Построение защищенной инфраструктуры доступа компании

на основе решений Fortinet

Юрий Захаров
Системный инженер
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

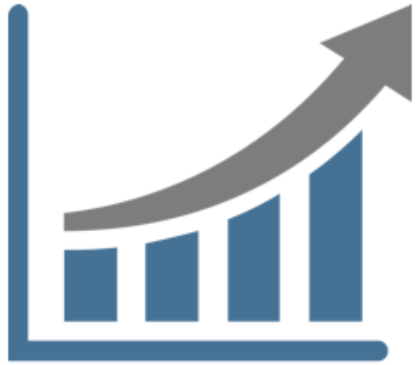
“Ваша сеть безопасна настолько, насколько безопасно ваше самое слабое звено”

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

FORTINET SECURITY FABRIC

Простое управление

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

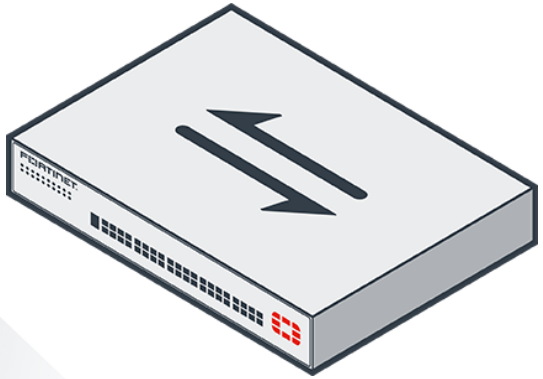
Интегрированная безопасность

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.



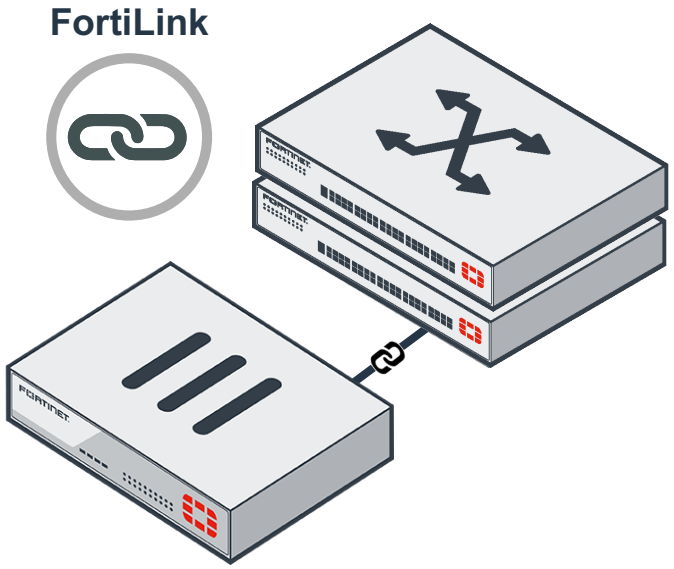
FORTINET

Варианты развертывания FortiSwitch

FortiLink

Управляется с FortiGate. Расширение Security Fabric на коммутаторы.

