



# Построение защищенной инфраструктуры доступа компании

на основе решений Fortinet

Юрий Захаров  
Системный инженер  
[yzakharov@fortinet.com](mailto:yzakharov@fortinet.com)

8 мая 2020

# О чем пойдет речь...

- ✓ Современный уровень доступа – сложности и решения
- ✓ Проводной уровень доступа
  - ❑ Коммутаторы уровня доступа и контроллер коммутаторов в операционной системе FortiOS
- ✓ Беспроводной доступ (Wi-Fi)
  - ❑ FortiGate в роли контроллера беспроводных точек
  - ❑ Режимы работы БЛВС:
    - Tunnel mode
    - Local Bridge mode
    - Local Standalone mode
  - ❑ Построение высокопроизводительных беспроводных сетей на базе контроллера FortiWLC

***“Ваша сеть безопасна настолько, насколько безопасно ваше самое слабое звено”***

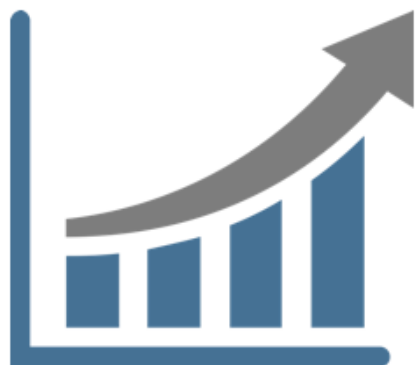


# **Коммутаторы уровня доступа и контроллер коммутаторов**

в операционной системе FortiOS

# Вызовы для уровня доступа

Количество устройств



30 млрд устройств к 2020

Безопасность



Угрозы становятся более продвинутыми

Управление



Возрастают затраты на персонал

# Вызовы для уровня доступа

Количество устройств



Снижается  
производительность

Безопасность



Сложность при интеграции  
с устройствами  
безопасности

Управление



Увеличивается  
время на решение  
инцидентов

# Fortinet Security Fabric

## Комплексная

Обеспечение полной видимости поверхности цифровой атаки для лучшего управления рисками ИБ

## Интегрированная

Уменьшение сложности сопровождения множества разнородных продуктов

## Автоматизированная

Увеличение скорости управления и отклика



# Безопасность уровня доступа компании

## FortiSwitch



### Простое управление

Интеграция с FortiGate создает единый простой GUI интерфейс для управления безопасностью и доступом

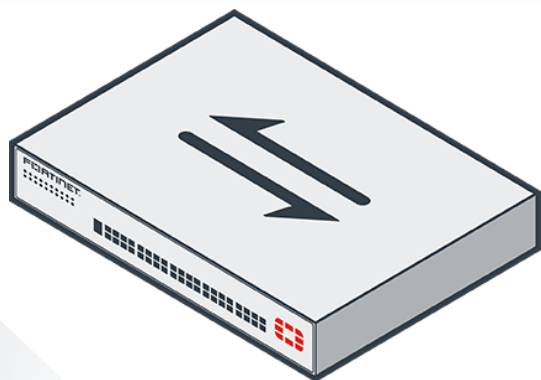
### Интегрированная безопасность

Интеграция с FortiGate делает из коммутатора NGFW экран мирового уровня.

Интеграция с Fortinet Security Fabric расширяет возможности до совокупного набора функций всей фабрики безопасности покрывая все виды угроз

### Масштабируемость

Большая линейка оборудования. Стекирование большого количества коммутаторов. Аппаратная акселерация FortiGate и FortiSwitch коммутационные матрицы без переподписки. Гибкость при установке. Централизованное управление. MCLAG для создания единого шасси из коммутаторов. Встроенная безопасность.



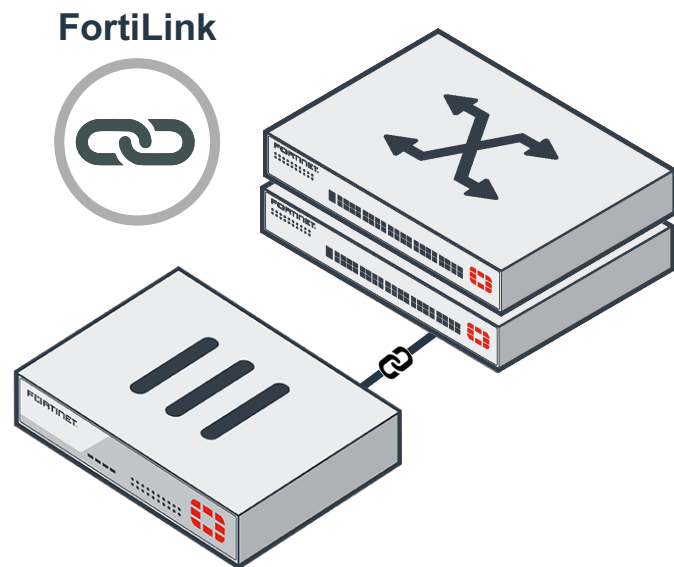


# Варианты развертывания FortiSwitch

## FortiLink

Управляется с FortiGate. Расширение Security Fabric на коммутаторы.

Наиболее распространенная модель развертывания

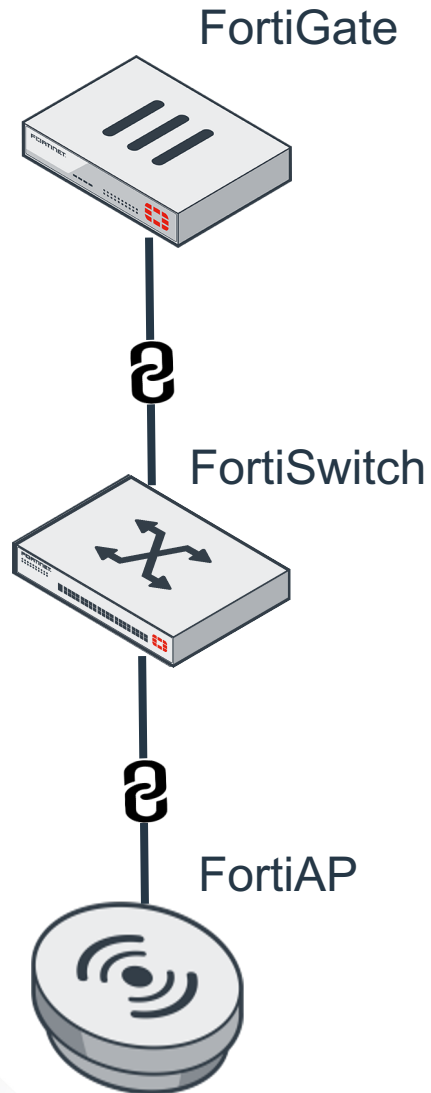


## Stand Alone

Стандартная модель развертывания  
Распространена в средах без FortiGate



# Развертывание и управление сетью с FortiLink



The screenshot shows the FortiGate 300E management interface for a device named 'Demo-ISFW-PRI'. The interface is displayed on a monitor with a keyboard in front of it. The left sidebar contains a navigation menu with the following items: Favorites, Dashboard, Security Fabric (expanded), Physical Topology (selected), Logical Topology, Security Rating, Automation, Settings, Fabric Connectors, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller (highlighted with a red box), Log & Report, and Monitor. The main area displays a network topology diagram. The diagram shows a central 'HA Active-Passive' cluster containing 'Demo-ISFW-PRI' and 'Demo-ISFW-BKP'. This cluster is connected to a 'DISTR-B' switch. From 'DISTR-B', connections lead to several other switches: 'FAC\_ACC\_SW', 'ENG\_ACC\_SW', 'FIN\_ACC\_SW', 'SALES\_ACC\_SW', 'IT\_ACC\_SW', 'Demo-ISFW-ENG', 'Demo-ISFW-FIN', 'Demo-ISFW-SALES', and 'HR\_ACC\_SW'. Additionally, there are connections to 'DISTR-A', 'SALES\_AP', 'FIN\_AP', and 'ENG\_AP'. On the right side, there are two circular nodes representing servers or storage devices, labeled 'FP22E131000882' (39.90 GB) and 'FP22E131000895' (34.34 GB). The interface also includes a search bar, 'Access Device' and 'No Access Device' buttons, 'Device Traffic' dropdown, 'now' time indicator, and a 'Sort By: Bytes (Sent/Received)' dropdown.

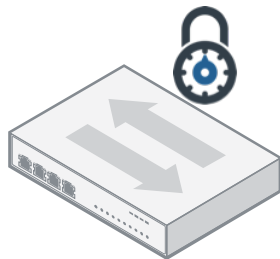
# КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

## ZERO-TOUCH PROVISIONING АВТОМАТИЗАЦИЯ УСТАНОВКИ И НАСТРОЙКИ



- Простое развертывание большого количества коммутаторов
- Централизованное управление
- Автообнаружение и настройка коммутаторов

## БЕЗОПАСНОЕ И ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ



- FortiGate является единой точкой управления
- Централизованное управление VLAN и других функций провизионинга

## ИНТЕГРАЦИЯ КОММУТАТОРОВ С SECURITY FABRIC



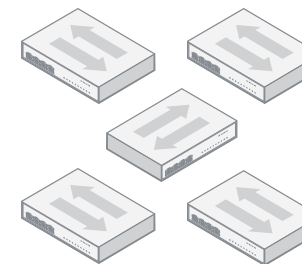
- Обнаружение подключаемых устройств
- Централизованная аутентификация
- Карантин на порту
- Динамическое назначение VLAN
- Логирование процессов

## FORTISWITCH STACK



- Стек FortiSwitch коммутаторов управляемых FortiGate (Single или H-A,A-A)
- MCLAG для коммутации без петель и отказоустойчивости на уровне коммутаторов

## БОЛЬШОЙ МОДЕЛЬНЫЙ РЯД



- Большая линейка FortiSwitch и FortiGate моделей для отраслей:
  - » Ритейл
  - » SMB
  - » Enterprise компаний
  - » Дата-центров
  - » Промышленного сектора

# FortiLink позволяет реализовать безопасный доступ

FortiLink протокол позволяющий FortiGate управлять доступом к сетевой среде

## Простота

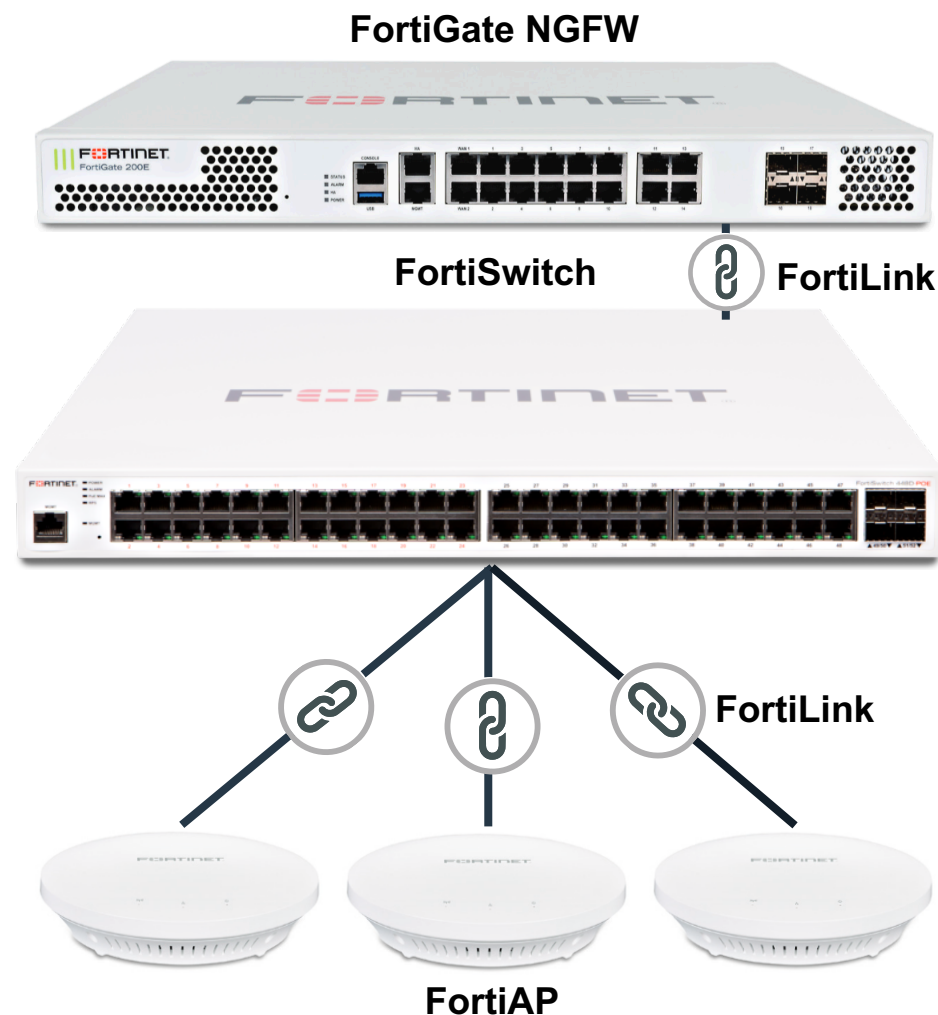
- Гибкая архитектура, масштабирование в соответствии с требованиями
- Прозрачность всего что происходит, аналитика, интеграция с wireless, и безопасность

## Безопасность

- Порты NGFW и коммутатора предоставляют одинаковый уровень безопасности, SSID напрямую связан с политиками NGFW
- Глобальные политики безопасности применяются к проводной и беспроводной среде

## Низкая стоимость владения

- Управление доступом включает SD-Branch. Не требует лицензирования.



