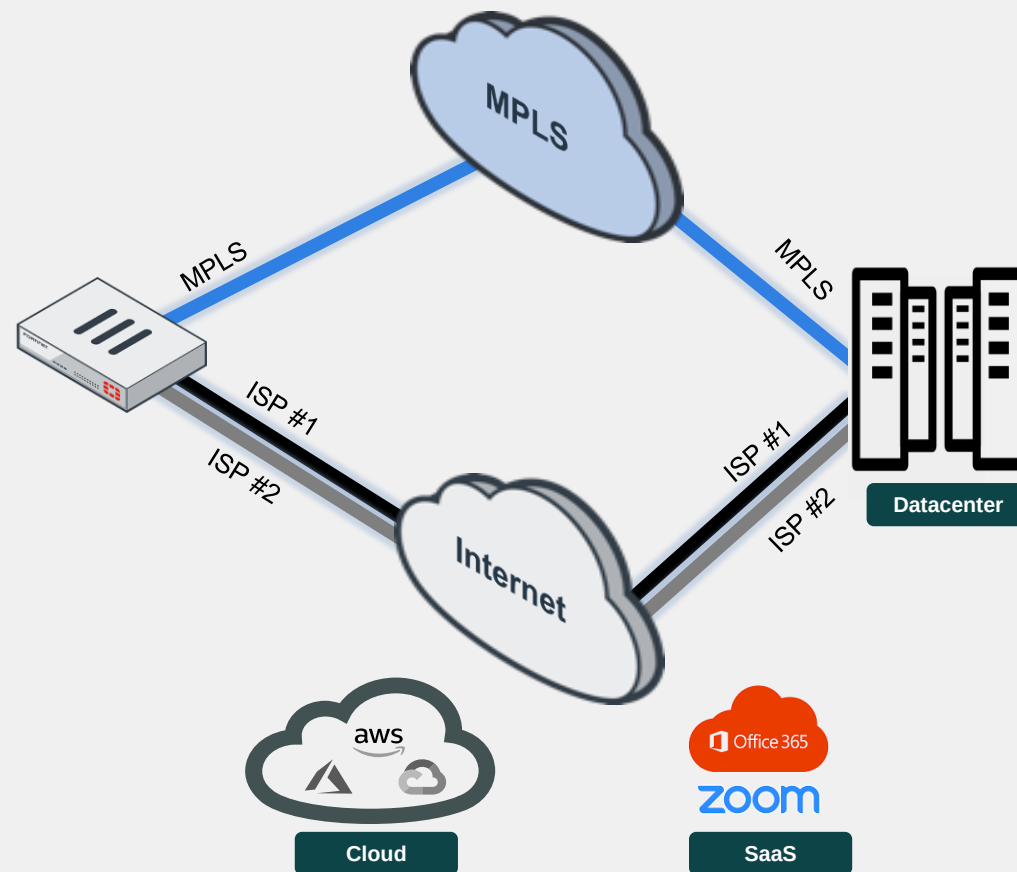


Пример использования SD-WAN #1

Использование множества линков ISP (MPLS, Broadband, LTE)

Улучшить производительность приложений и уменьшить стоимость эксплуатации с использованием широкополосных каналов и LTE для расширения или замены MPLS.

- Направление трафика выбранных приложений позволяет селективно маршрутизировать сетевой трафик через имеющиеся каналы связи
- Мониторинг приложений и каналов с помощью Performance SLA позволяет динамически интеллектуально выбирать сетевой путь для приложения и обеспечивать видимость трафика приложения в сети
- Конвергенция безопасности: SD-WAN zone приводят к упрощению управления политиками, сохраняя единый уровень безопасности для всех членов зоны
- Безопасные оверлеи в публичные и частные облака
- Технология ADVPN улучшает взаимодействие между филиалами и уменьшает требования к устройствам в роли Hub.

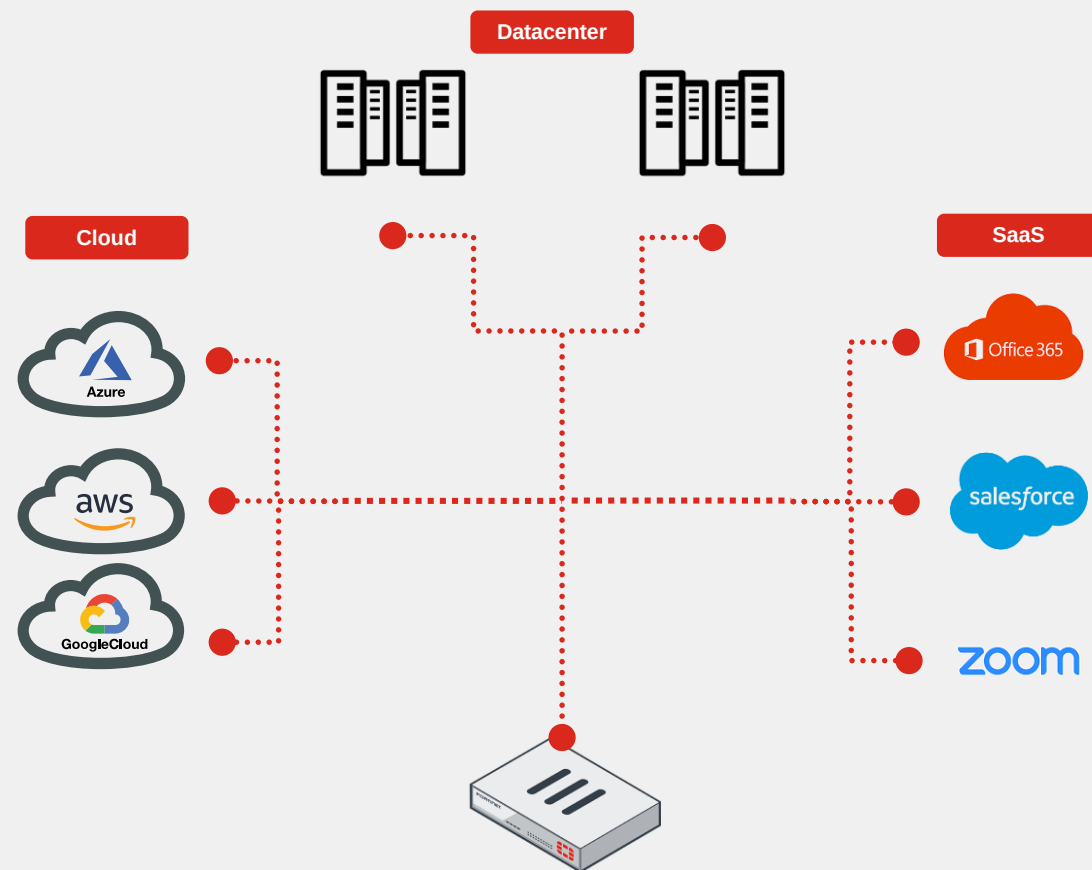


Пример использования SD-WAN #2

Переход к облачной модели использования приложений

Миграция приложений в облака требует подключений multi-cloud и упрощенного развертывания