Наиболее распространенная модель развертывания

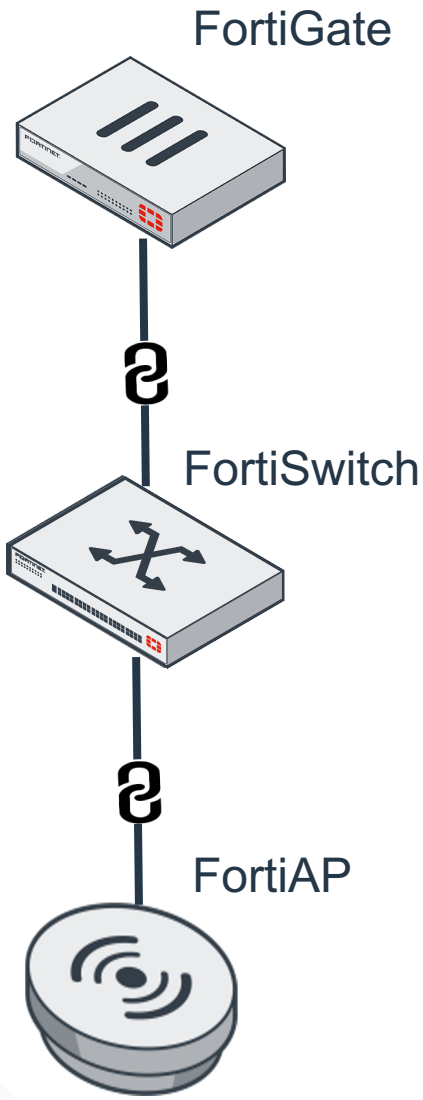


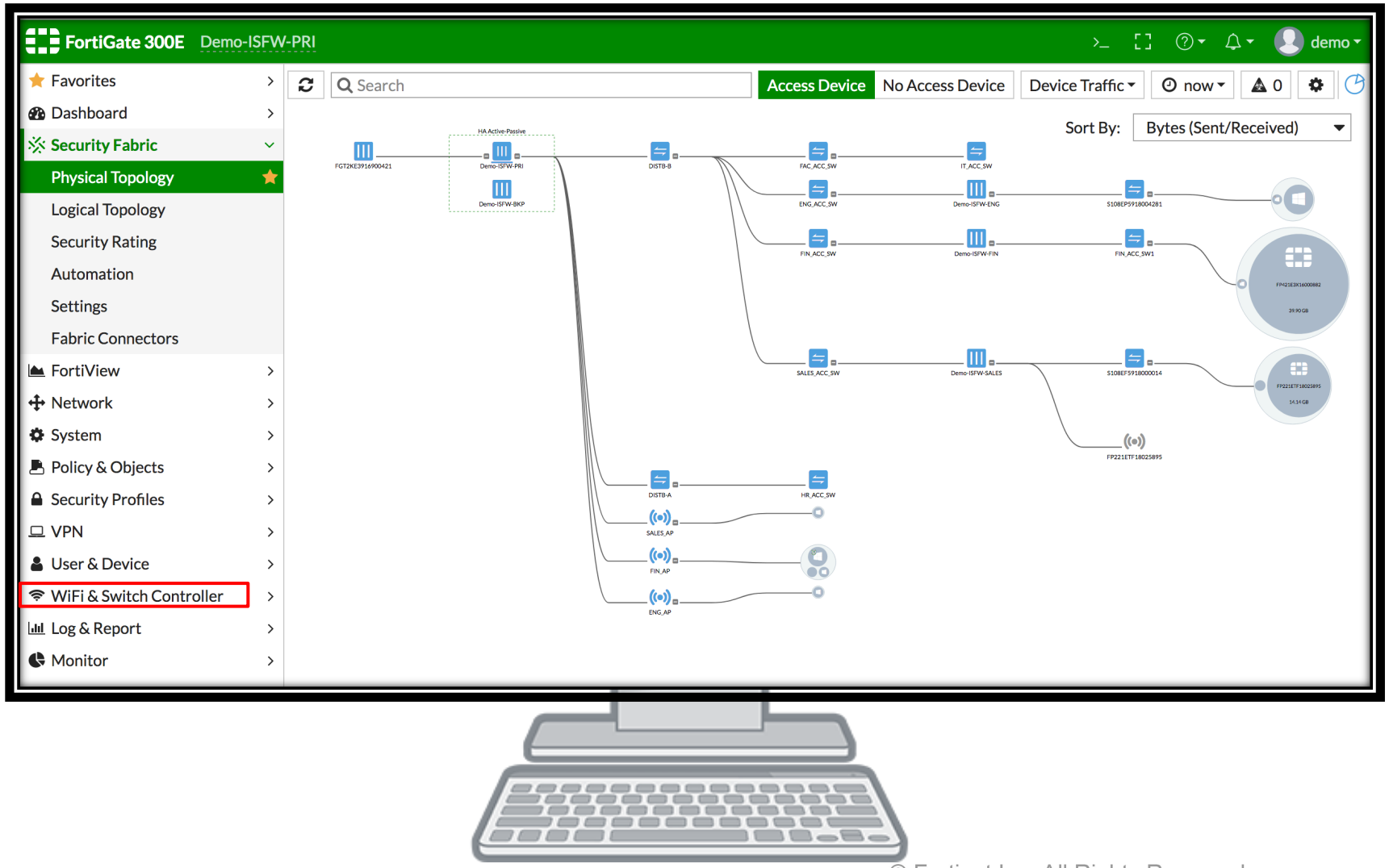
Stand Alone

Стандартная модель развертывания

Распространена в средах без FortiGate

Развертывание и управление сетью с FortiLink



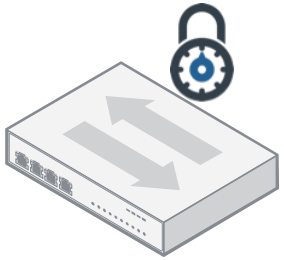


КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

ZERO-TOUCH PROVISIONING
АВТОМАТИЗАЦИЯ УСТАНОВКИ И НАСТРОЙКИ

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

БЕЗОПАСНОЕ И ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

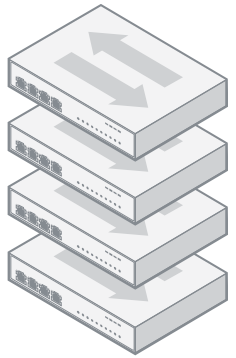


- FortiGate является единой точкой управления
- Централизованное управление VLAN и других функций провижининга

ИНТЕГРАЦИЯ КОММУТАТОРОВ С SECURITY FABRIC

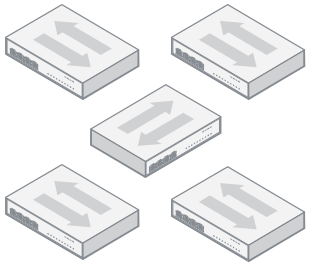
- Обнаружение подключаемых устройств
- Централизованная аутентификация
- Карантин на порту
- Динамическое назначение VLAN
- Логирование процессов

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

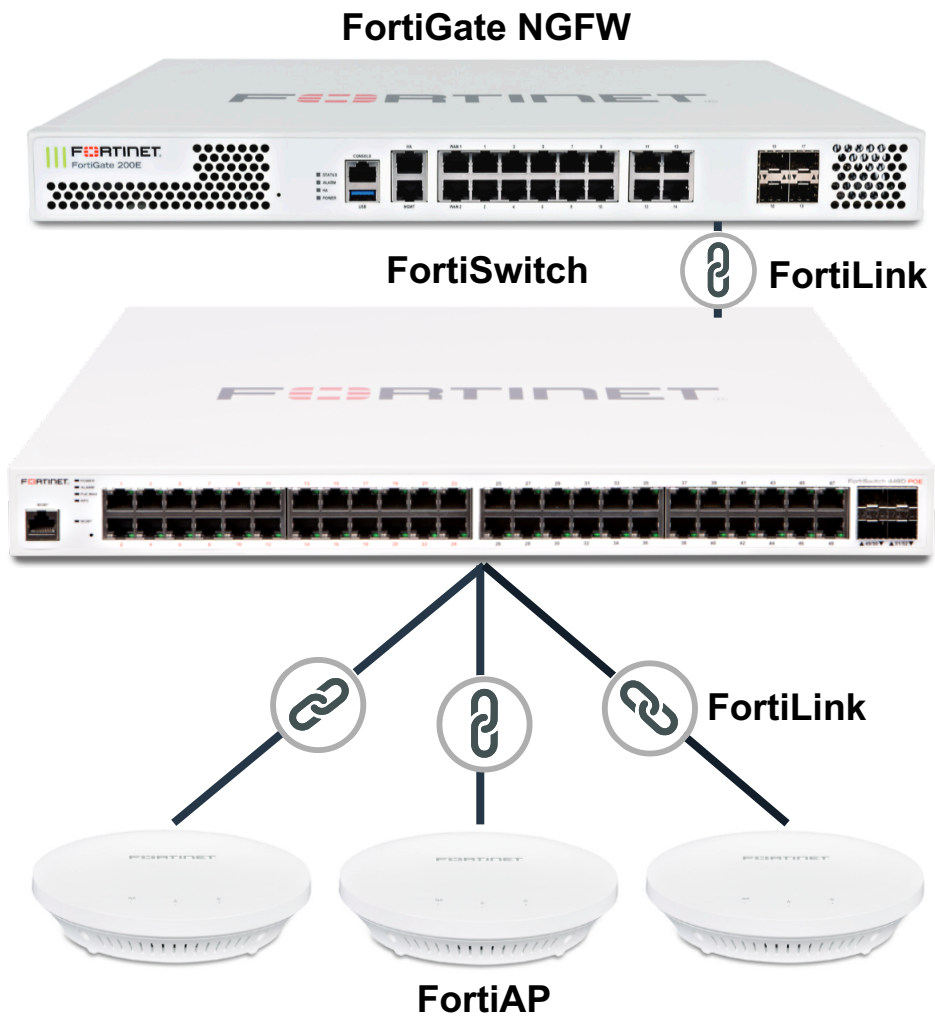
- Гибкая архитектура, масштабирование в соответствии с требованиями
- Прозрачность всего что происходит, аналитика, интеграция с wireless, и безопасность