# FortiSwitch Access Switch Family

## Коммутаторы начального уровня

### 100 Серия

- Коммутаторы начального уровня
- От 8 до 48 гигабитных Ethernet портов, POE/POE+ коммутаторы
- Desktopные или для установки в стойку
- (2-4) Гигабитных Ethernet SFP uplink порта



## Коммутаторы среднего уровня

### 200 Серия

- Коммутаторы среднего уровня
- От 24 до 48 гигабитных Ethernet порта с POE+
- Для установки в стойку
- (4) Гигабитных Ethernet SFP uplink порта



## Продвинутые коммутаторы

### 400 Серия

- Enterprise коммутаторы
- От 24 до 48 гигабитных Ethernet порта с POE+
- Высокая пропускная способность.
- До (4) 10 Гигабитных Ethernet SFP порта



FortiSwitch 424D-FPOE



FortiSwitch 448D-FPOE

## Уровень агрегации

### 500 Серия

- Коммутаторы агрегации
- От 24 до 48 гигабитных Ethernet портов с POE+
- До (4) 10 Гигабитных Ethernet или (2) x 40 Гигабитных Ethernet SFP uplink портов



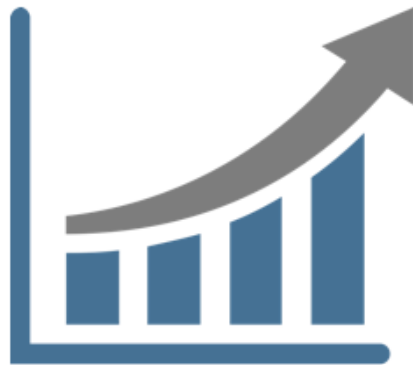
FortiSwitch 524D-FPOE



FortiSwitch 548D-FPOE

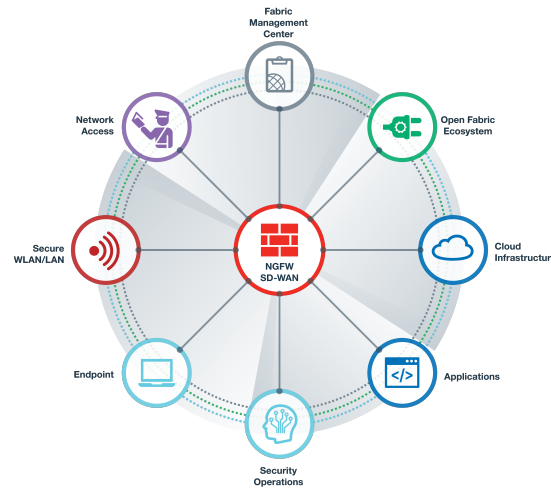
# В результате

Количество устройств



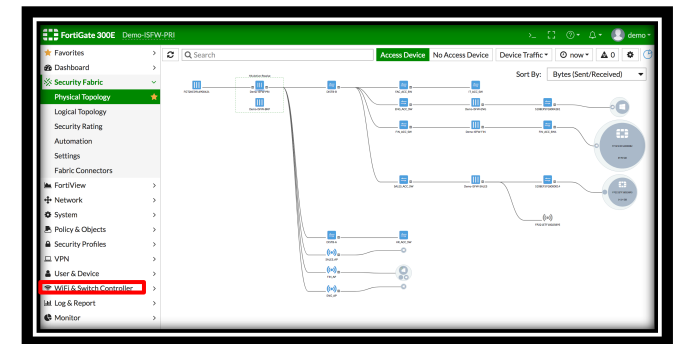
FortiSwitch – масштабируемое решение

Безопасность



Fortinet Security Fabric выявляет и блокирует угрозы

Управление



Единая консоль для управления МСЭ, коммутаторами и сетями Wi-Fi

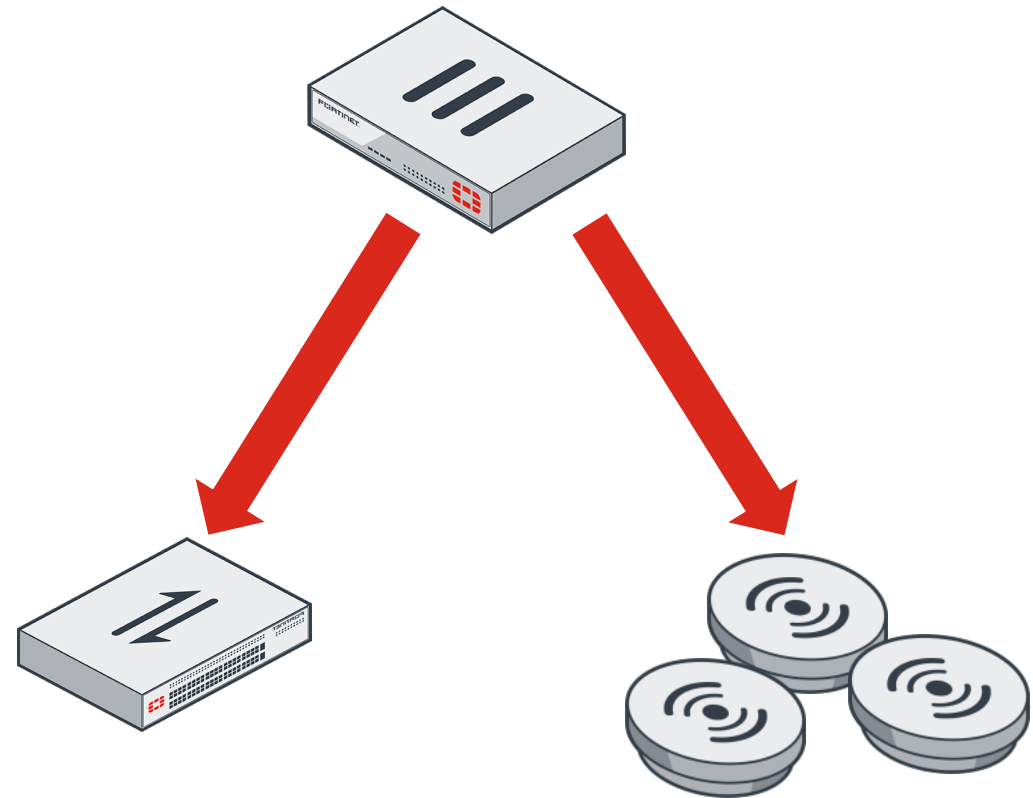
# Security Driven Networking

- Security Driven Networking объединяет безопасность и сетевые функции
- Сетевой уровень доступа создается со встроенными функциями безопасности
- Подобная архитектура более эффективна в части защиты и одновременно – простая в повседневной эксплуатации



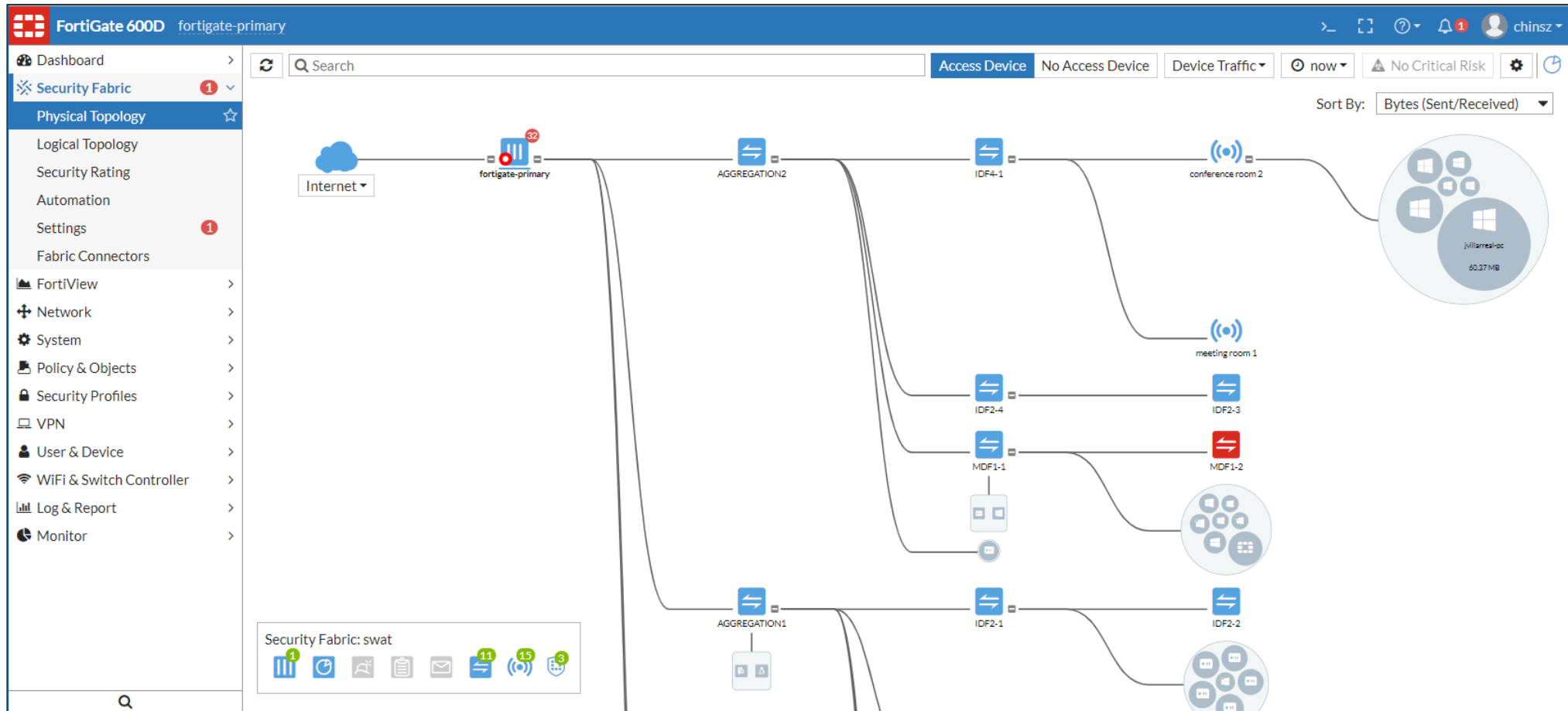
# Security Driven Networking

- Security Driven Networking объединяет безопасность и сетевые функции
- Сетевой уровень доступа создается со встроенными функциями безопасности
- Подобная архитектура более эффективна в части защиты и одновременно – простая в повседневной эксплуатации





# Расширение Security Fabric до уровня доступа



# Уровень доступа Fortinet

Расширенные функции безопасности на уровне доступа

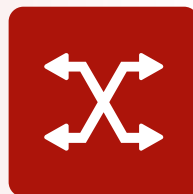
Большинству продуктов уровня доступа не хватает интеграции с решениями безопасности и управления. Защитные функции FortiGate могут быть расширены на сеть доступа



FortiGate



FortiAP



FortiSwitch

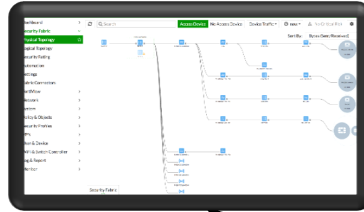
- Расширяет безопасность до уровня доступа
- Упрощает повседневные операции
- Решение SD-Branch