- Направление трафика приложений к частным и публичным облакам
- Двухсторонняя интеграция в облако с помощью External Fabric Connectors
- Упрощенное подключение к облакам / облачным приложениям из филиалов
- Отказоустойчивость WAN-подключений к SaaS приложениям помощью DIA и RIA (MPLS backhaul)



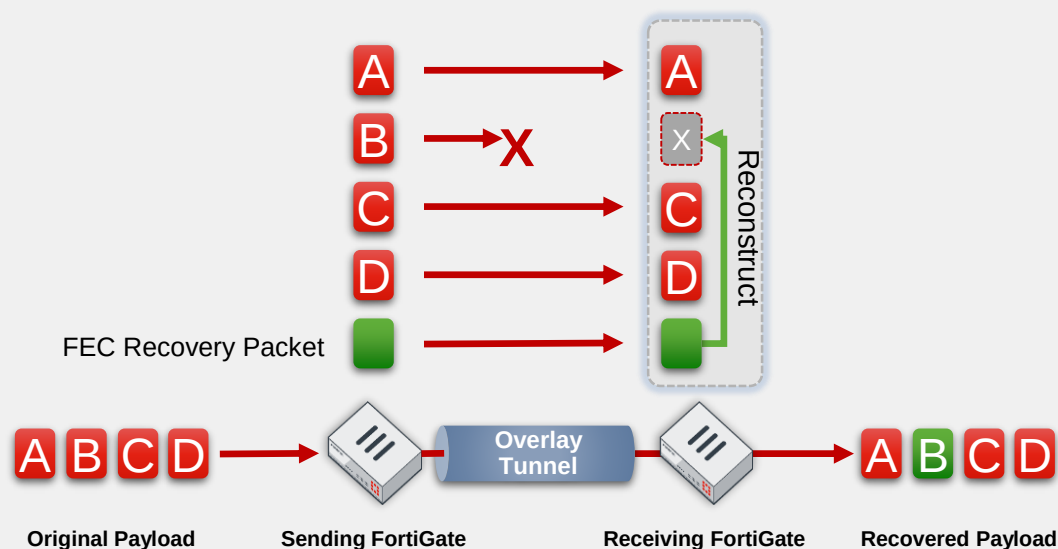
Пример использования SD-WAN #3

Устойчивость работы приложений: WAN Path Remediation

Поддержка устойчивости / выживаемости для бизнес-критичных приложений в случае деградации качества WAN линков

Forward Error Correction (FEC)

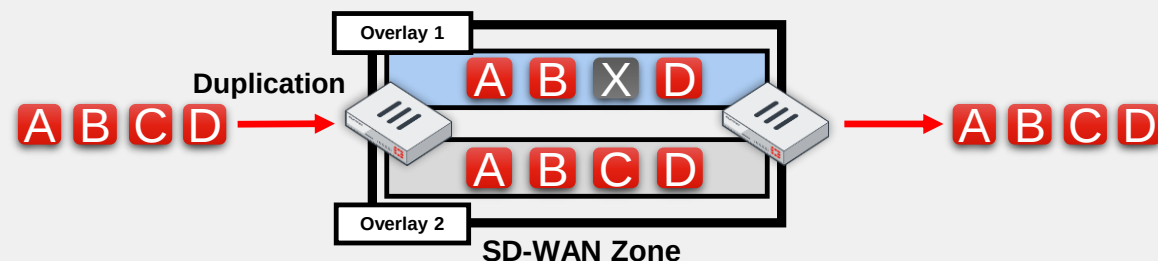
- Enabled per overlay to recover from packet loss on a lossy link



Forward Error Correction (FEC)

Packet Duplication

- Duplicates packets across SDWAN members in a zone to recover from complete packet on a link