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

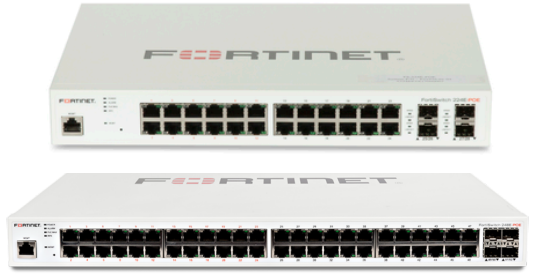
100 Серия

- Коммутаторы начального уровня
- От 8 до 48 гигабитных Ethernet портов, POE/POE+ коммутаторы
- Десктопные 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

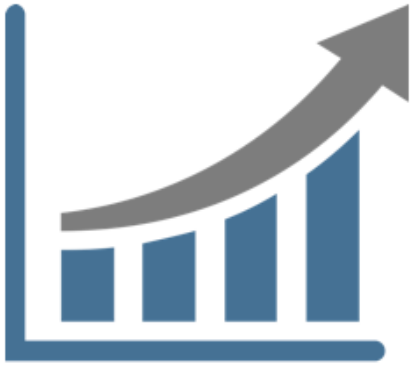
- Коммутаторы агрегации
- От 24 до 48 гигабитных Ethernet портов с POE+
- До (4) 10 Гигабитных Ethernet или (2) x 40 Гигабитных Ethernet SFP uplink портов

FortiSwitch 524D-FPOE

FortiSwitch 548D-FPOE

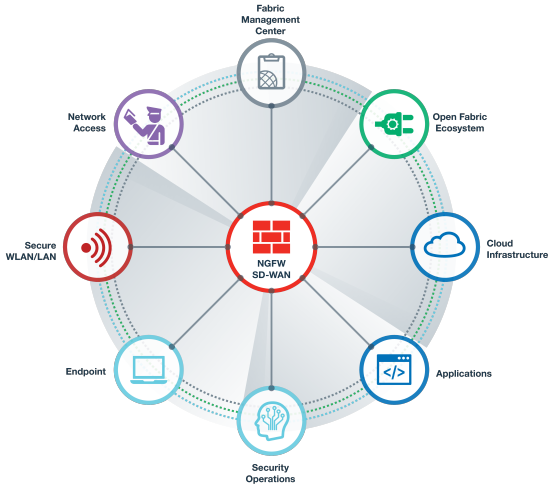
В результате

Количество устройств



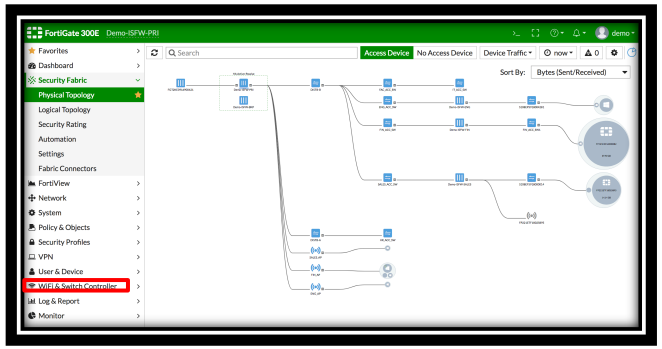
FortiSwitch – масштабируемое решение

Безопасность



Fortinet Security Fabric выявляет и блокирует угрозы

Управление



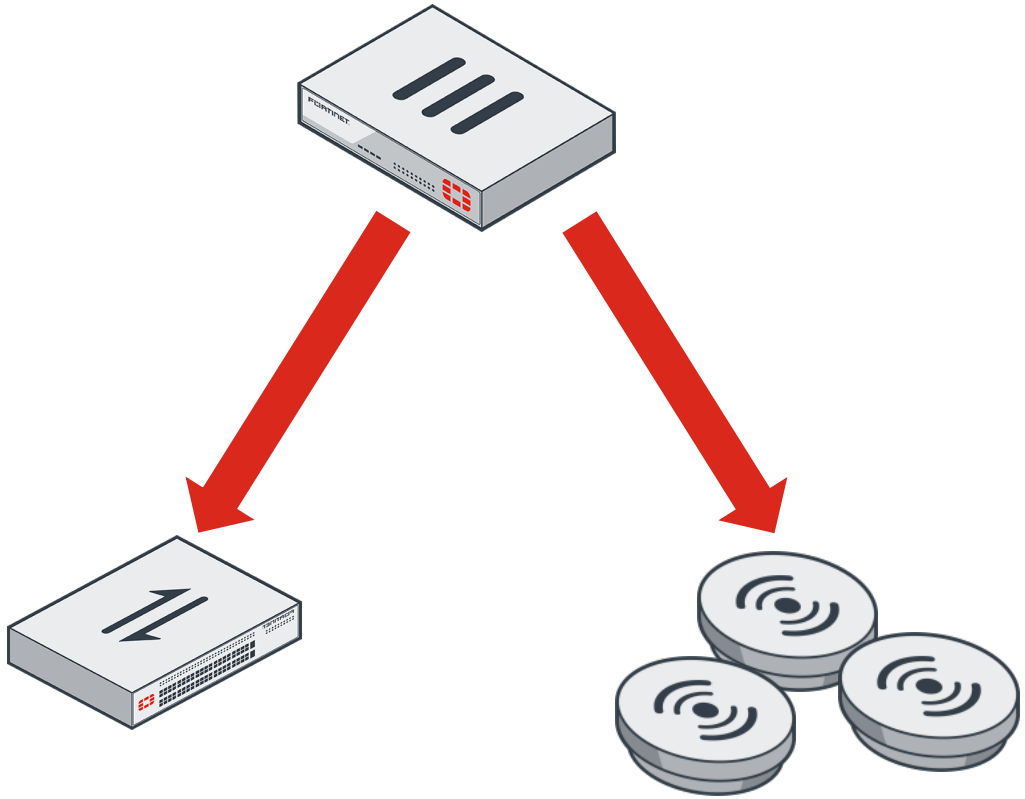
Единая консоль для управления МСЭ, коммутаторами и сетями Wi-Fi