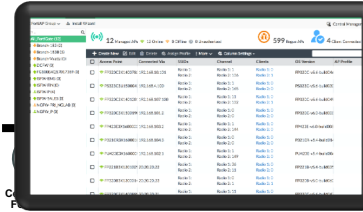
# Secure Access Solution

## Management and Analytics

FortiGate



FortiManager



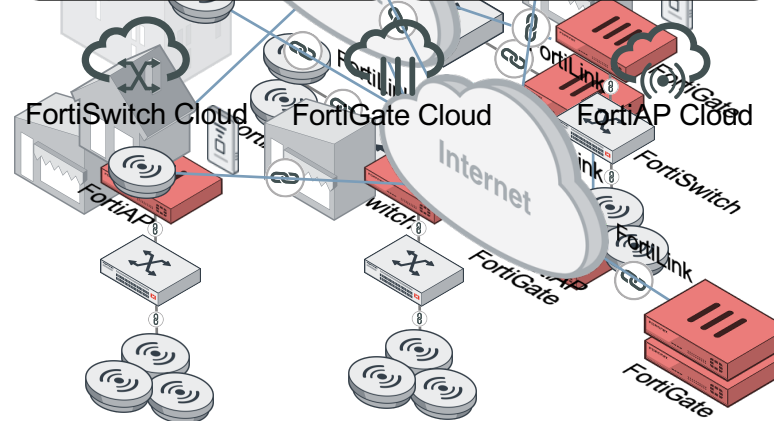
FortiPresence



FortiWLM



Campus



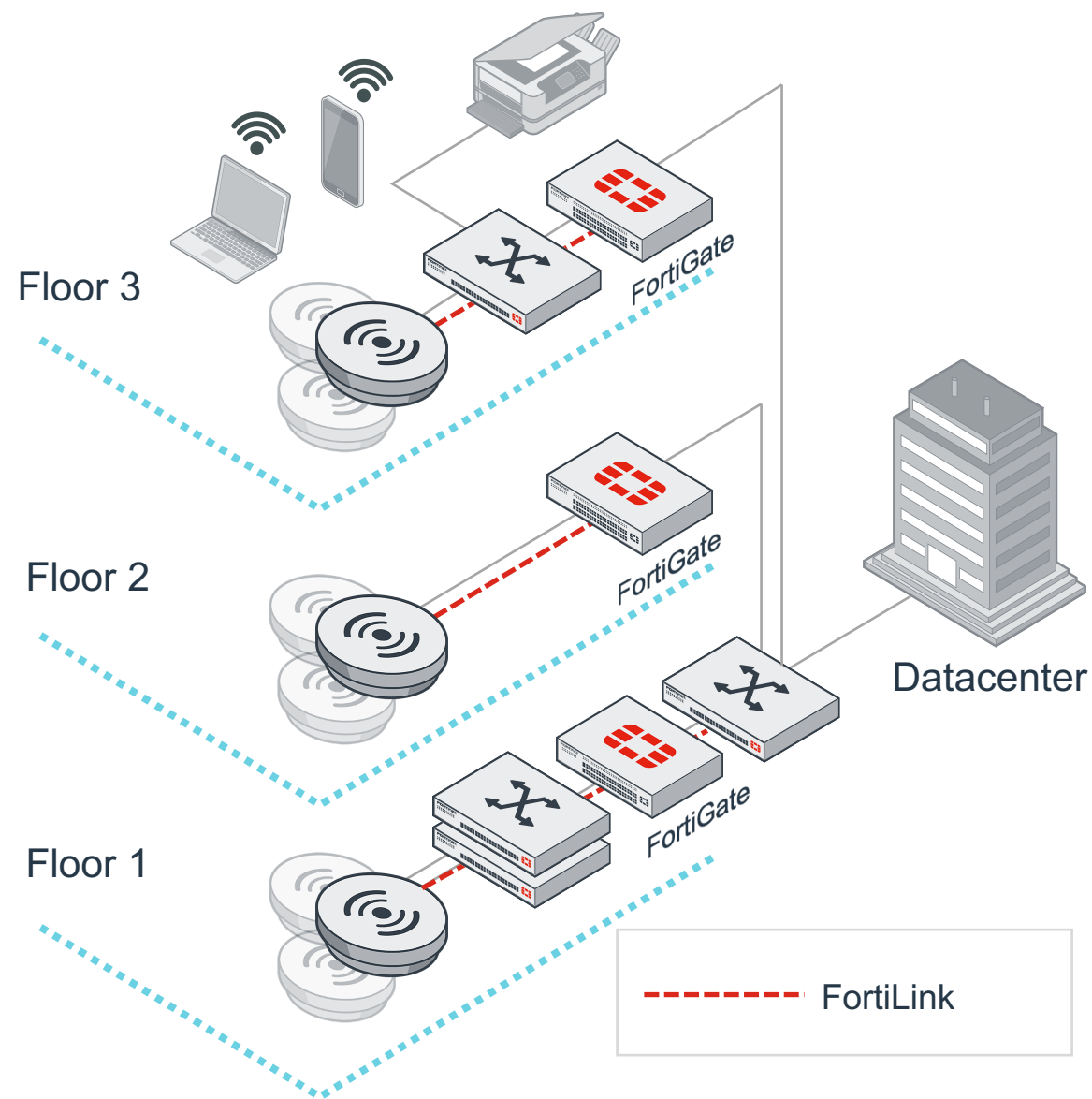
SD-Branch

Teleworker

# Сценарии применения

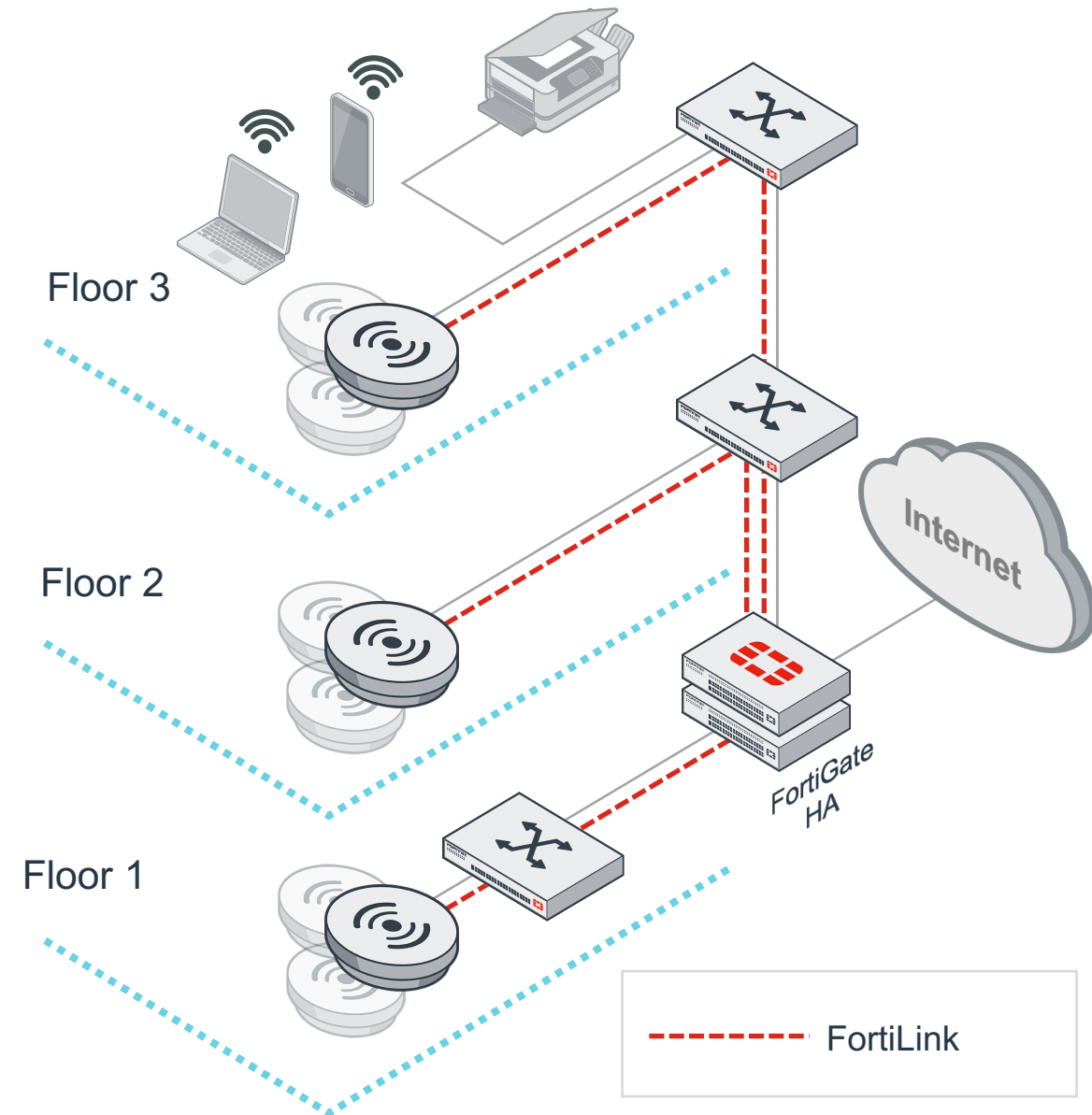
# Кампусная сеть

- МСЭ FortiGate выполняют функции внутренней сегментации, а также управляют уровнем доступа в своей зоне
- Дополнительные FortiGates размещаются в ЦОД в роли DCFW
- FortiManager / FortiAnalyzer используются как инструмент NOC/SOC для централизованного управления всей инфраструктурой



# Кампусная сеть

- Централизованный контроль уровня доступа обеспечивает кластер FortiGate
- Дополнительные FortiGate могут быть установлены для внутренней сегментации



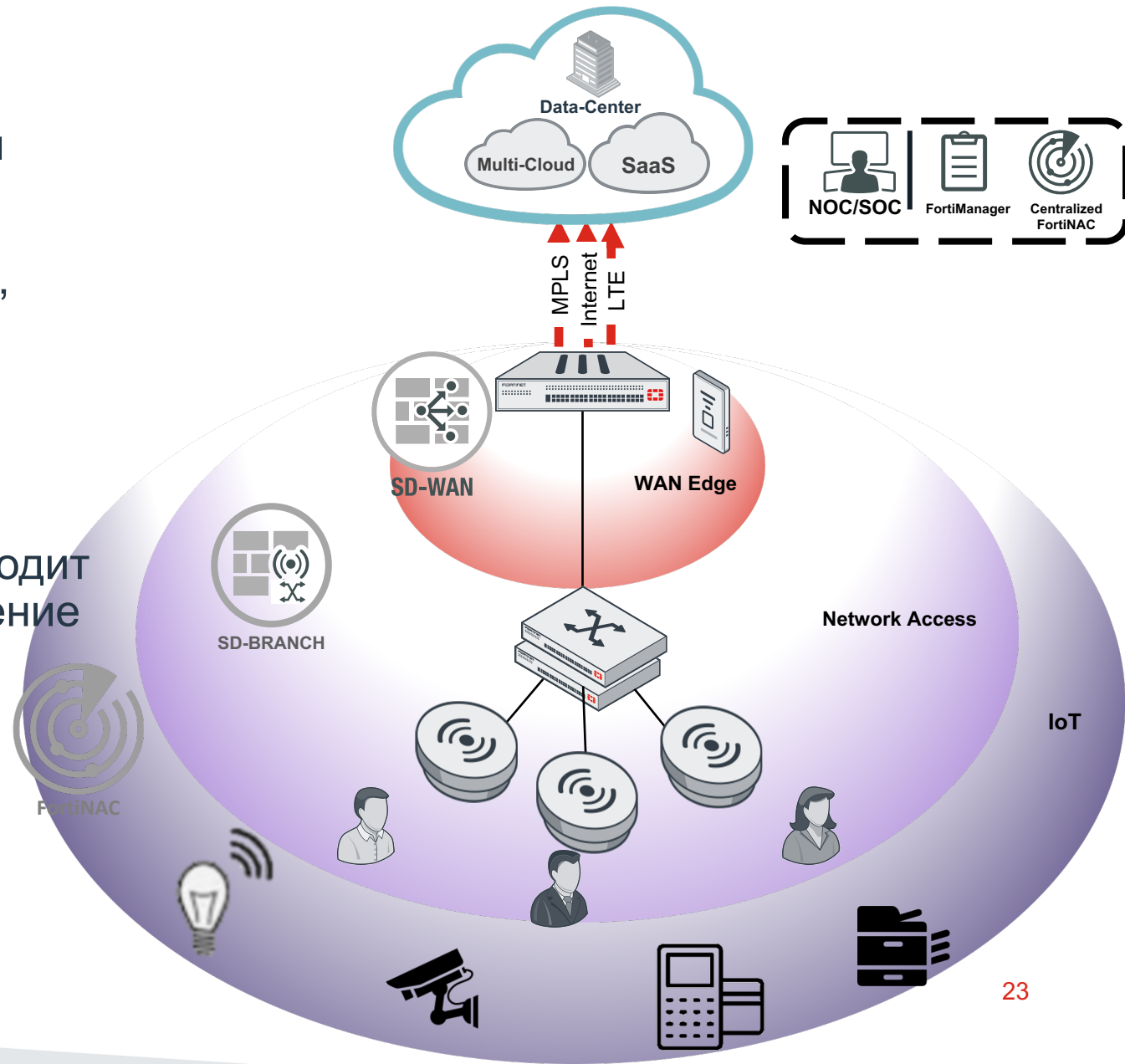
# Интеллект на уровне контроля доступа

## Преимущества от интеграции

**Безопасный доступ** – интеллектуальный контроль на уровне доступа

- Видимость больше (инспекция SSL/TLS, SSH).
- FortiSwitch и FortiAP интегрированы в FortiGate как расширения NGFW - безопасность
- Уникальная архитектура идеально подходит для SD-филиала, deployments - управление
- **NGFW, EMS,**
- **NAC, FortiDeceptor,**
- **FAC, SIEM,**
- **FAZ, FortiWeb,**
- **FSA, FortiMail и т.д**