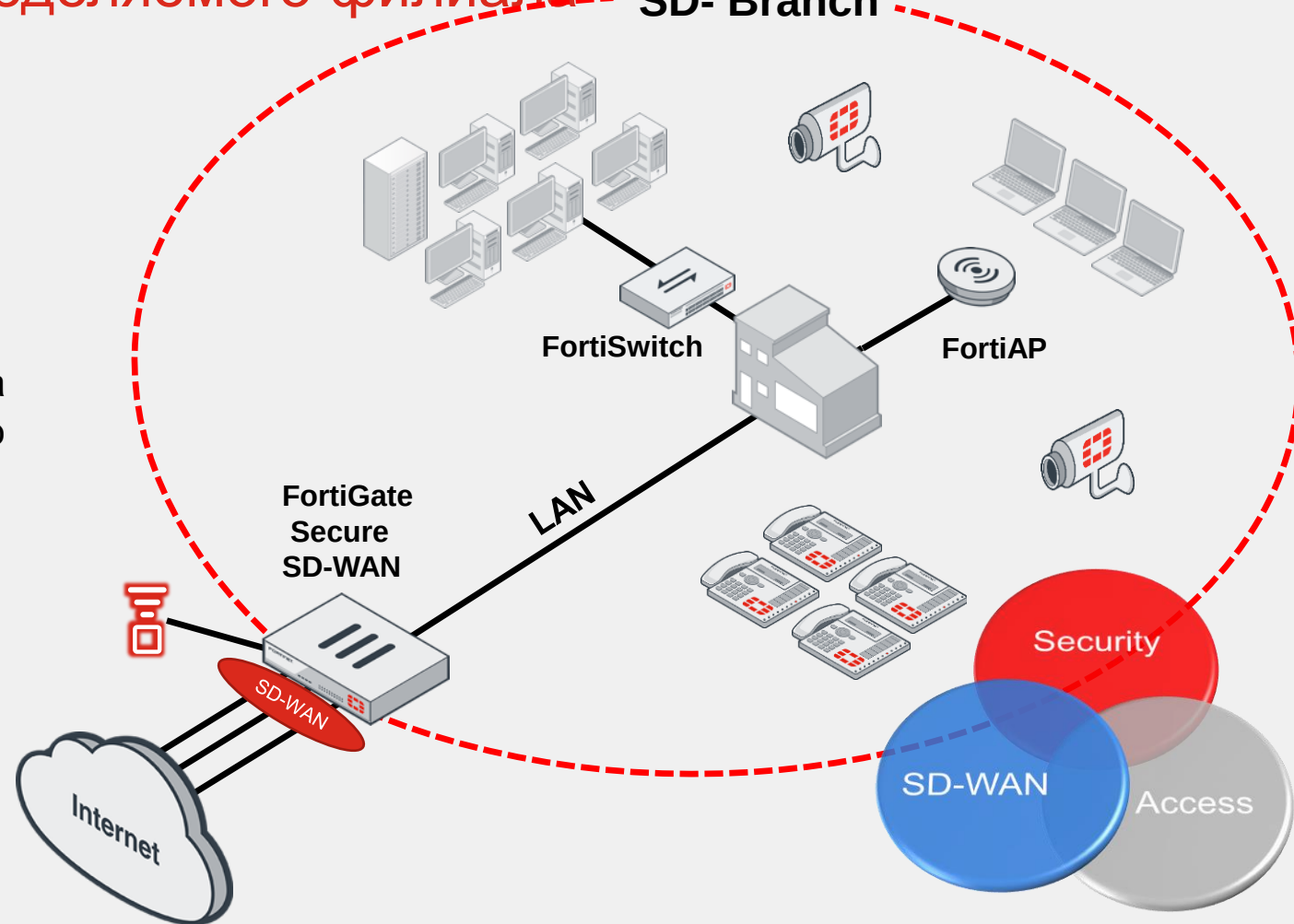
Packet Duplication

Пример использования SD-WAN #4

Инфраструктура программно-определяемого филиала - SD- Branch

Единое окно управления для SD-WAN, сетевой безопасности и уровня доступа (Switch & Wireless)

- Конвергенция SD-WAN, сетевой безопасности и доступа на одной платформе
- Быстрое развертывание инфраструктуры филиала целиком - Zero Touch Provisioning (ZTP) с помощью FortiManager, Ansible Playbook
- Унифицированное решение для филиала
 - Secure SD-WAN
 - Security Inspection
 - Guest Management
 - Network Segmentation
 - Network Access Control
 - User & Entity Behavior Analytics
 - Wired and Wireless
 - Camera, VoIP

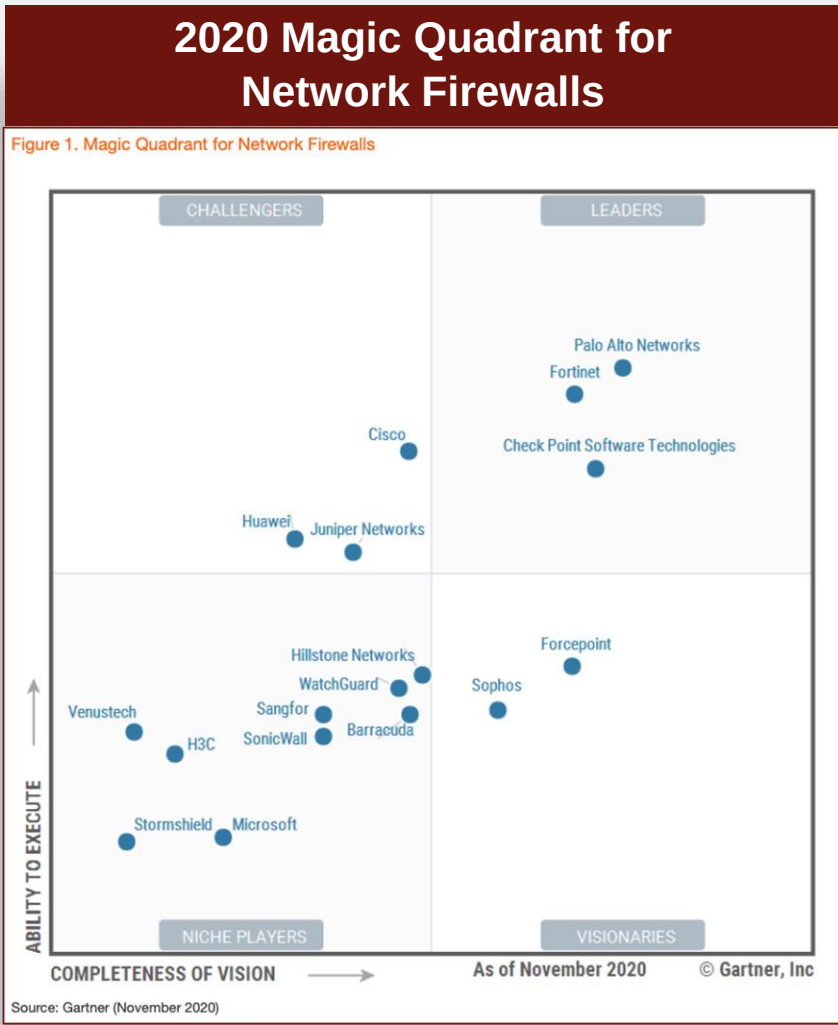




Восприятие индустрией Fortinet Secure SD-WAN



Лидерство Fortinet в безопасности и организации WAN-инфраструктуры !



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.