Security Driven Networking

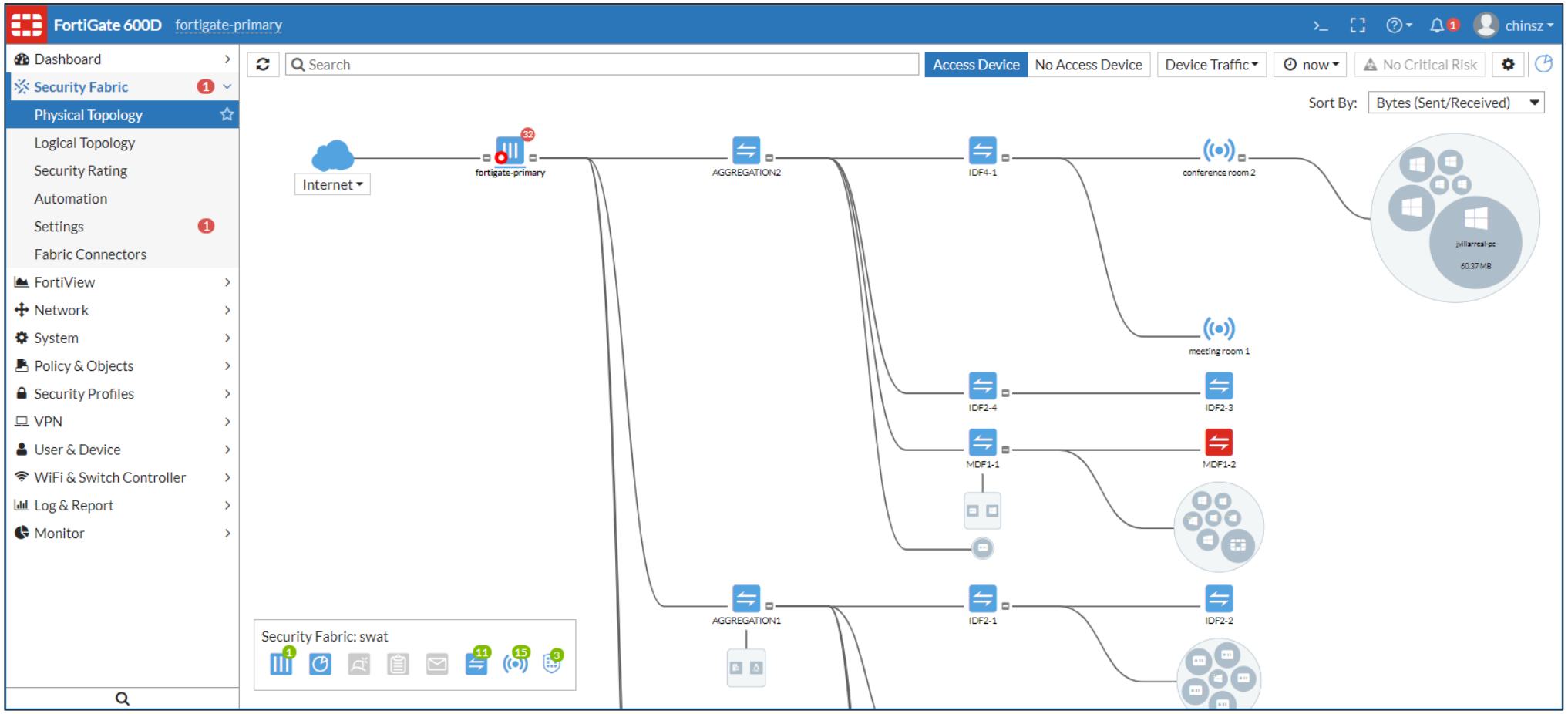
- Security Driven Networking объединяет безопасность и сетевые функции
- Сетевой уровень доступа создается со встроенными функциями безопасности
- Подобная архитектура более эффективна в части защиты и одновременно – простая в повседневной эксплуатации