**FORTINET**

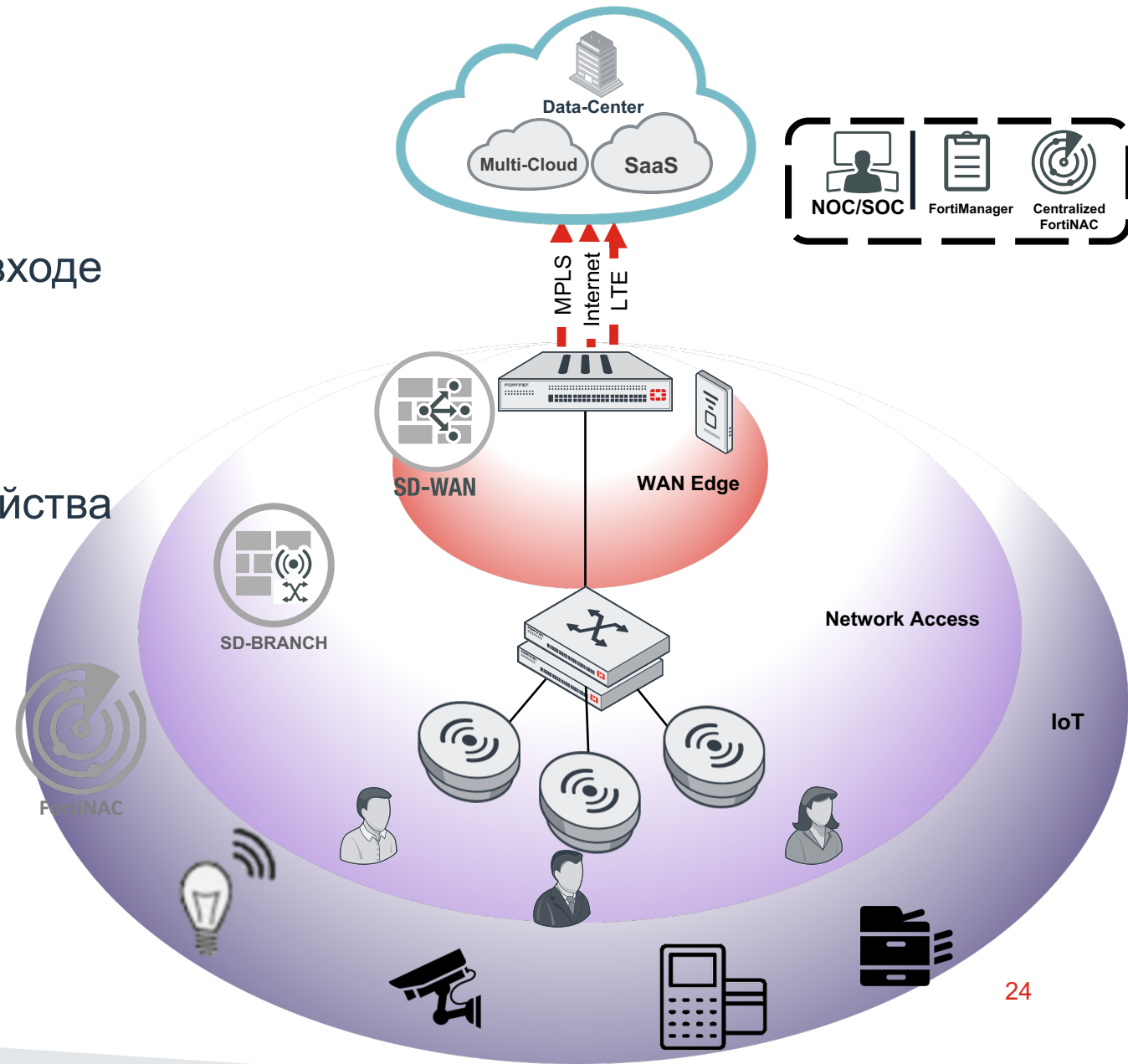


# Интеллект на уровне контроля доступа

## Пример: FortiNAC

### FortiNAC защиты на уровне устройств

- Обнаружение, классификация, контроль, профилирование, оценка состояния при входе устройств в сеть
- Увеличение видимости и обнаружение аномалий
- FortiGate как сенсор, не нужны доп. устройства

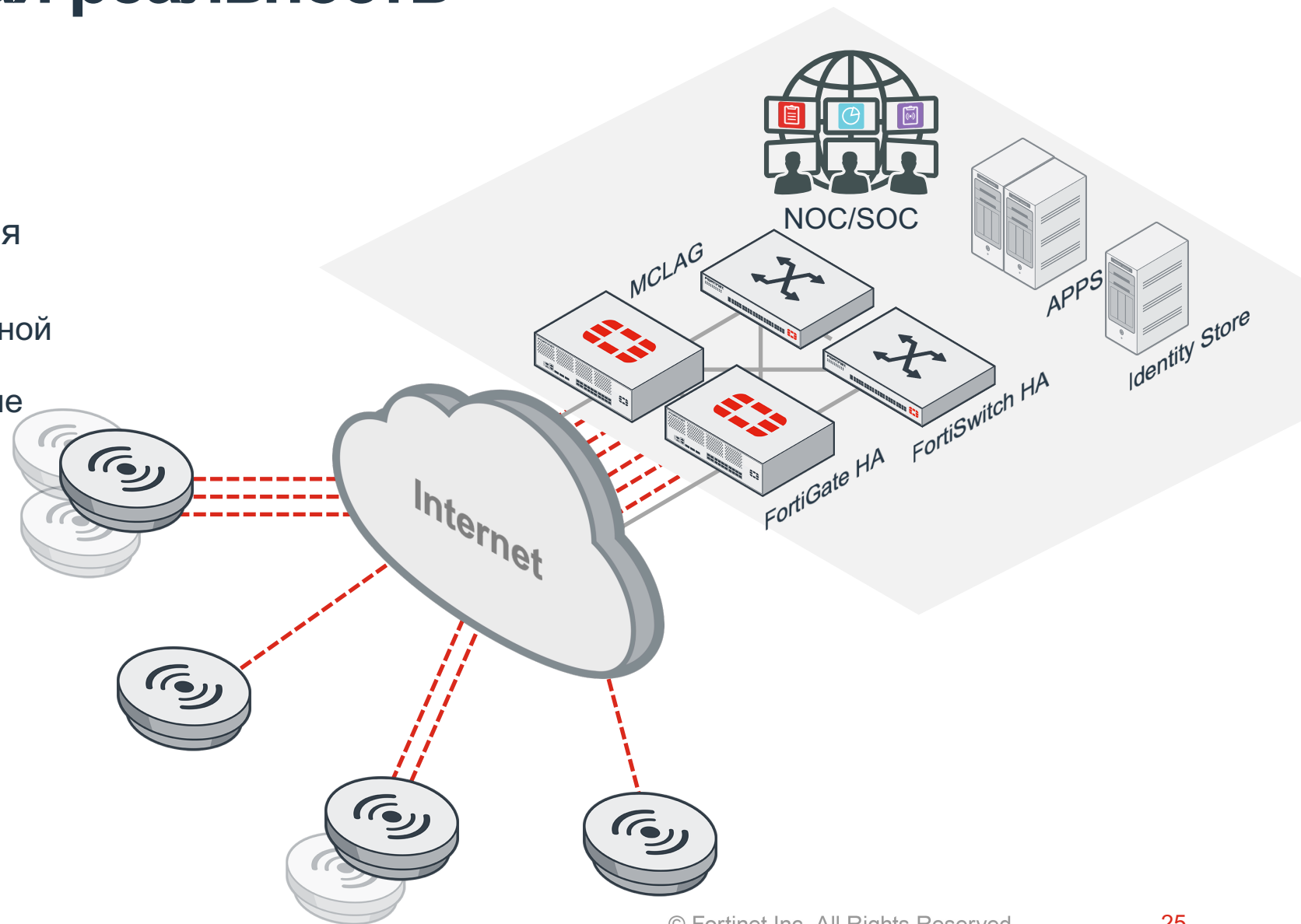




# «Удалёнка» - новая реальность

## Remote AP

- Может использоваться любая FortiAP
- Wallplate модели с дополнительной настольной подставкой удобны, когда требуются дополнительные порты на столе
- Централизованное управление через FortiGate
- FortiDeploy для zero touch
- Split tunnel для отделения некорпоративного трафика



# Унифицированный уровень доступа с расширенными функциями безопасности

## FortiGate



- Множество моделей
- Next Generation Firewall
- Контроллер WLAN
- Контроллер коммутаторов

## Точки доступа



- Более 20 моделей
  - 802.11ac и Wi-Fi 6
  - Встроенные или внешние антенны
- Интеграция с FortiGate (FortiLink)
- Indoor/Outdoor/Настенного исполнения

## Коммутаторы



- Более 20 моделей
  - Edge коммутаторы
  - ToR коммутаторы
- Интеграция с FortiGate (FortiLink)
- L2/L3 + Advanced Services

# Беспроводные решения Fortinet

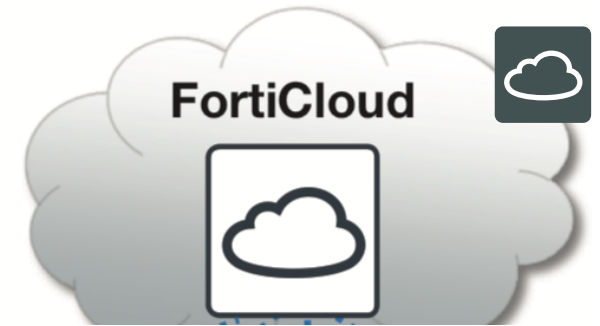
Integrated (FortiGate)



Controller (FortiWLC)

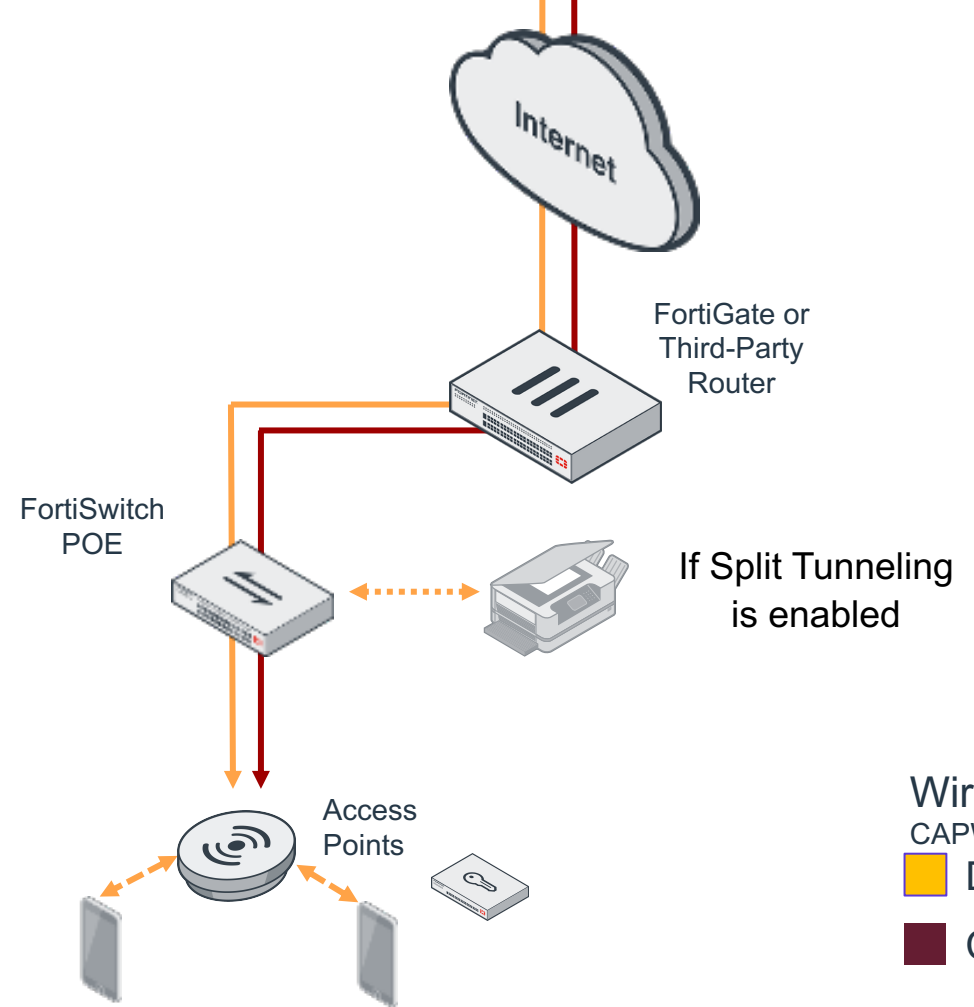
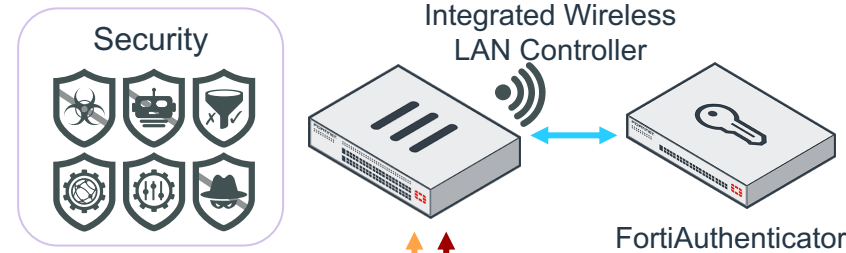
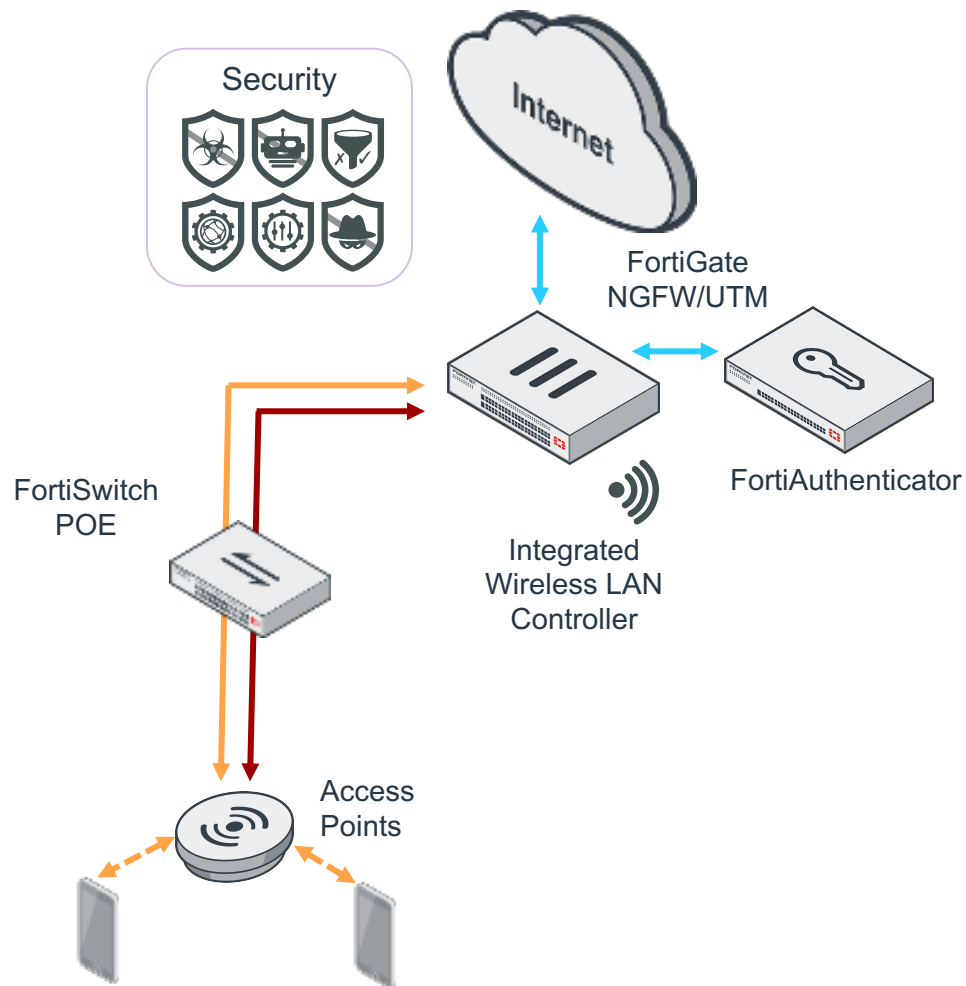