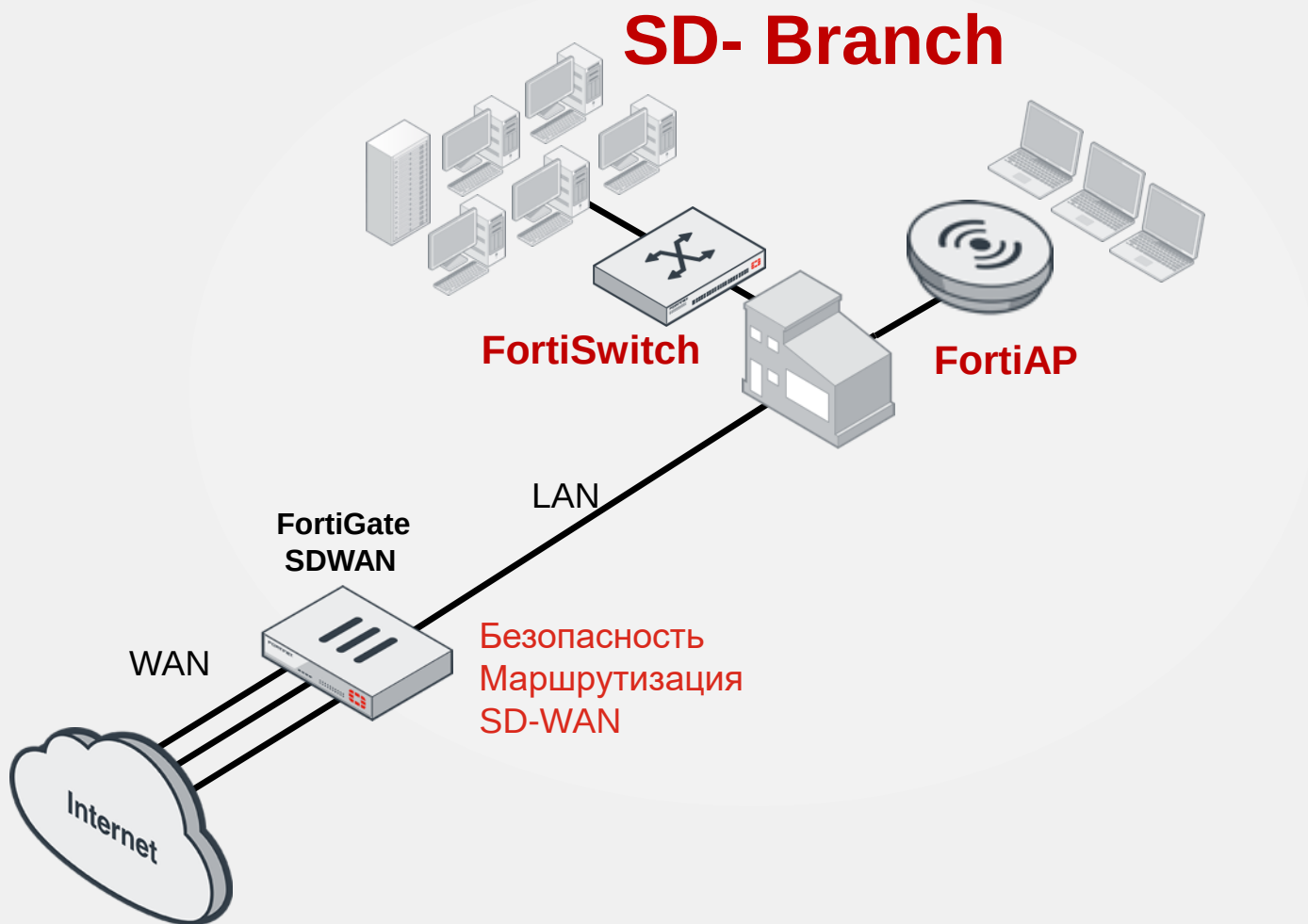


SD-Branch – расширение Secure SD-WAN для филиальных сетей

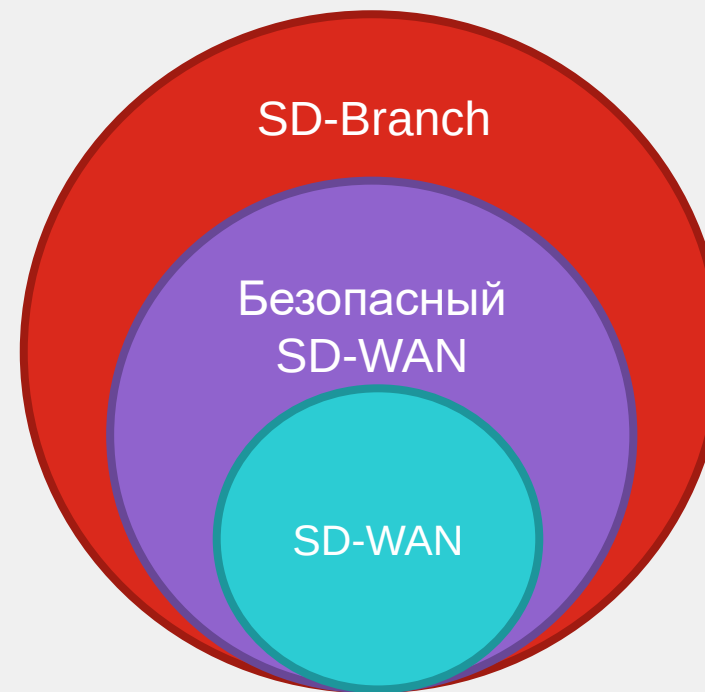


Консолидация сервисов в SD-Branch

Единая консоль управления безопасностью LAN и WAN

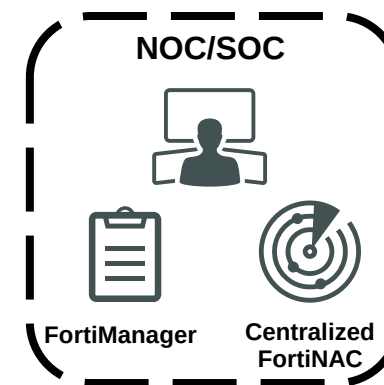
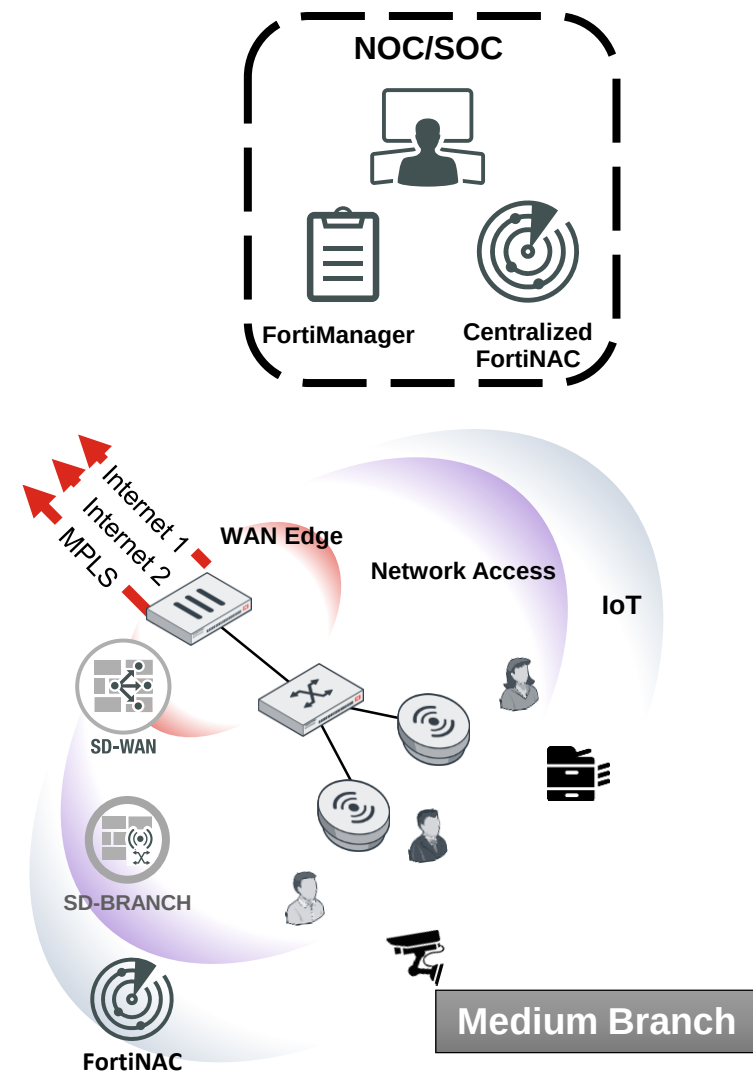
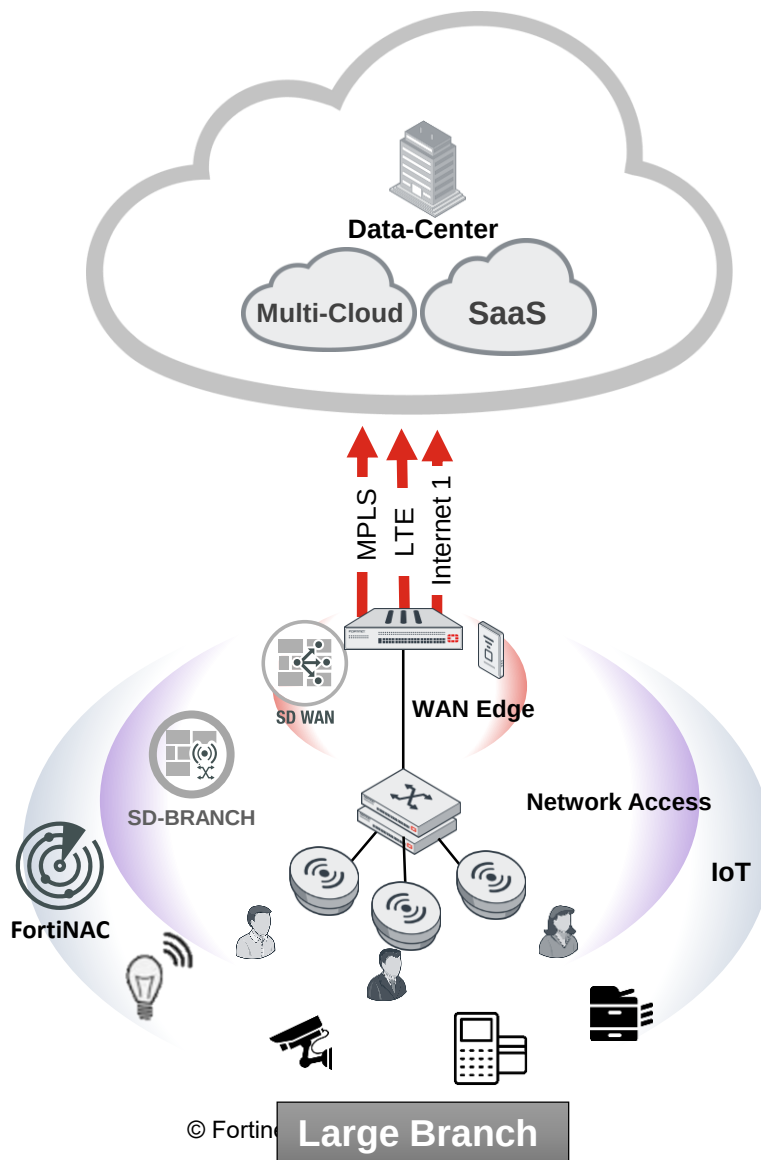
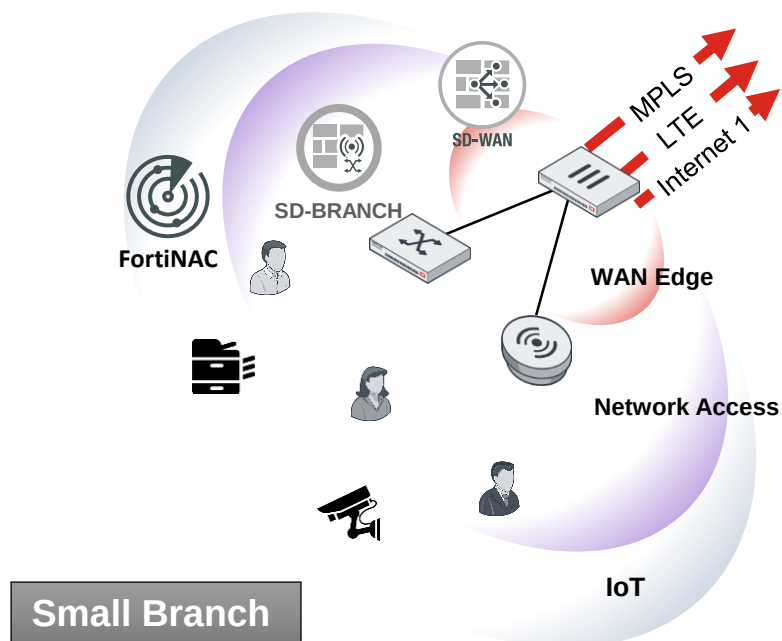


- Fortinet единственный вендор с интегрированными возможностями по управления коммутаторами и точками доступа
- Не требует лицензирования в FortiOS



Secure SD-Branch развёртывание