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

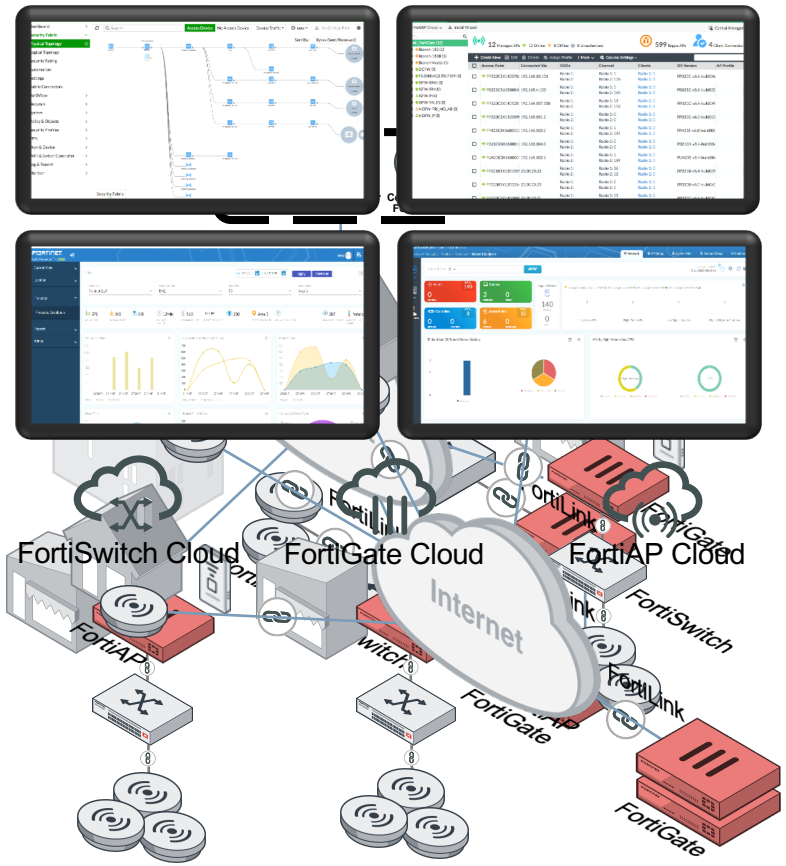
Management and Analytics

FortiGate

FortiManager

FortiPresence

FortiWLM



Campus

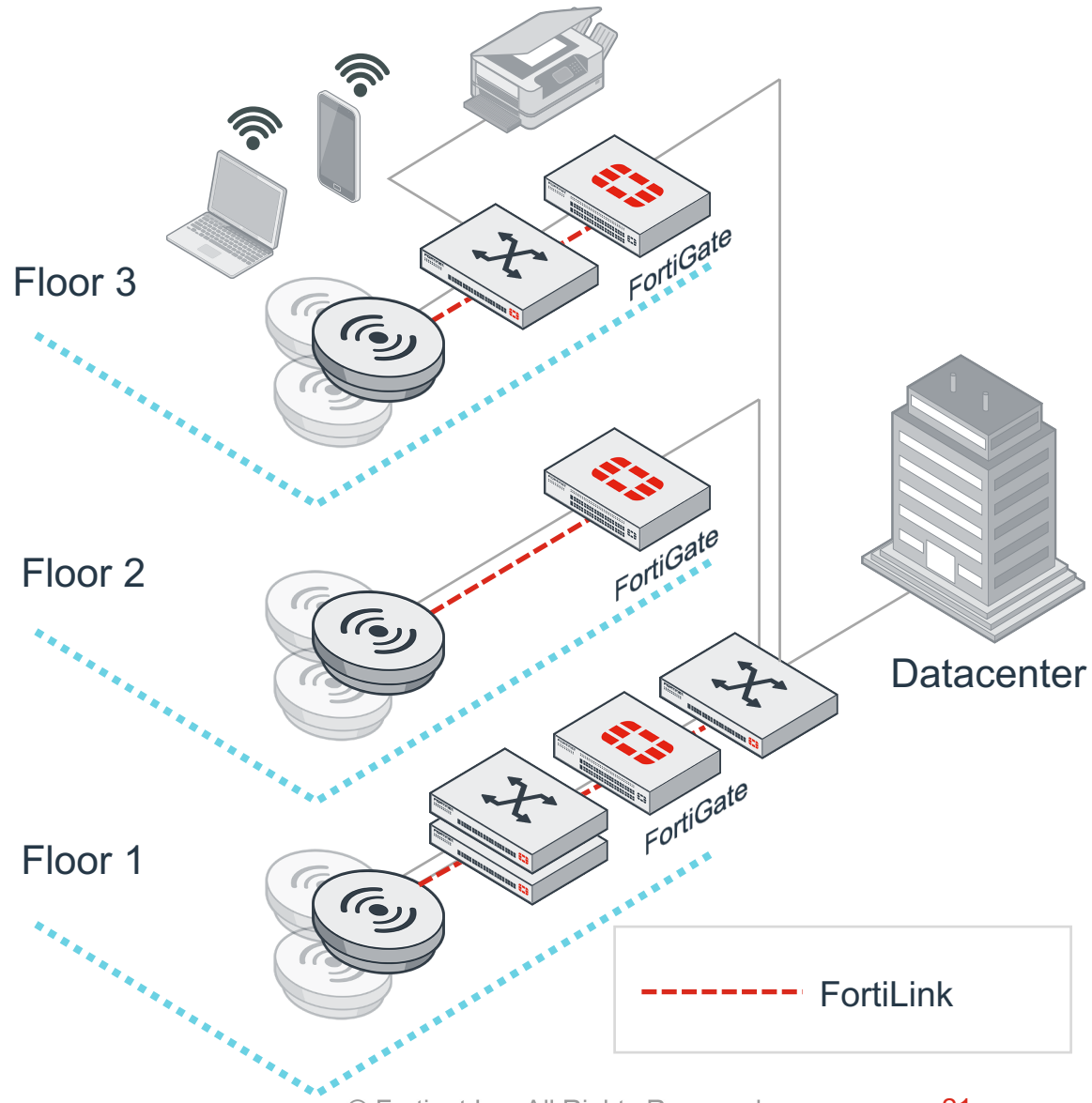
SD-Branch

Teleworker

Сценарии применения