Cloud



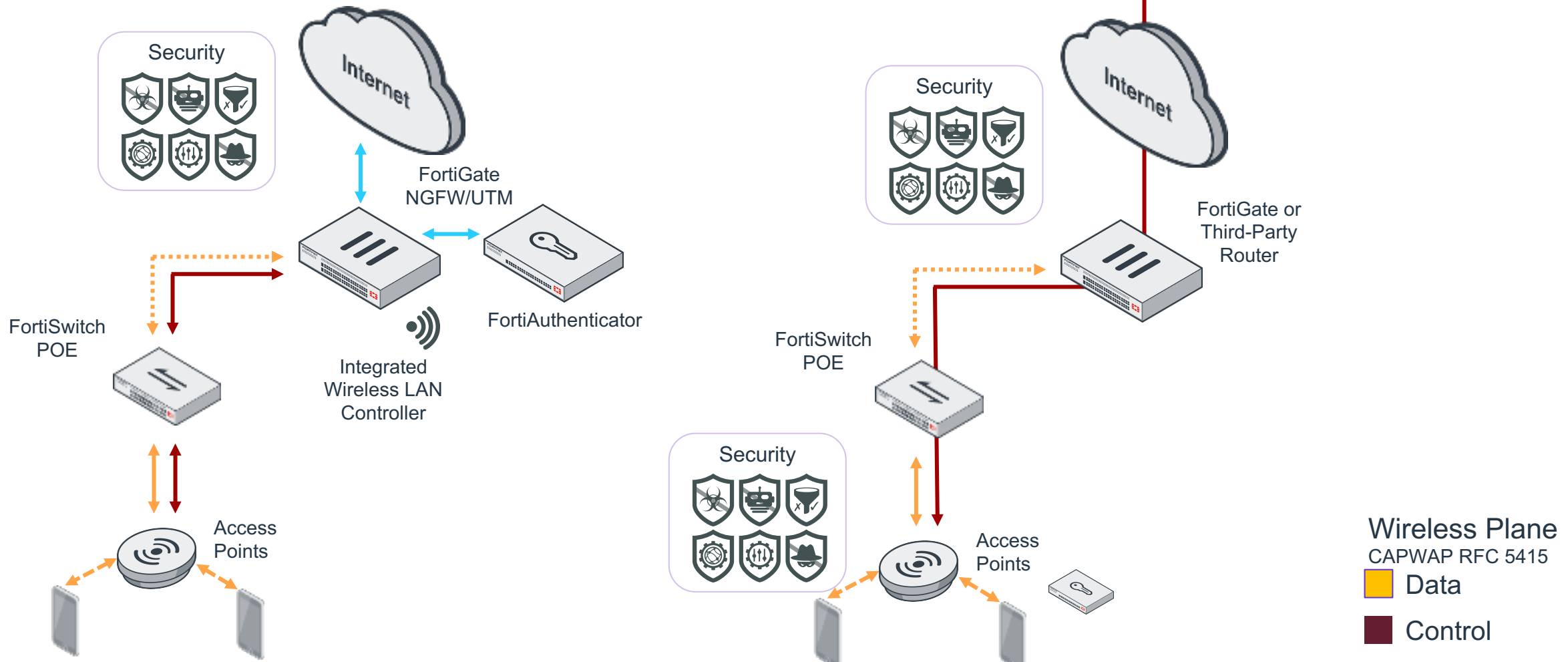
# Tunnel Mode

## Сценарии применения



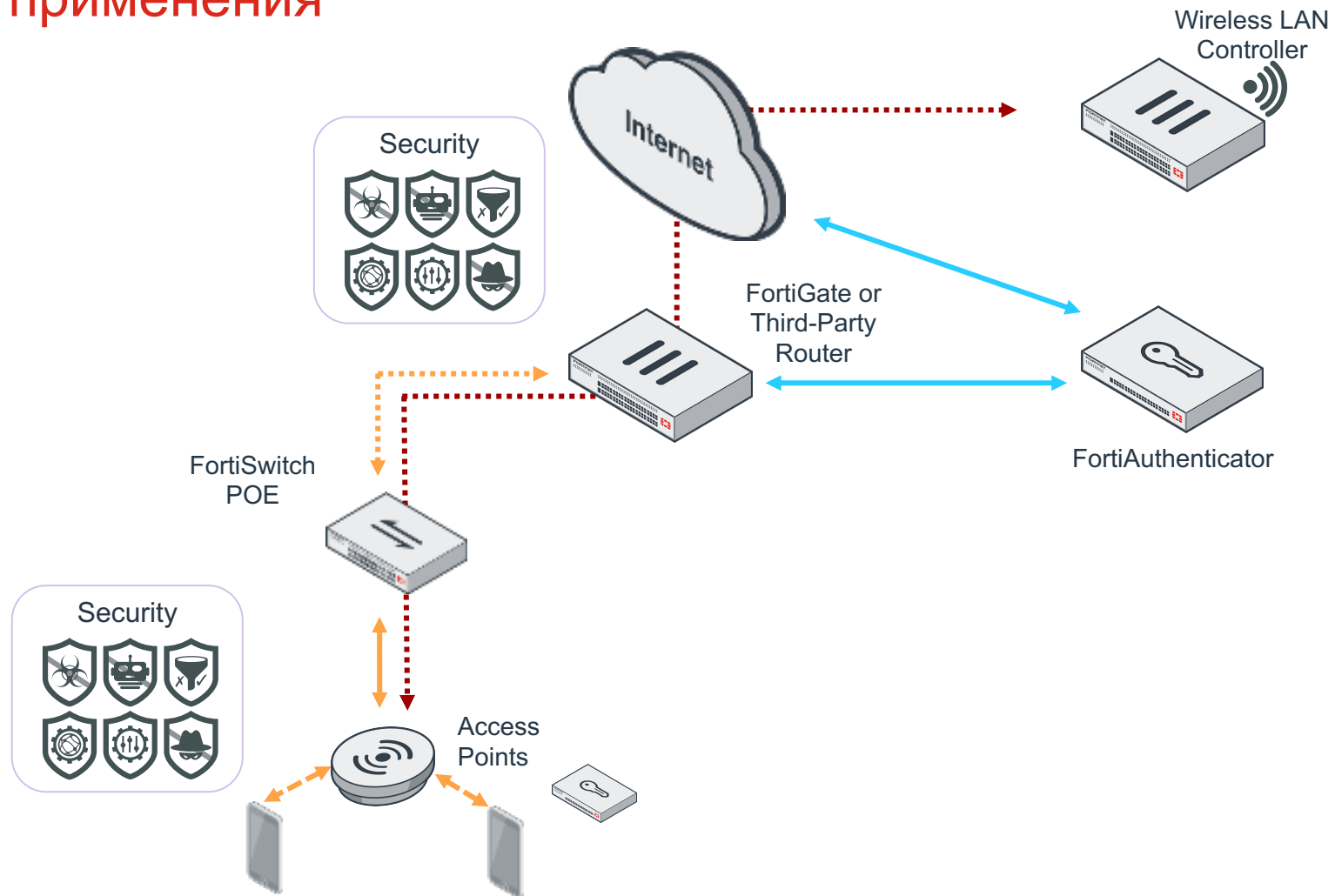
# Local Bridge Mode

## Сценарии применения



# Local Standalone

## Сценарии применения



Wireless Plane  
CAPWAP RFC 5415

■ Data

■ Control

■ Internet

# Local Standalone Configuration

The screenshot shows the Fortinet FortiGate configuration interface for a WiFi SSID. The left sidebar contains a navigation menu with the following items: Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller (expanded), Managed FortiAPs, WiFi Maps, SSID (selected), FortiAP Profiles, WIDS Profiles, and Security Profile Groups. The main content area is titled 'Edit Interface' and shows the following configuration details:

- Interface Name: SSID1
- Alias: b
- Type: WiFi SSID
- Traffic Mode: Bridge

Below the interface settings is a 'Tags' section with an 'Add Tag Category' button. The 'WiFi Settings' section includes:

- SSID: Remote
- Security Mode: WPA2 Personal
- Pre-shared Key: [Redacted]
- Local Standalone:  (highlighted with a red box)
- Local Authentication:  (highlighted with a red box)
- Client Limit per Radio:

# Поддерживаемые функции в зависимости от используемого режима (для версии 6.0.4)

Feature	Tunnel	Local Bridge	Local Standalone
<b>Authentication</b>			
Captive Portal	Yes	No	No
MAC-Auth Captive portal bypass	Yes	No	No
RADIUS Authentication	Yes	Yes	Yes
RADIUS Accounting	Yes	Yes	Yes
RADIUS CoA	Yes	Yes	Yes
RADIUS Dynamic VLAN	Yes	Yes	Yes
RADIUS User Group	Yes	Yes	Yes
<b>Wireless</b>			
Probe response suppression	Yes	Yes	Yes
Band steering	Yes	Yes	Yes
Data rates customization	Yes	Yes	Yes
Channel Utilization	Yes	Yes	Yes
802.11kvr	Yes	Yes	No
Multiple PSK	Yes	Yes	Yes
Broadcast suppression	Yes	Yes	Yes
Opportunistic Key Caching	Yes	Yes	Yes
Quality of Service	Yes	Yes	Yes
<b>Deployments</b>			
Point-to-Point Mesh	Yes	Yes	Yes
Lan Isolation	N/A	N/A	Yes(1)
Local-standalone-nat	N/A	N/A	Yes
Local-standalone-nat bypass	N/A	N/A	Yes
Bridge Lan to SSID	Yes	Yes	Yes
Split tunneling	Yes	N/A	N/A
High Availability (1+1)	Yes	Yes	N/A
VLAN Pooling - AP Group based	Yes	Yes	No
VLAN Pooling (Hash & RR )	Yes	No	No
<b>Security</b>			
Client Quarantine	Yes	No	No
UTM On FAP	No	Yes	Yes

(1) Only available when local-standalone-nat is enabled



# **FortiOS Wireless Controller**

Примеры настройки

# Create SSID

FortiGate 300E Demo-ISFW-PRI HA: Master 54 admin

Navigation menu:

- ★ Favorites
- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller**
- Managed FortiAPs
- WiFi Maps
- SSID**
- FortiAP Profiles
- WIDS Profiles
- FortiLink Interface
- Managed FortiSwitch
- FortiSwitch VLANs
- FortiSwitch Ports
- FortiSwitch Security Policies
- Log & Report
- Monitor

Create New SSID

Name:

Alias:

Type: WiFi SSID

Traffic mode:  Tunnel  Bridge  Mesh

Address

IP/Netmask:

Create address object matching subnet:

Name:

Destination: 0.0.0.0/0.0.0.0

Secondary IP address:

Administrative access

IPv4:  HTTPS  HTTP  PING  FMG-Access  SSH  SNMP  FTM  RADIUS Accounting  Security Fabric Connection

DHCP Server

Network

Device detection:

WiFi Settings

SSID:

OK Cancel

# AP Profile

The screenshot displays the FortiGate 300E configuration interface. The top navigation bar shows 'FortiGate 300E Demo-ISFW-PRI' and 'HA: Master'. The left sidebar contains a menu with 'WiFi & Switch Controller' expanded, and 'FortiAP Profiles' highlighted. The main area shows the 'New FortiAP Profile' dialog box with the following configuration:

- Name: [Empty text box]
- Comments: Write a comment... (0/255)
- Platform: FAP221E
- Country / Region: Use default (United States) Specify
- AP login password: Set Leave Unchanged Set Empty
- Administrative access:  HTTPS  SSH  SNMP
- Radio 1:
  - Mode: Disabled Access Point Dedicated Monitor
  - WIDS profile:
  - Radio resource provision:
  - Client load balancing:  Frequency Handoff  AP Handoff
  - Band: 2.4 GHz 802.11n/g
  - Channel width: 20MHz
  - Short Guard Interval:
  - Channels:  1  6  11
  - TX power control: Auto Manual
  - TX power: [Slider] 100%
  - SSIDs: Auto Manual
  - Monitor channel utilization:
- Radio 2: [Empty text box]


At the bottom of the dialog are 'OK' and 'Cancel' buttons.