Упрощенное управление
Комплексная безопасность
Снижение TCO





Базовые шаги настройки Fortinet Secure SD-WAN

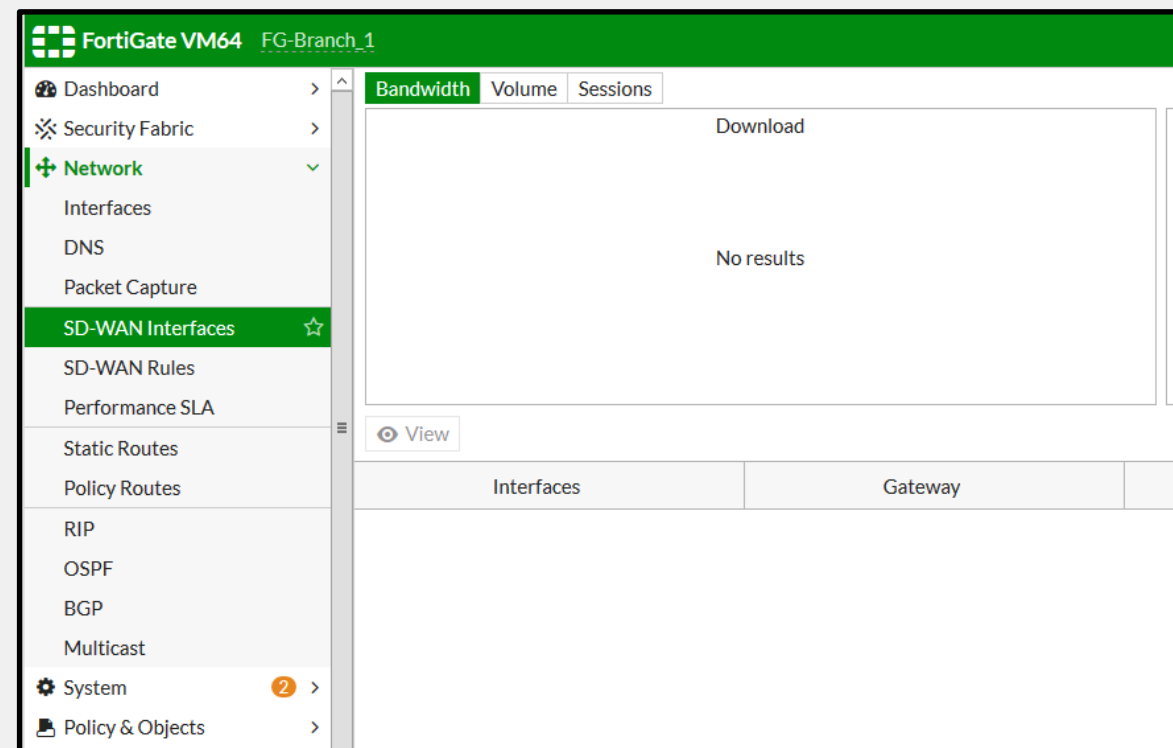


Методы конфигурирования SD-WAN

- **FortiManager (Managed SD-WAN)**
 - Рекомендуемый метод
 - Универсальный комплексный подход для большого количества филиалов
- **FortiManager with SD-WAN Orchestrator**
 - Поддержка с FortiManager 6.4 и выше
 - Специализированный упрощенный подход для большого количества филиалов
- **Local FortiGate (Local SD-WAN Mgmt)**
 - Когда у Вас нет FortiManager
 - Малое количество филиалов (per device management)