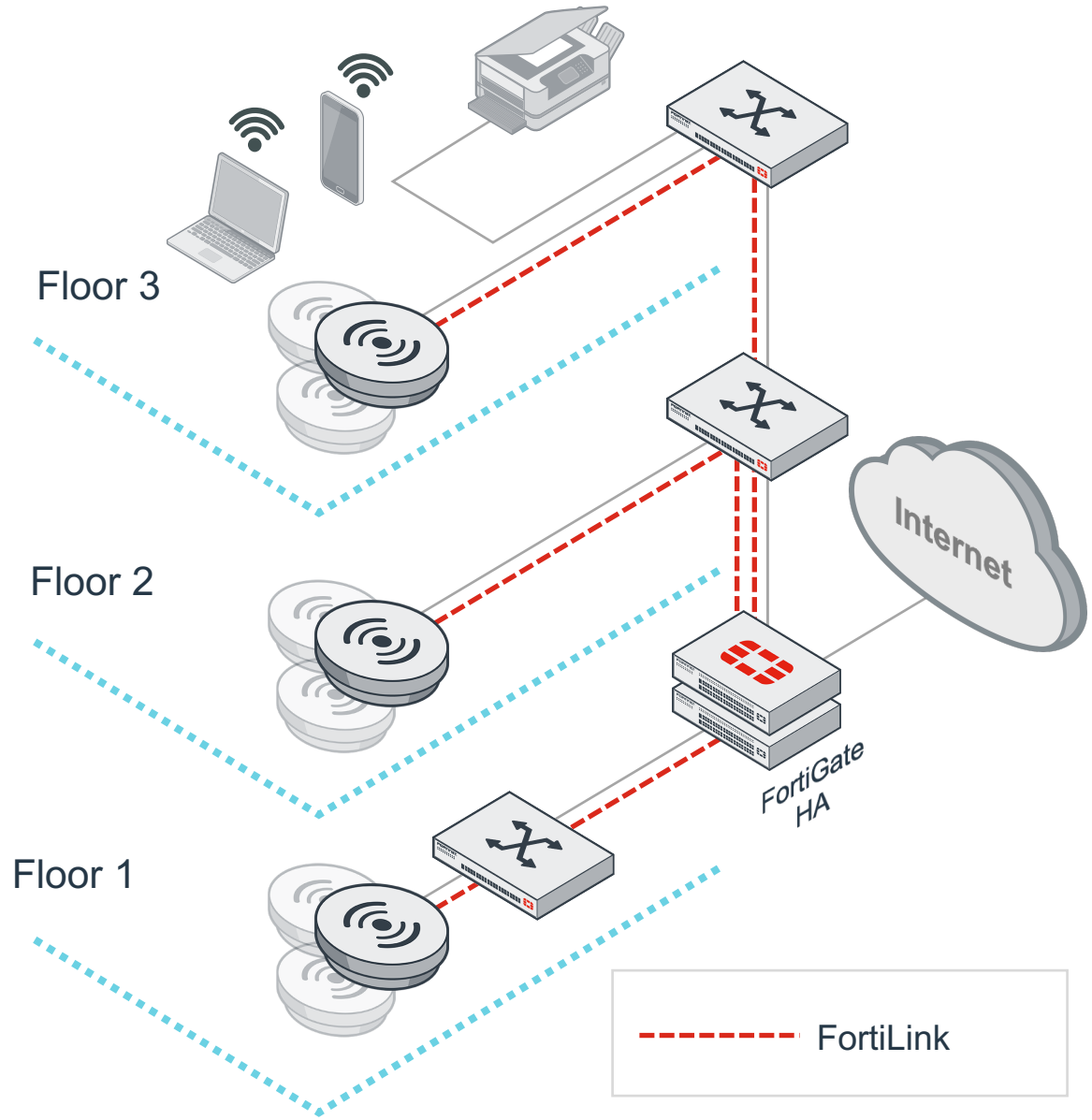
Кампусная сеть

- 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

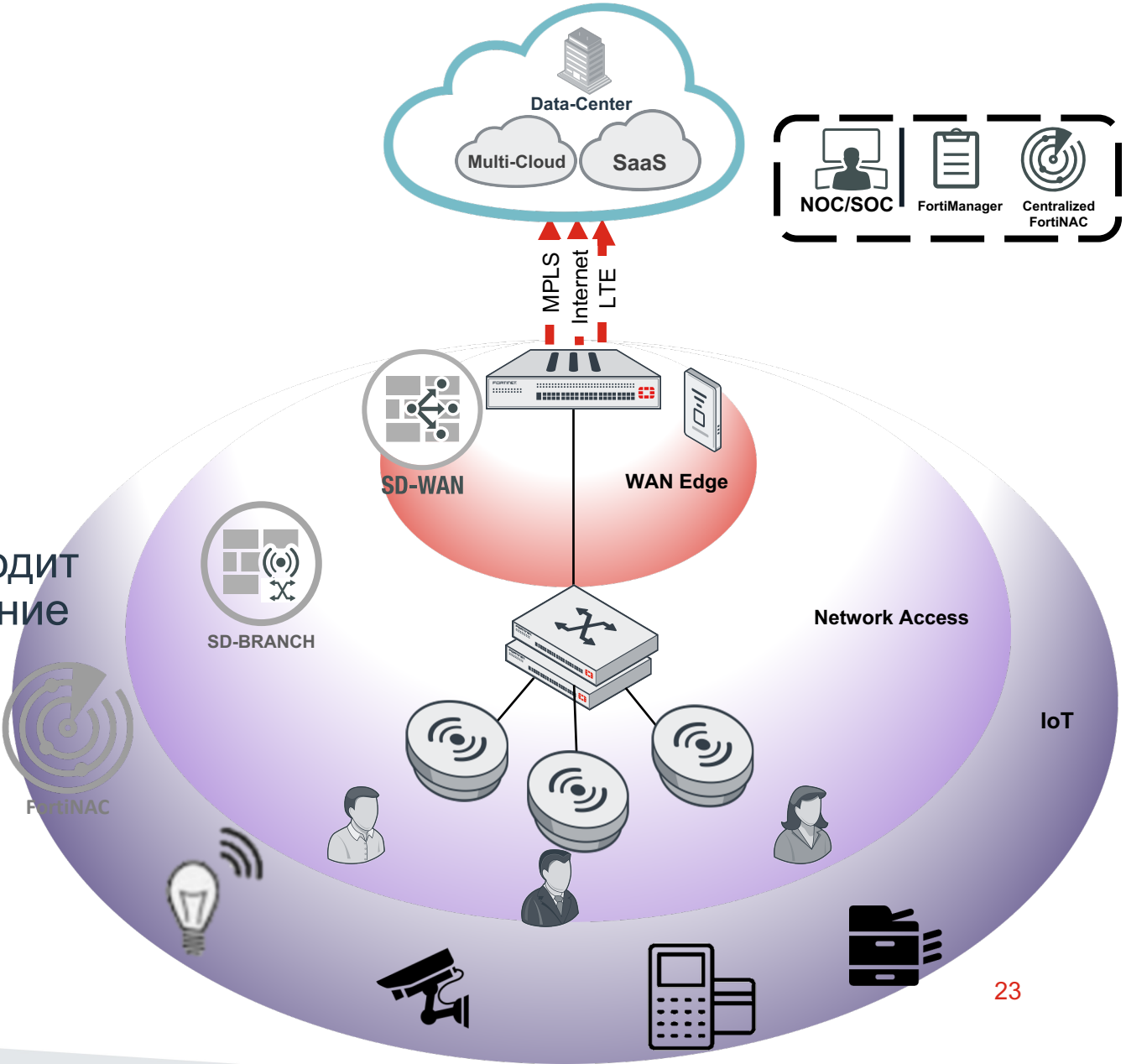


Интеллект на уровне контроля доступа

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**