# Managed APs

FortiGate 300E Demo-ISFW-PRI HA: Master 54 admin


- ★ Favorites
- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Managed FortiAPs
- WiFi Maps
- SSID
- FortiAP Profiles
- WIDS Profiles
- FortiLink Interface
- Managed FortiSwitch
- FortiSwitch VLANs
- FortiSwitch Ports
- FortiSwitch Security Policies
- Log & Report
- Monitor

Status



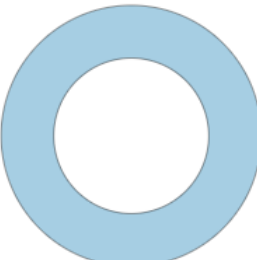
■ Disconnected  
■ Online

Health



■ Fair

Model



■ FAPU431F

+ Create New
✎ Edit
🗑 Delete
🔄 Refresh
🔍 Search

Access Point	Status	SSIDs	Channel	Health	Clients	OS Version	LLDP	FortiAP
FIN_AP1	Disconnected	R1 DemoLab_WiFi_Corp (WlanCorp) AP DemoLab_WiFi_Guest (WlanGuest) DemoLab_WiFi_Staff (WlanStaff) R2 DemoLab_WiFi_Corp (WlanCorp) AP DemoLab_WiFi_Guest (WlanGuest) DemoLab_WiFi_Staff (WlanStaff) R3 N/A	R1 0 R2 0 R3 N/A		0		No LLDP neighbors found.	FAPU
ENG_AP1	Disconnected	R1 DemoLab_WiFi_Corp (WlanCorp) AP DemoLab_WiFi_Guest (WlanGuest) DemoLab_WiFi_Staff (WlanStaff) R2 DemoLab_WiFi_Corp (WlanCorp) AP DemoLab_WiFi_Guest (WlanGuest) DemoLab_WiFi_Staff (WlanStaff) R3 N/A	R1 0 R2 0 R3 N/A		0		No LLDP neighbors found.	FAPU
SALES_AP1	Online	R1 DemoLab_WiFi_Corp (WlanCorp) AP DemoLab_WiFi_Guest (WlanGuest) DemoLab_WiFi_Staff (WlanStaff)	R1 161 R2 6 R3 N/A	Fair	4	PU431F-v6.0-build0019	No LLDP neighbors found.	FAPU

# AP Details (w/ Spectrum)

FortiGate VM64 FGVM010000137228
admin

- Dashboard >
- Security Fabric >
- FortiView >
- Network >
- System >
- Policy & Objects >
- Security Profiles >
- VPN >
- User & Device >
- WiFi & Switch Controller >
- Managed FortiAPs ☆
- WiFi Maps
- SSID
- FortiAP Profiles
- WIDS Profiles
- Log & Report >
- Monitor >

Status Online


+ Create New Edit Delete Refresh Search

Access Point	Status	SSIDs	Channel
FP221E3X17000066	Online	R1 N/A R2 N/A	R1 N/A R2 N/A
FP421E-Spectrum	Online	R1 N/A R2 N/A	R1 N/A R2 N/A

Summary of FP221E3X17000066

Radios Clients Logs CLI Access Spectrum Analysis

### Signal Interference



### Signal Interference Spectrogram



### Duty Cycle



### Duty Cycle Spectrogram

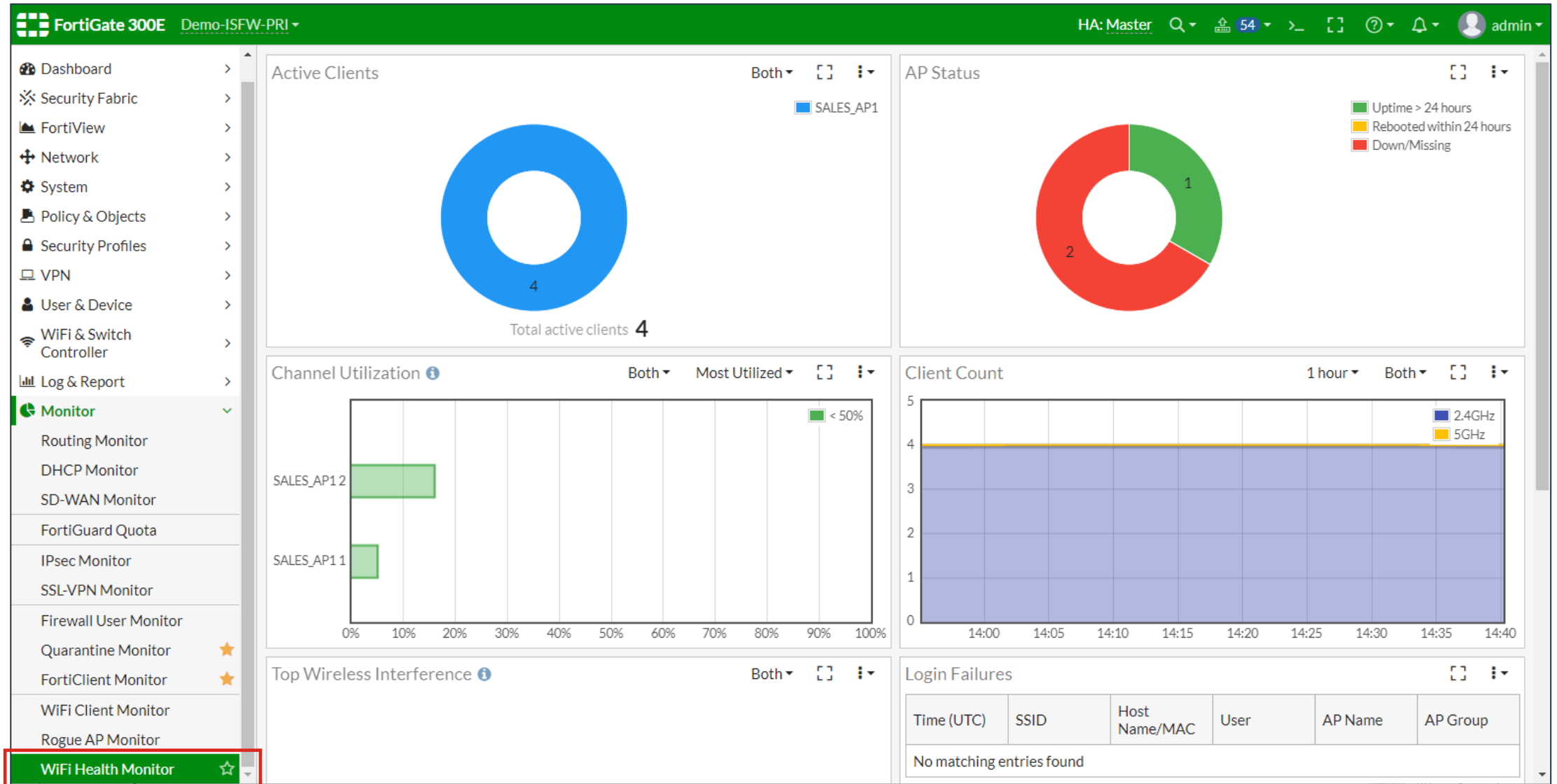


Close

# MAP

The screenshot displays the FortiGate 300E WiFi Maps interface. The top navigation bar shows 'FortiGate 300E Demo-ISFW-PRI' on the left and 'HA: Master' with user 'admin' on the right. A search bar indicates '0 Unplaced AP(s)'. Below the search bar are controls for 'Both Bands', 'Client Count', and 'LAB'. The main area shows a floor plan with three access points: SALES\_AP1 (blue icon, Client Count: 4), FIN\_AP1 (red icon), and ENG\_AP1 (red icon). The left sidebar lists various configuration options, with 'WiFi Maps' highlighted in green. The bottom right corner has zoom controls (+ and -).

# Wi-Fi Overview



# Security Rating

FortiGate 2000E NGFW-PRI HA: Master interim build1528 demo

Security Rating

Score: **-615.8**  
 Ran: 3 hour(s) and 6 minute(s) ago

Search: wireless

Buttons: All Results, Failed, Export, Run Now

Compliance	Security Control	Devices	Priority Result
Audit Logging & Monitoring (AL) 1			
FSBP AL06.1	Secure <b>Wireless</b> Monitoring All discovered APs should be classified as rogue, accepted or suppressed.	NGFW-PRI ISFW_PRI DCFW ISFW-FIN +3	Unlicensed
Network Design & Policies (ND) 3/4			
FSBP ND02.2	Secure <b>Wireless</b> Connections All <b>wireless</b> networks should be secured.	NGFW-PRI ISFW_PRI DCFW ISFW-FIN +3	Unlicensed
FSBP ND01.3	Rogue AP Detection From the <b>wireless</b> AP profile, ensure a WIDS profile is enabled with at least Rogue AP detection enabled.	NGFW-PRI ISFW_PRI DCFW ISFW-FIN +3	Failed
FSBP ND02.1	Secure <b>Wireless</b> Connections - Insecure Protocols <b>Wireless</b> networks should not permit insecure protocols such as WEP or other less secure algorithms	NGFW-PRI ISFW_PRI DCFW ISFW-FIN +3	Unlicensed

Security Control Details: Select a Security Control to see details.



# Интерфейсы (в том числе SSIDs)

The screenshot shows the FortiGate 300E management interface. The left sidebar has the 'Network' menu expanded, with 'Interfaces' highlighted in green. The main content area displays a summary of interface types and a table of WiFi SSIDs.

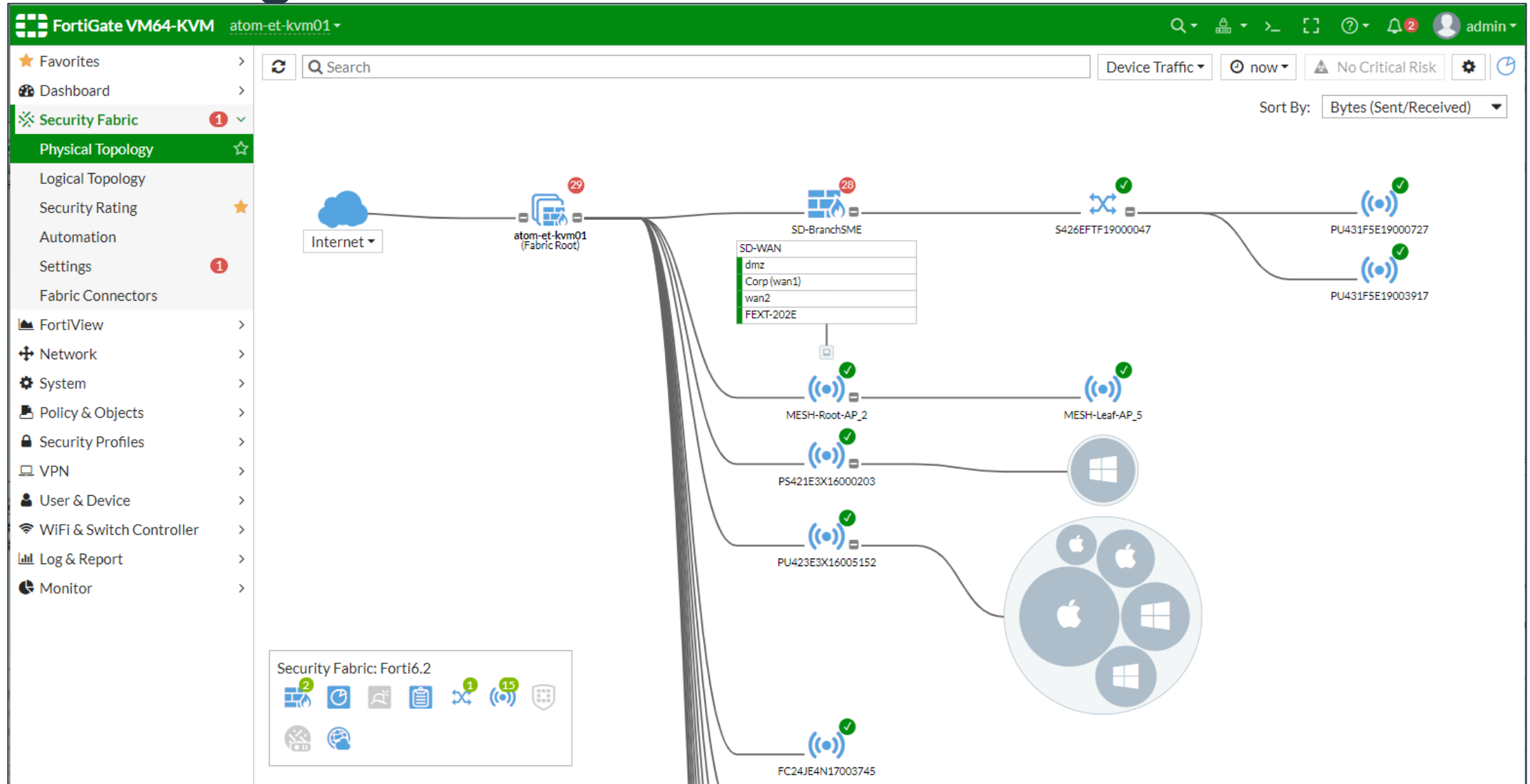
**Summary:**

- 802.3ad Aggregate: 12
- Physical Interface: 8
- Software Switch: 2
- Virtual Wire Pair: 3
- WiFi SSID: 4