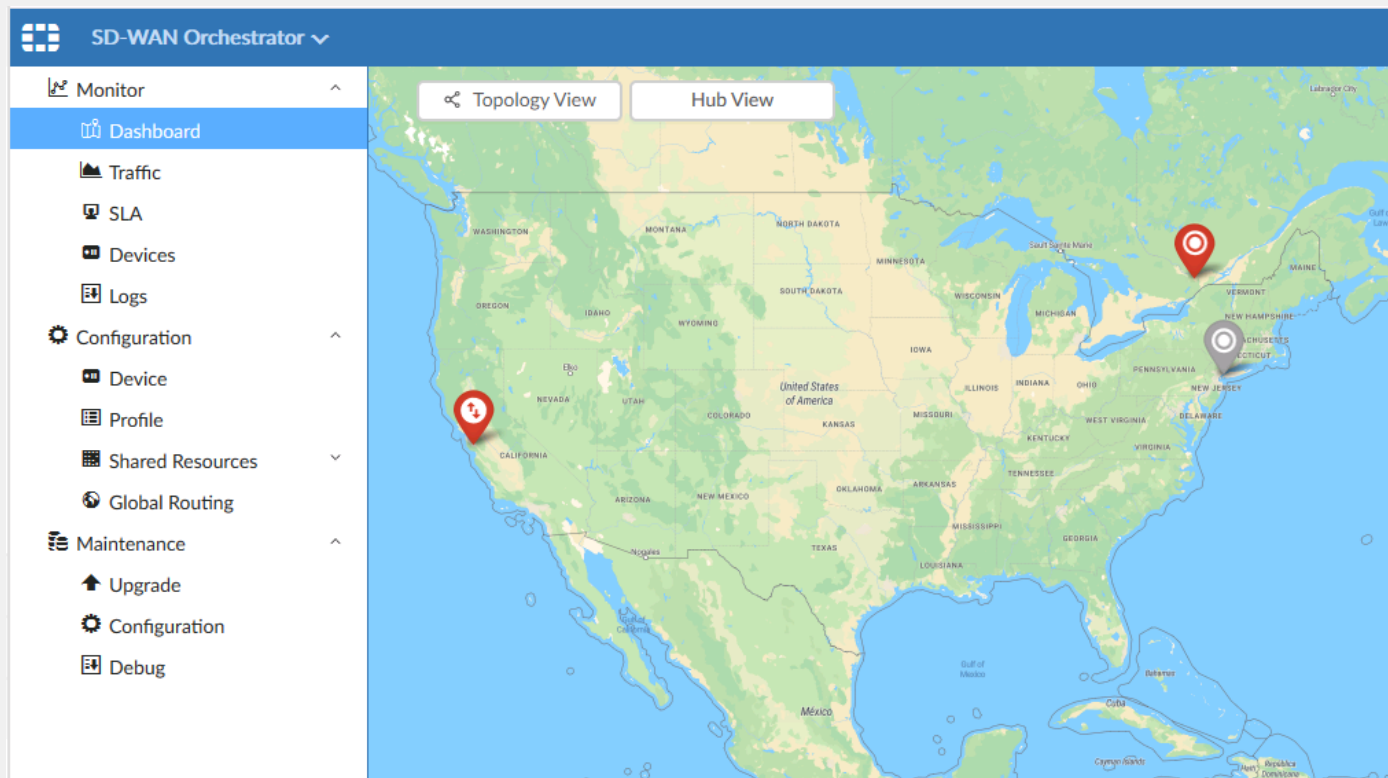
Метод «Local FortiGate (Local SD-WAN Mgmt)»

- Основные шаги:
 - Enable SD-WAN
 - Configure routes
 - Configure security policies
 - Configure performance SLA
 - Configure SD-WAN rules
- Должны быть выполнены на всех устройствах FortiGate индивидуально



Метод «FortiManager with SD-WAN Orchestrator»

- Основные шаги:
 - Configure shared resources
 - Intranet addresses
 - Network
 - SLA
 - System
 - Health threshold
 - Create profiles
 - Add devices



Метод «FortiManager (Managed SD-WAN)»

- Основные шаги:
 - Setup the VPNs
 - VPN Manager > IPsec VPN
 - Configure shared resources
 - Interface members
 - Health-check servers
 - BGP neighbors
 - Input interfaces
 - Create templates
 - Assign templates to devices

The screenshot displays the FortiManager web interface for configuring SD-WAN. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', 'License', 'Provisioning Templates', 'Scripts', and 'SD-WAN'. The left sidebar shows the 'SD-WAN Templates' menu with options for 'Interface Members', 'Health-Check Servers', 'BGP Neighbors', 'Input Interfaces', and 'Monitor'. The main content area is titled 'Create New' and contains the following fields and sections:

- Name:** A text input field containing 'SD-WAN Template'.
- Description:** A large text area for additional details.
- SD-WAN Status:** A toggle switch currently set to 'ON'.
- Interface Members:** A section with a table listing configured interfaces.
- Performance SLA:** A section with a table listing configured SLA entries.

#	ID	Port
1	1	ISP_1
2	2	ISP_2

#	Name	Detect Server	Detect Protocol
1	SLA_1	HealthCheck-Server	Ping

Performance SLA—Link Health Monitor

Create New Performance SLA

Name: SLA_1

IP Version: IPv4

Detect Protocol: Ping

Detect Server: HealthCheck-Server

Participants: All SD-WAN Members Specify

Enable Probe Packets: ON

SLA

+ Create New Edit Clone Delete

ID	Jitter Threshold (Milliseconds)	Latency Threshold (Milliseconds)	Packet Loss
1	5	5	5

Link Status

Interval: 500 Milliseconds

Failure Before Inactive: 5 (max 3600)

Restore Link After: 5 (max 3600)