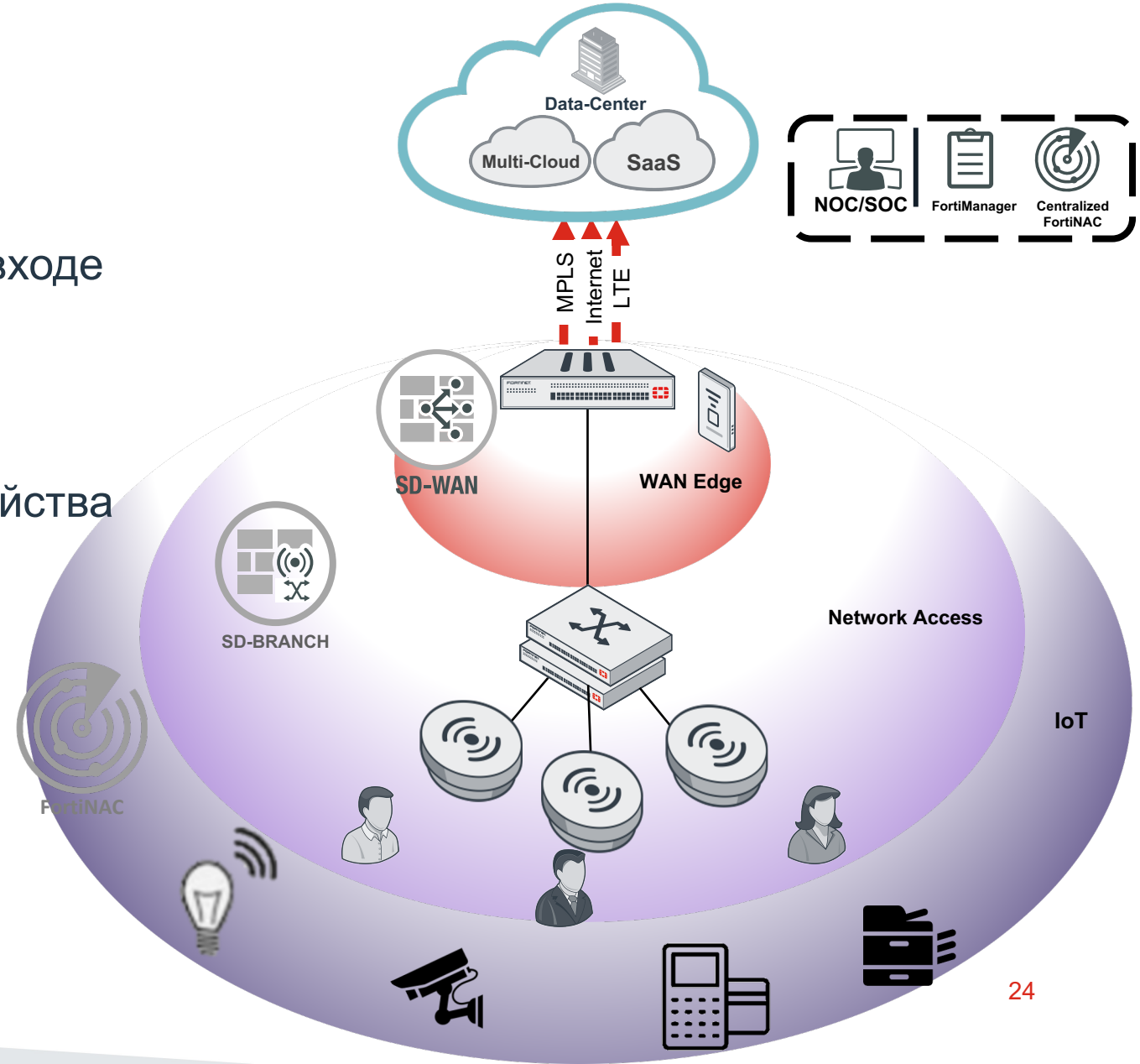


Интеллект на уровне контроля доступа

Пример: FortiNAC

FortiNAC защиты на уровне устройств

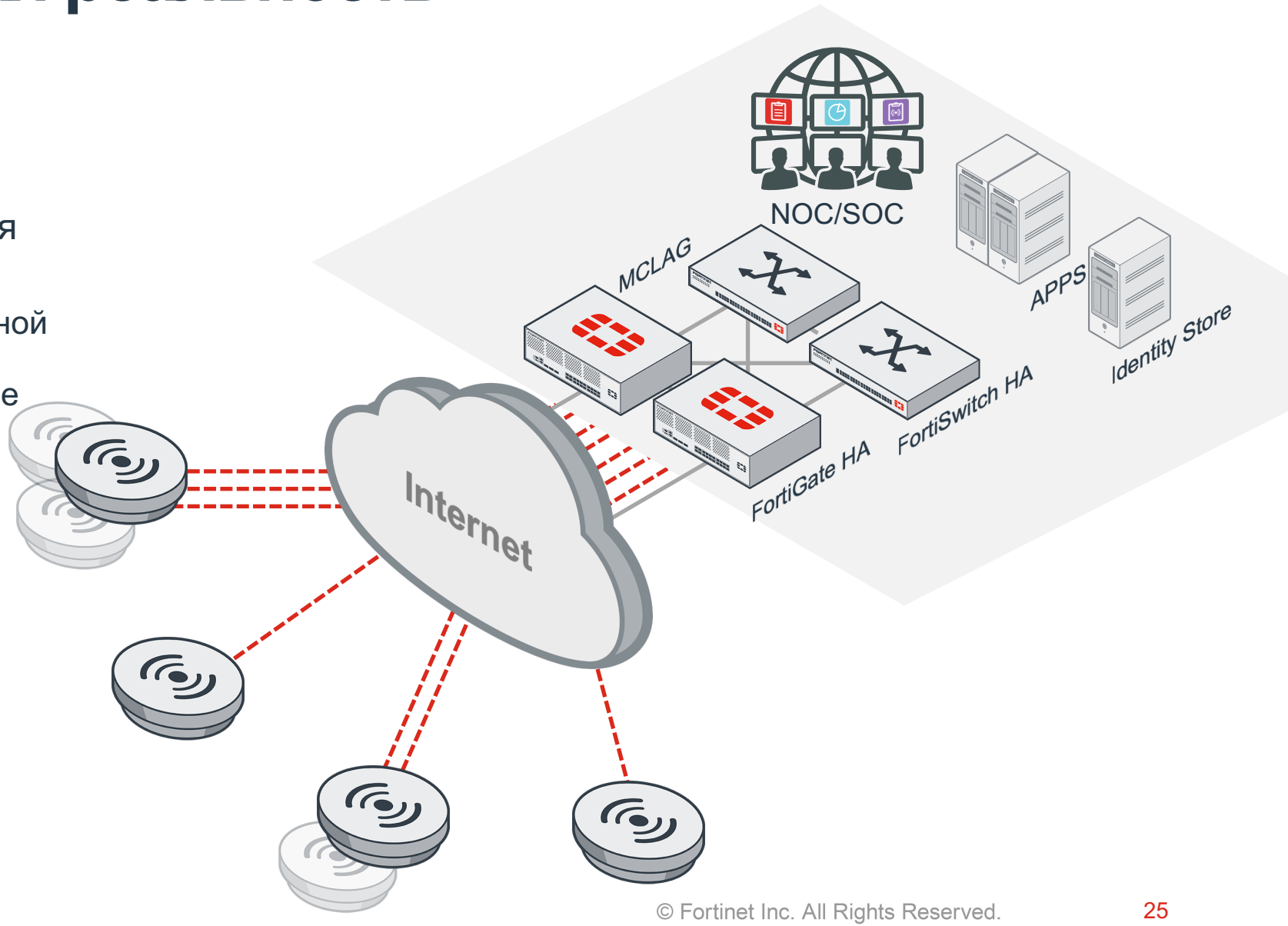
- Обнаружение, классификация, контроль, профилирование, оценка состояния при входе устройств в сеть