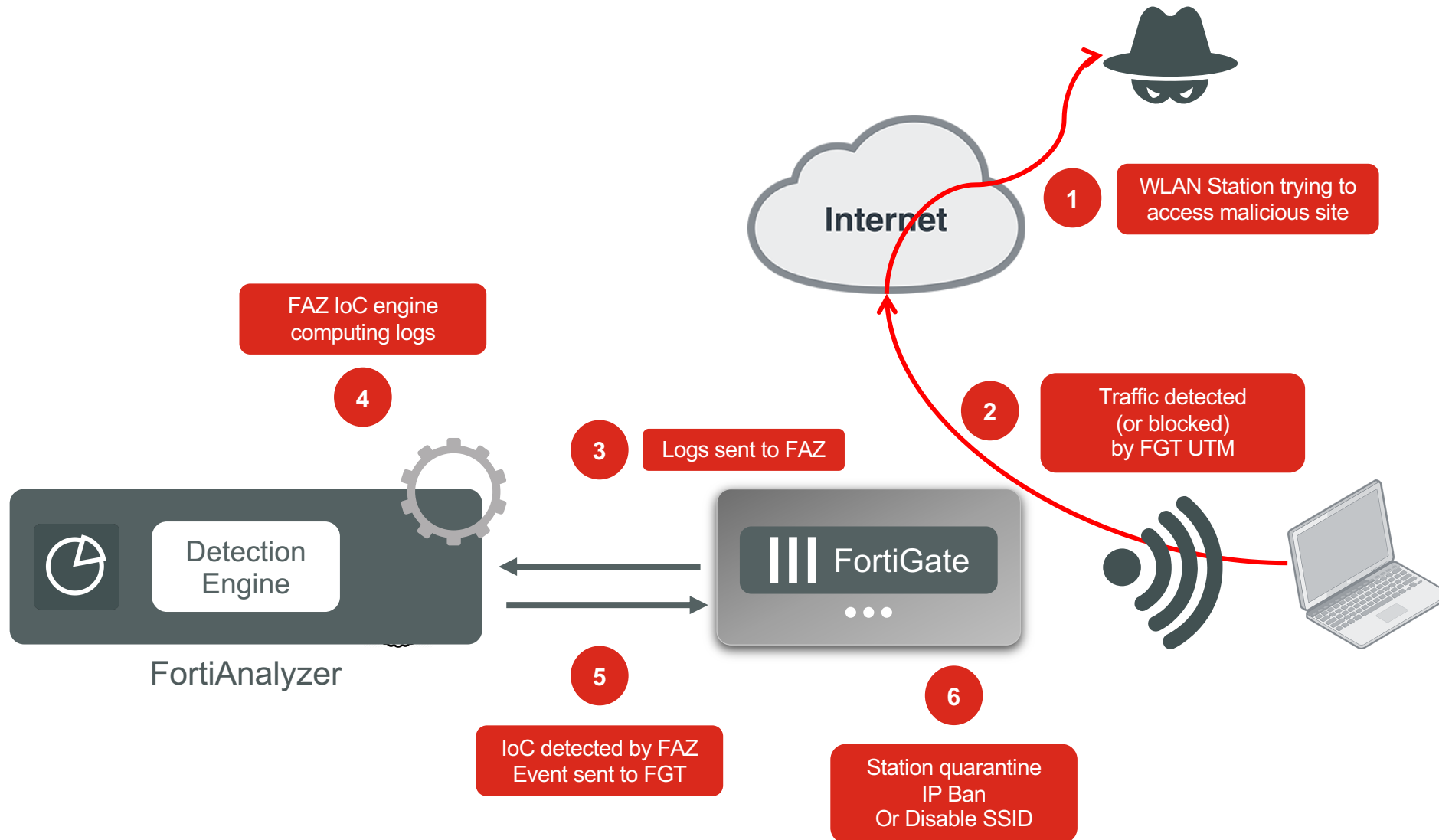
**WiFi SSID Table:**

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP
DemoLab_WiFi_Corp (WlanCorp)	WiFi SSID		10.89.101.99/255.255.255.0		PING HTTPS SSH SNMP +3		
DemoLab_WiFi_Guest (WlanGuest)	WiFi SSID		0.0.0.0/0.0.0.0				
DemoLab_WiFi_Staff (WlanStaff)	WiFi SSID		10.89.102.99/255.255.255.0				10.89.102.1- 10.89.102.10

# Fabric diagram



# Integrated wireless Quarantine



# **Построение высокопроизводительных беспроводных сетей**

на базе контроллера FortiWLC

# Контроллеры Fortinet

ESXi, Hyper-V, KVM



**FWC-50D**

50 точек доступа  
1500 клиентов

ESXi, Hyper-V, KVM



**FWC-200D**

200 точек доступа  
2500 клиентов

ESXi, Hyper-V, KVM



**FWC-500D**

500 точек доступа  
10 GbE  
7500 клиентов

ESXi, Hyper-V, KVM



**FWC-1000D**

1000 точек доступа  
20К клиентов

ESXi, Hyper-V, KVM



**FWC-3000D**

3000 точек доступа  
45К клиентов

✓ Не нужны лицензии на точки для новых FWC

**В чем основные сложности при  
строительстве современных  
БЛВС?**

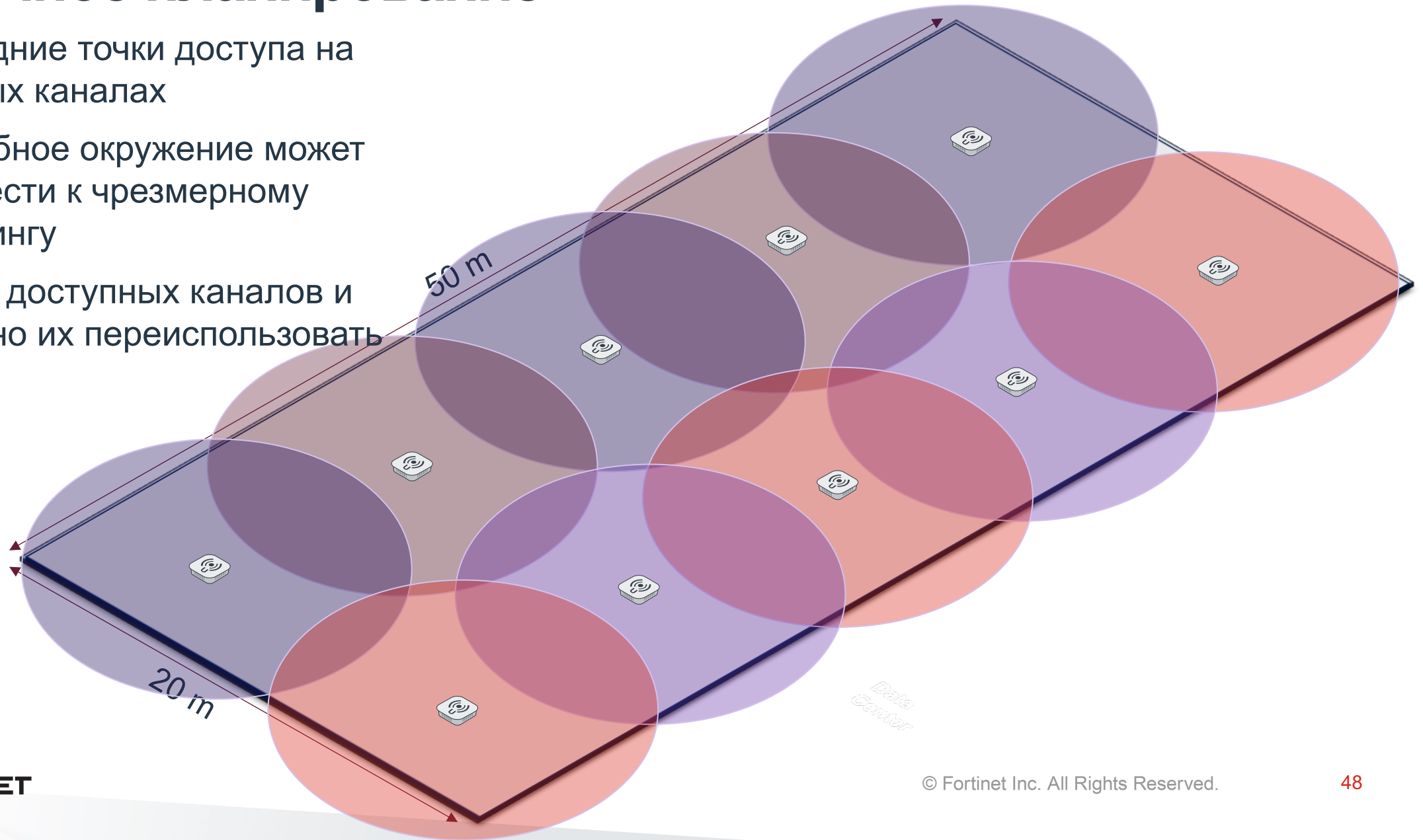
# Обычный офис

- 200 рабочих мест
- В среднем по 2-3 Wi-Fi устройства у каждого
- Итого: 500 Wi-Fi устройств
- Сколько потребуется точек?
- 10 (40-50 клиентов на ТД)



# Обычное планирование

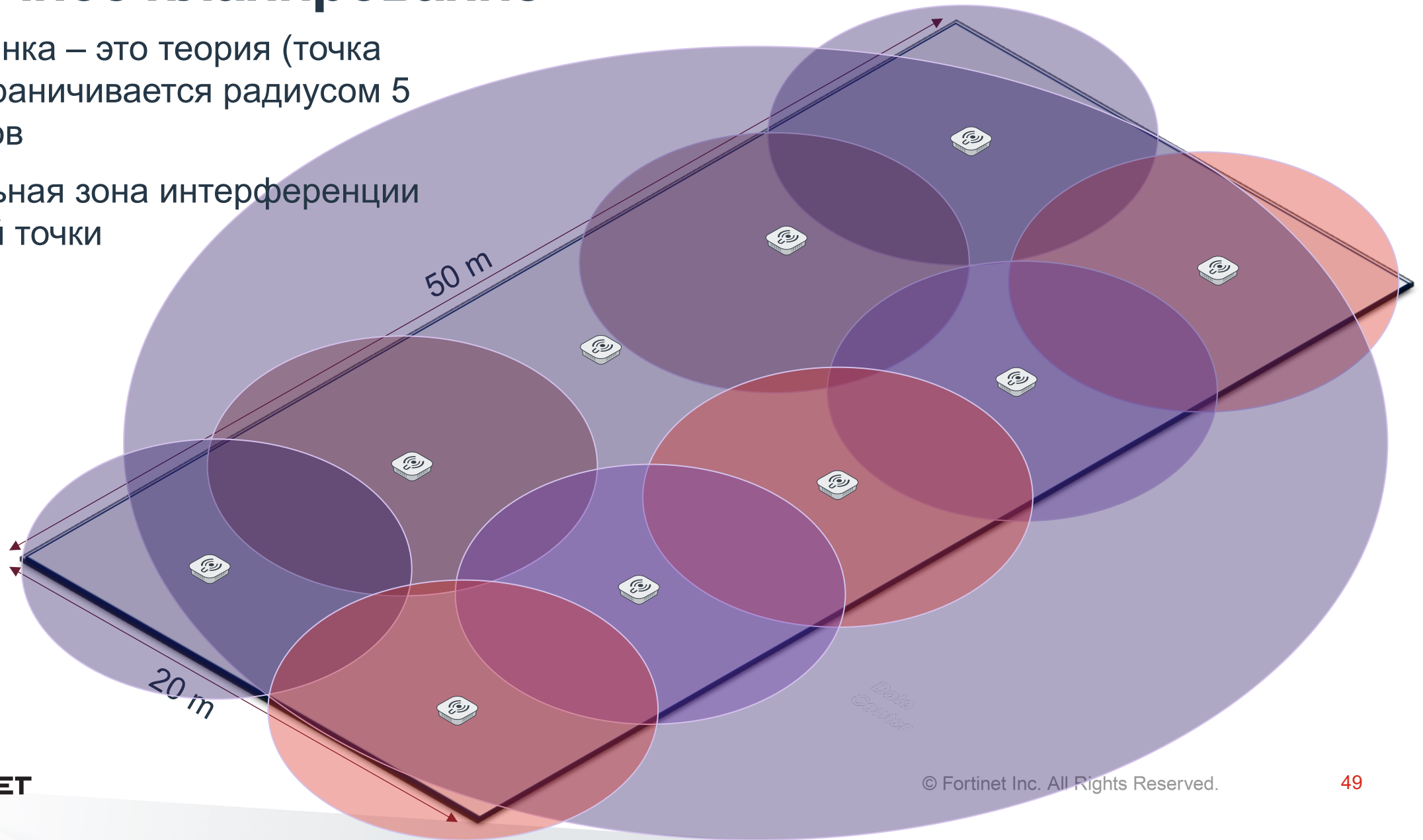
- Соседние точки доступа на разных каналах
- Подобное окружение может привести к чрезмерному роумингу
- Мало доступных каналов и сложно их переиспользовать