Ping

DNS

HTTP

Ping

TCP ECHO

TWAMP

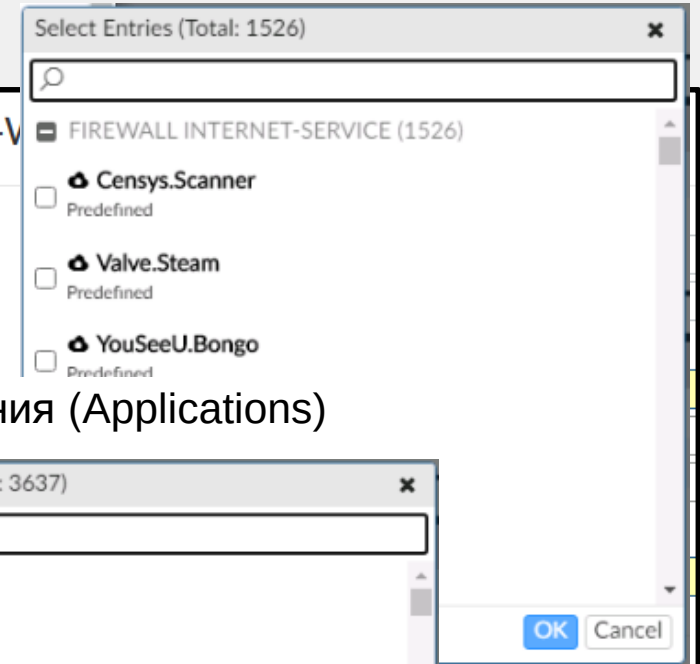
UDP ECHO

- FortiManager link health monitor options:
 - DNS, HTTP, PING, TCP echo, UDP echo, TWAMP
- SD-WAN Orchestrator: Ping, HTTP
- FortiGate: Ping, HTTP
 - CLI: DNS, HTTP, PING, TCP echo, UDP echo, TWAMP

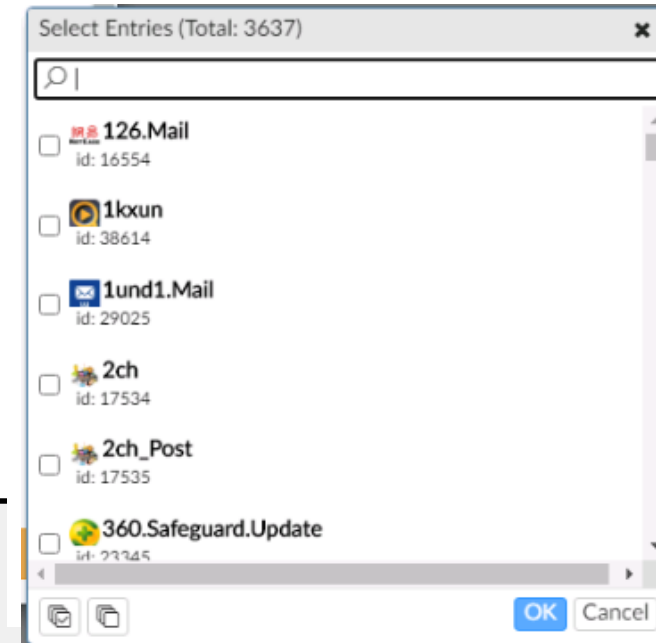
SD-WAN Rules

- Правила могут определять соответствие трафика на основе:
 - Source IP address, destination IP address, or port number
 - Internet services database (ISDB) address object
 - Users or user groups
 - Type of service (ToS)
- Используйте правила для маршрутизации трафика через member interfaces, которые лучше всего соответствуют Вашим потребностям
- Правила могут быть созданы для определенных интернет-служб или приложений

Интернет-службы (Internet Services)



Приложения (Applications)



SD-WAN Rules—Manual

Outgoing Interfaces

Strategy	ManualBest QualityLowest Cost (SLA)Maximize Bandwidth (SLA)
Interface Preference	Click here to select

- Введен в FortiOS 6.2
- Используйте правило Manual, чтобы закрепить одно или несколько приложений на определенном интерфейсе из состава SD-WAN member interfaces

SD-WAN Rules—Best Quality

Outgoing Interfaces

Strategy

ManualBest QualityLowest Cost (SLA)Maximize Bandwidth (SLA)

Interface Preference

ISP_1

ISP_2

2 Entries Selected

Measured SLA

SLA_1

Quality Criteria

Latency

Latency

Jitter

Packet Loss

Inbandwidth

Outbandwidth

Bibandwidth

Custom-profile-1

Custom-Profile-1
Link quality = (a*latency)+(b*jitter)+(c*packet loss)+(d/bandwidth)



SD-WAN Rules—Lowest Cost (SLA)

Outgoing Interfaces

Strategy: Manual Best Quality **Lowest Cost (SLA)** Maximize Bandwidth (SLA)

Interface Preference

Required SLA Target

ISP_1	×
ISP_2	×
2 Entries Selected	

SLA_1#1	×
1 Entry Selected	

- Весь трафик, соответствующий правилу, будет направлен на один интерфейс с наименьшей стоимостью (cost)
- Использует стоимость интерфейса (cost value) из состава SD-WAN member interfaces

SD-WAN Rules—Maximize Bandwidth (SLA)

Outgoing Interfaces

Strategy: Manual | Best Quality | Lowest Cost (SLA) | **Maximize Bandwidth (SLA)**

Interface Preference

Required SLA Target

ISP_1	×
ISP_2	×
2 Entries Selected	

SLA_1#1	×
1 Entry Selected	

- Введен в FortiOS 6.2
- Балансировка нагрузки множества сессий между участвующими интерфейсами из состава SD-WAN member interfaces, которые соответствуют SLA

Заключение:

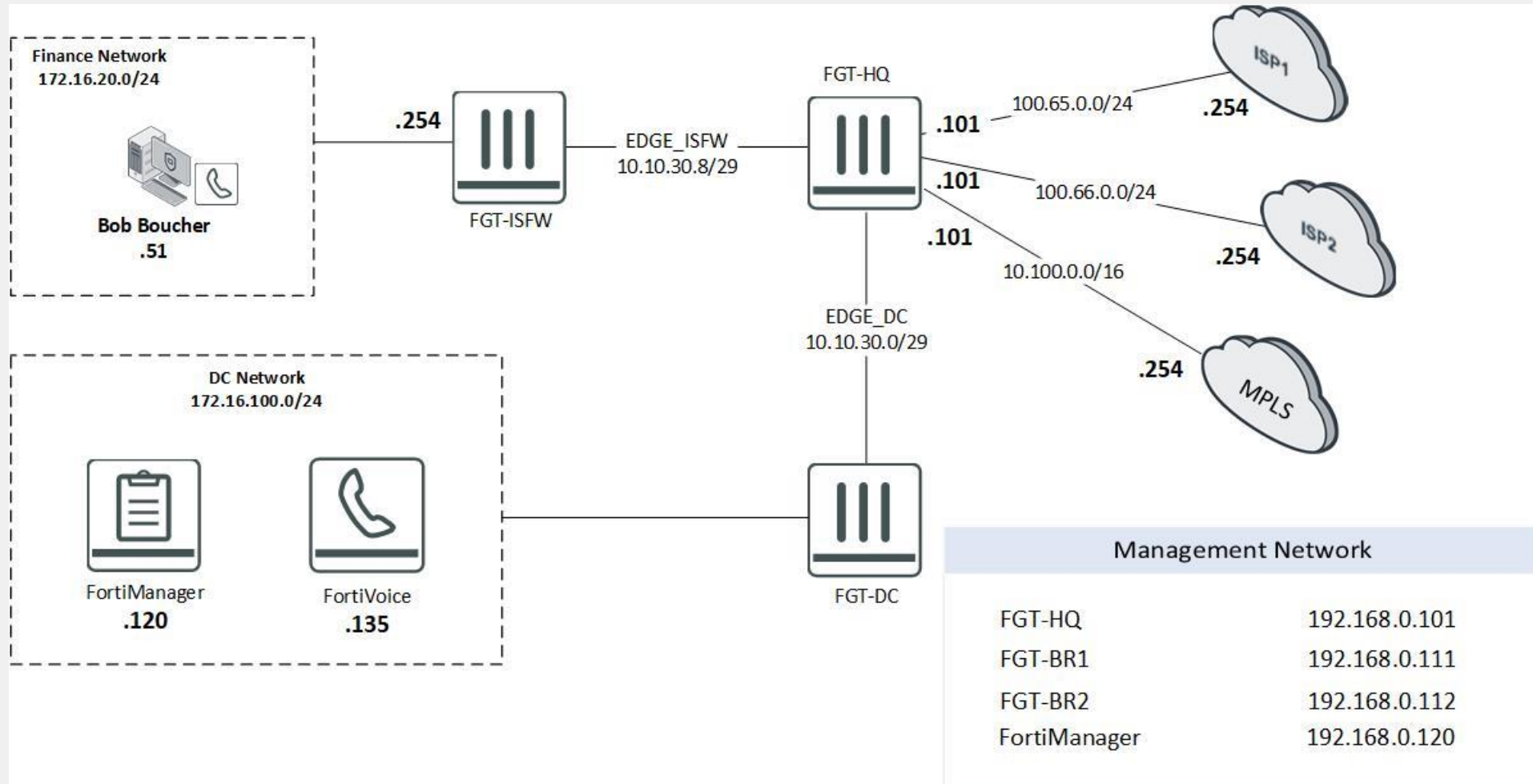
- Заказчики хотят WAN с локальным выходом в Интернет
 - SD-WAN позволяет обеспечить локальный выход в Интернет, но это означает дополнительные риски безопасности
 - Большинство поставщиков SD-WAN не имеют надежной NGFW защиты
 - Многие поставщики SD-WAN рекомендуют несколько устройств для SD-WAN и безопасности
 - Использование нескольких устройств увеличивает сложность и стоимость
- Что нужно Заказчикам, так это Secure SD-WAN
 - Одно устройство отвечает как за безопасность, так и за SD-WAN



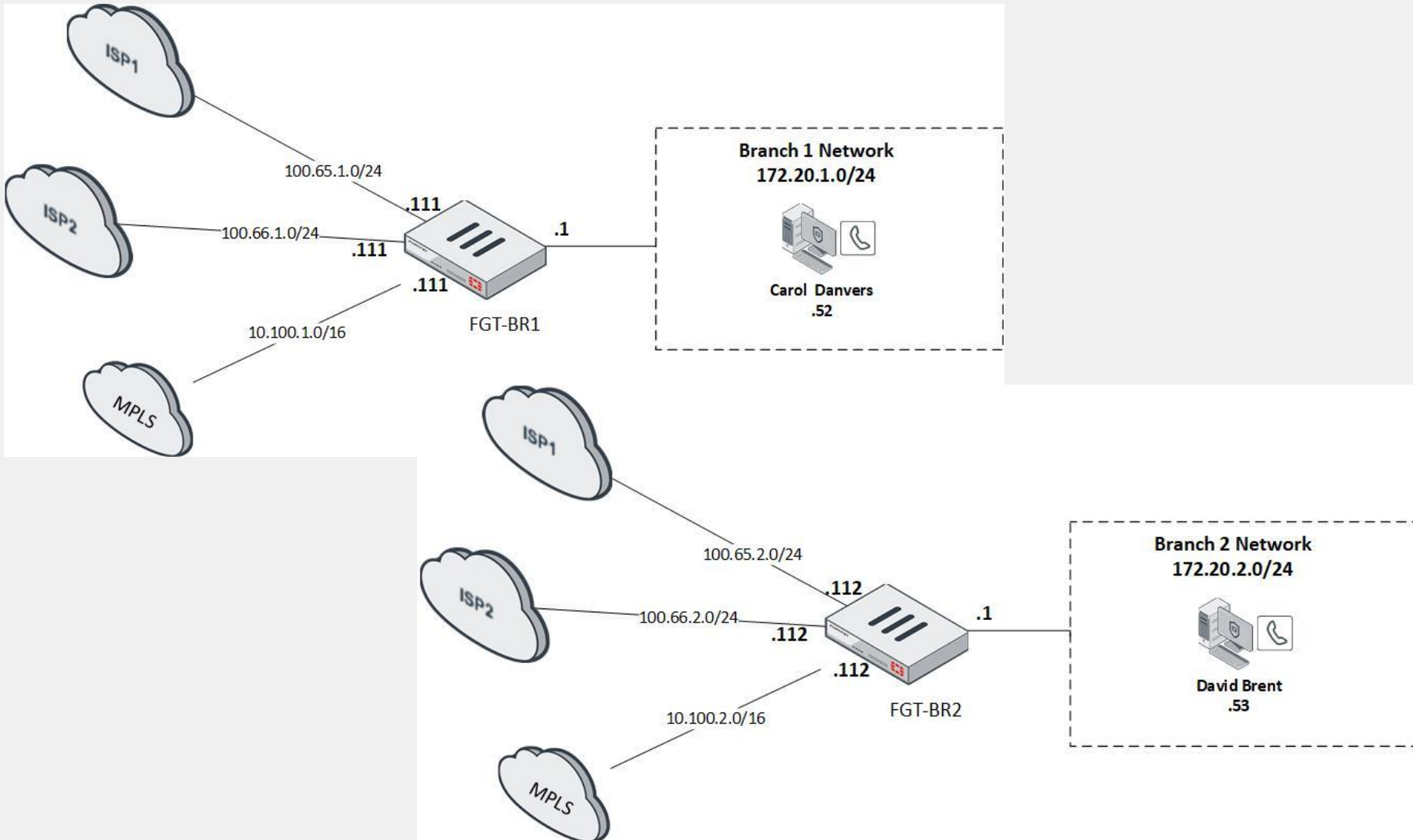
Лабораторная работа «Managed SD-WAN» FMG 7.0, FOS 7.0



Lab—Network Diagram



Lab—Network Diagram





Вопросы ?

Пишите: cis@fortinet.com