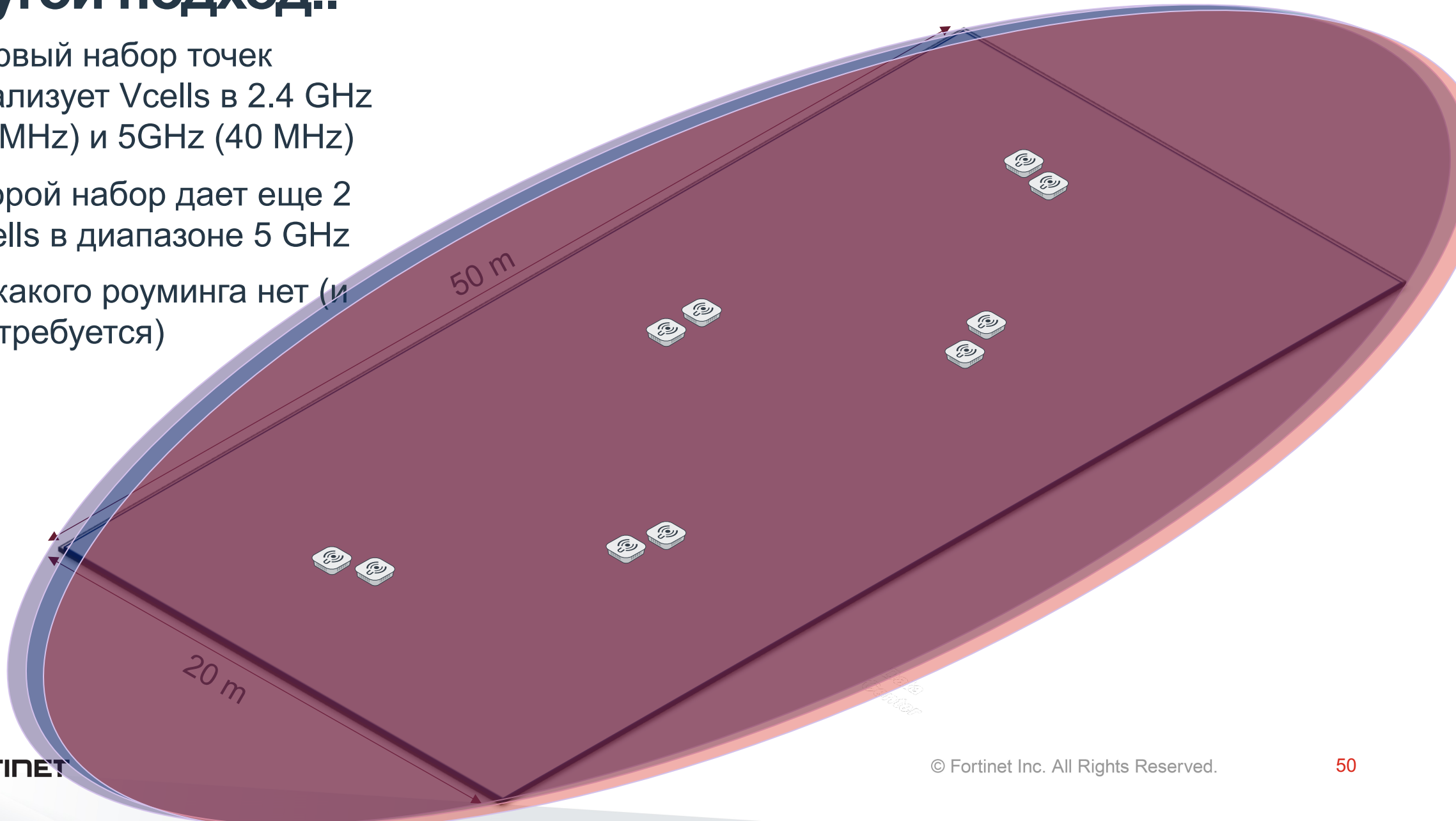
# Обычное планирование

- Картинка – это теория (точка не ограничивается радиусом 5 метров)
- Реальная зона интерференции одной точки



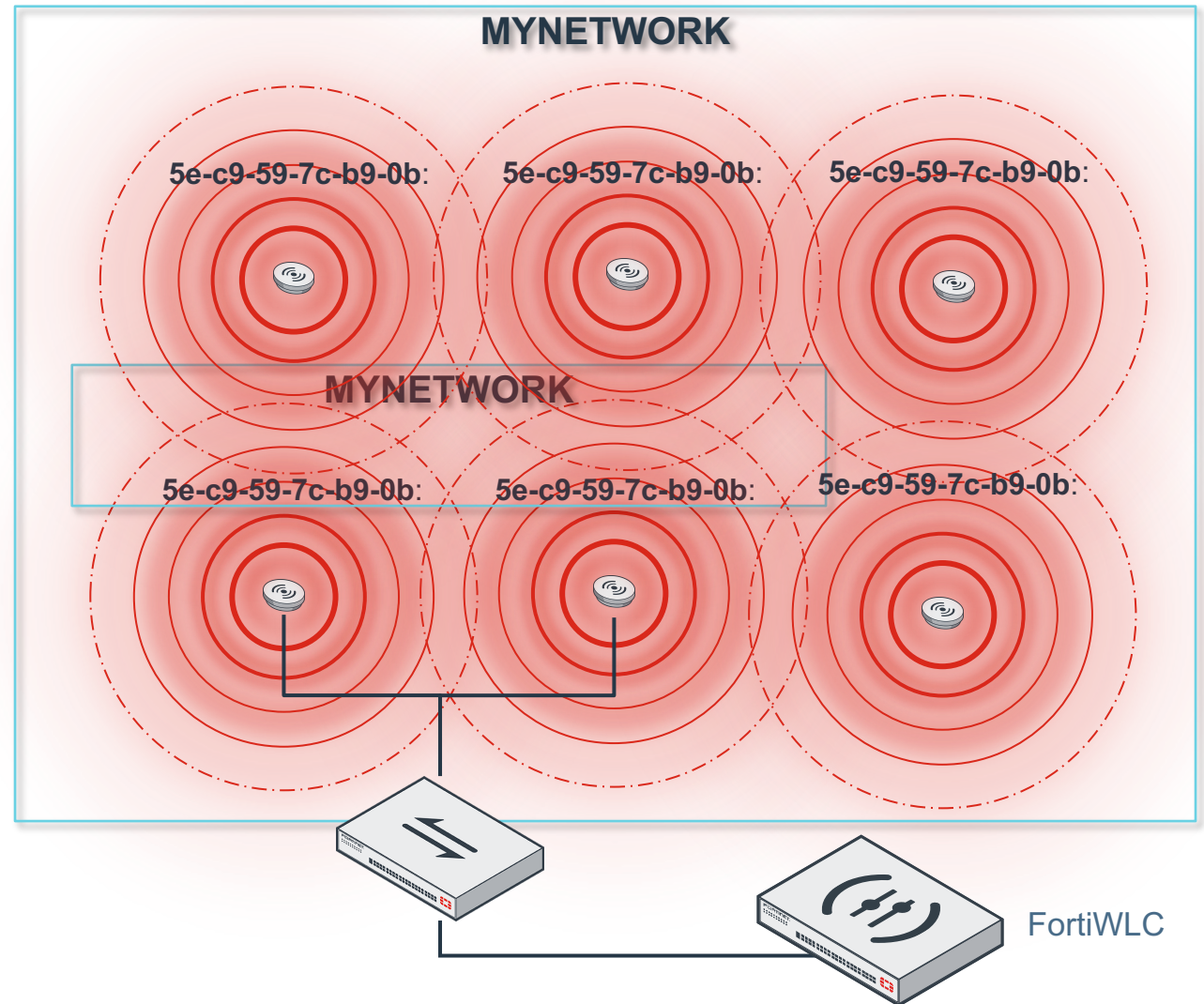
# Другой подход..

- Первый набор точек реализует Vcells в 2.4 GHz (20MHz) и 5GHz (40 MHz)
- Второй набор дает еще 2 Vcells в диапазоне 5 GHz
- Никакого роуминга нет (и не требуется)



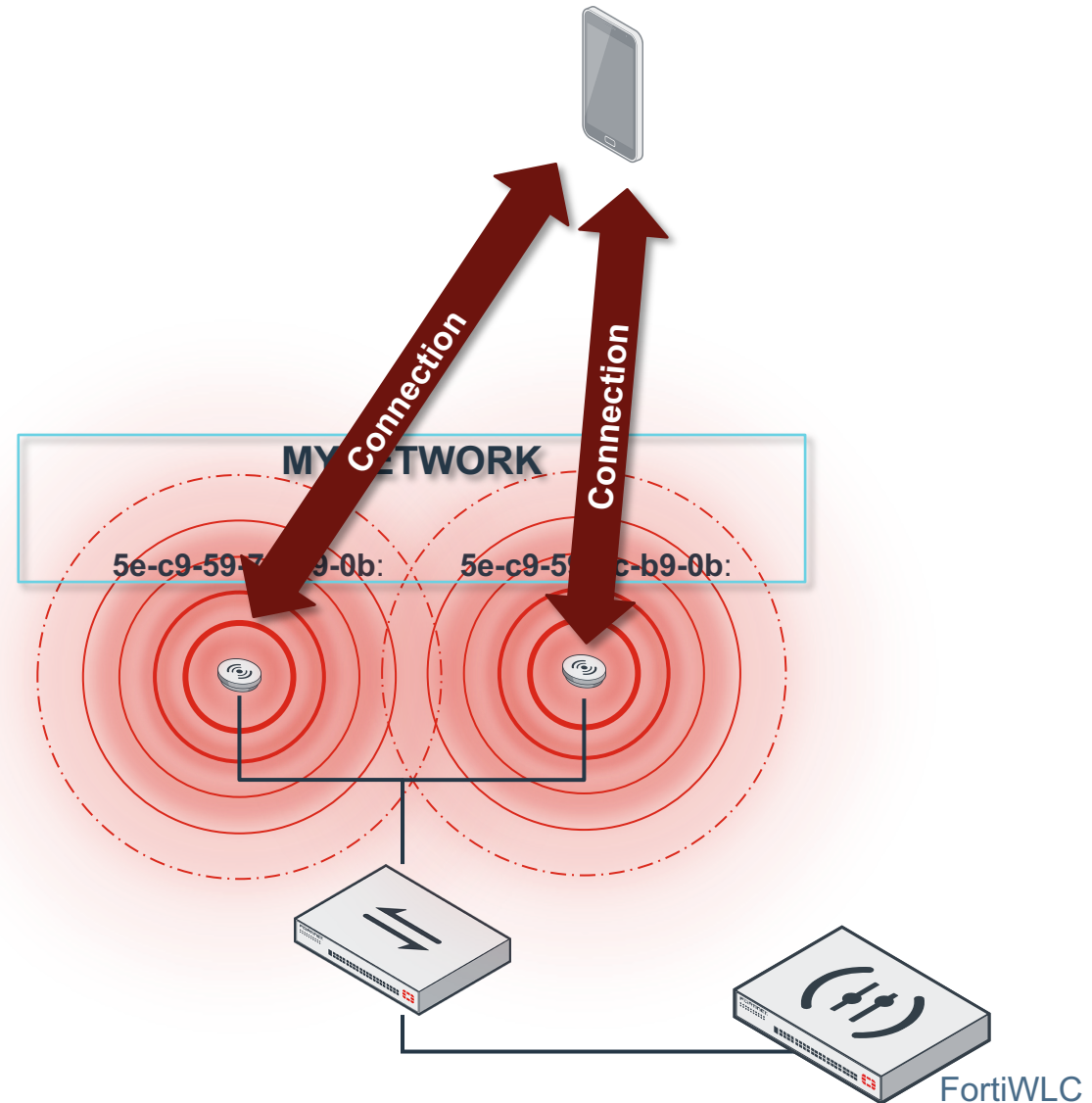
# Virtual Cell – виртуализация Wi-Fi сети

- Каждая точка доступа группы работает на одном и том же канале
- Используется один и тот же BSSID
- Wi-Fi сеть для клиента представляет одну точку доступа с очень обширным покрытием
- При перемещении клиент не совершает роуминга (он так думает)
- Легко добавить покрытия или емкости (увеличив количество точек в зоне)
- Решение соответствует стандарту 802.11



# Virtual Cell – процесс роуминга

- Когда клиент перемещается...
  - Он видит только одну «точку доступа»
  - Контроллер отслеживает SNR клиента
  - .. и когда это необходимо, переключает его на соседнюю точку доступа в рамках того же vcell
  - Клиент продолжает работу и не осведомлен, что теперь он работает физически с другой точкой доступа



# Virtual Cell – виртуализация Wi-Fi сети

NetSpot - Discover and analyze wireless networks around you

DISCOVER SURVEY EXPORT USER GUIDE ASK A QUESTION UPGRADE NOW

SSID	BSSID	Channel	Band	Security	Vendor	Mode	Level (SNR)	Signal	Signal...	Avg	Max	Min	Noise	Nois...	Last seen
<input type="checkbox"/> SECURITYDAY	00:0C:E6:02:8A:4F	149,+1	5GHz	WPA2 Personal	Meru	ac		-62	38%	-57	-48	-62	-77	23%	now
<input type="checkbox"/> SECURITYDAY	00:0C:E6:02:DC:0C	1	2.4GHz	WPA2 Personal	Meru	g/n		-51	49%	-51	-47	-61	-77	23%	now

FORTINET FortiWLC 8.4-4build-8 | FortiWLC-200D-VM 12:37:35 FWC-200D-VM@192.168.1.110

Monitor Configuration System Config Security Wireless ESS

ESS-AP Configuration (6 entries)

ESS Profile ESS-AP Table Security Profiles Hotspot Profiles

REFRESH ADD EDIT DELETE VIEW

	ESS Profile	AP ID	AP Name	Interface Index	Channel	Operating Channel	Admin State	Max Calls	BSSID	Owner
<input type="checkbox"/>	ESS	5	AP-2	2	149	149	Up	0	00:0c:e6:02:8a:4f	controller
<input type="checkbox"/>	ESS	6	AP-1	2	149	149	Up	0	00:0c:e6:02:8a:4f	controller
<input type="checkbox"/>	ESS	7	AP-3	2	149	149	Up	0	00:0c:e6:02:8a:4f	controller
<input type="checkbox"/>	ESS	5	AP-2	1	1	1	Up	0	00:0c:e6:02:dc:0c	controller
<input type="checkbox"/>	ESS	6	AP-1	1	1	1	Up	0	00:0c:e6:02:dc:0c	controller
<input type="checkbox"/>	ESS	7	AP-3	1	1	1	Up	0	00:0c:e6:02:dc:0c	controller

# Различия между MSA и vCell



Клиенты сами решают, когда совершить переключение

Клиенты конкурируют за доступ к среде



Контроллер управляет приемом и передачей

Сеть контролирует (=определяет) момент роуминга для каждого клиента (без его участия)

Сеть определяет доступ к среде

# Точки доступа 802.11ax (Wi-Fi6)



 802.11ax | Tri-Radio 5 GHz + 5 GHz + 2.4 GHz or 5 GHz + 2.4 GHz + scanning | 10 Antennas

 4x4 MIMO | Up to 4,804 Mbps + 4,804 Mbps + 300 Mbps





**F**ORTINET®