- Увеличение видимости и обнаружение аномалий
- FortiGate как сенсор, не нужны доп. устройства



«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)

FortiAP

Controller (FortiWLC)

AP

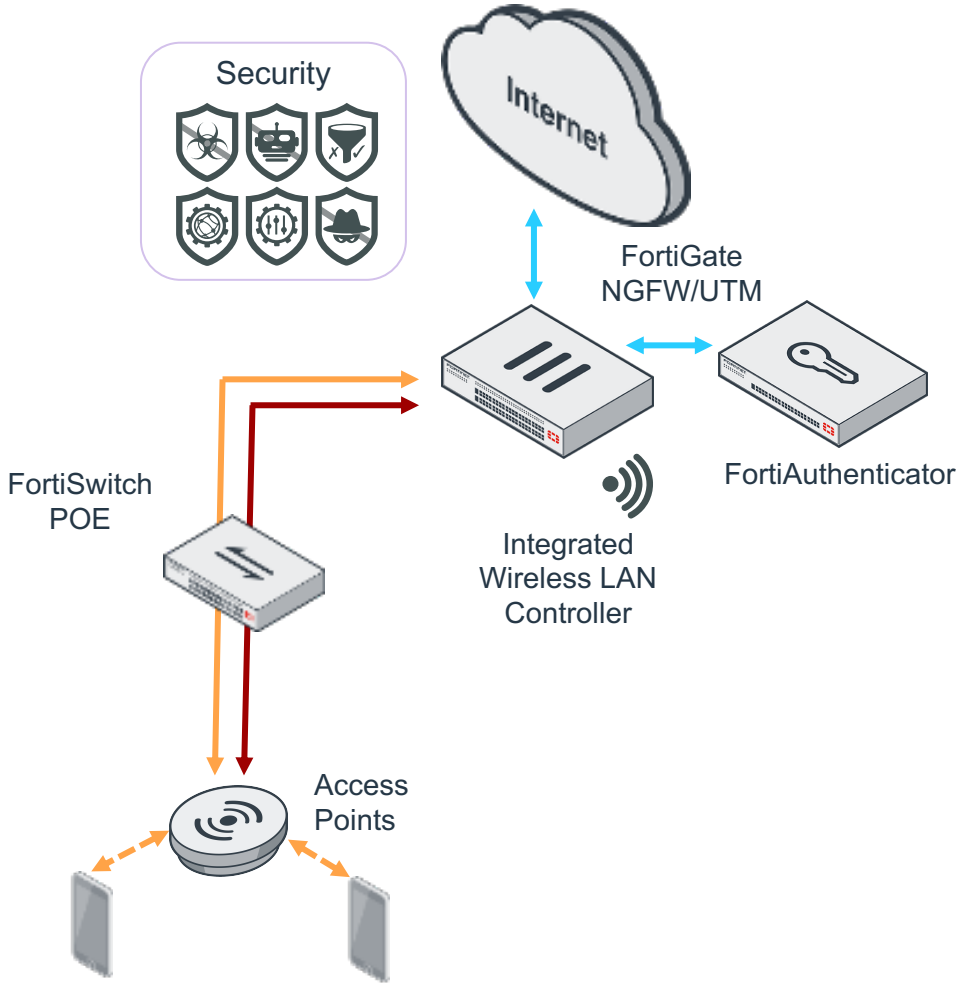
FortiAP-U

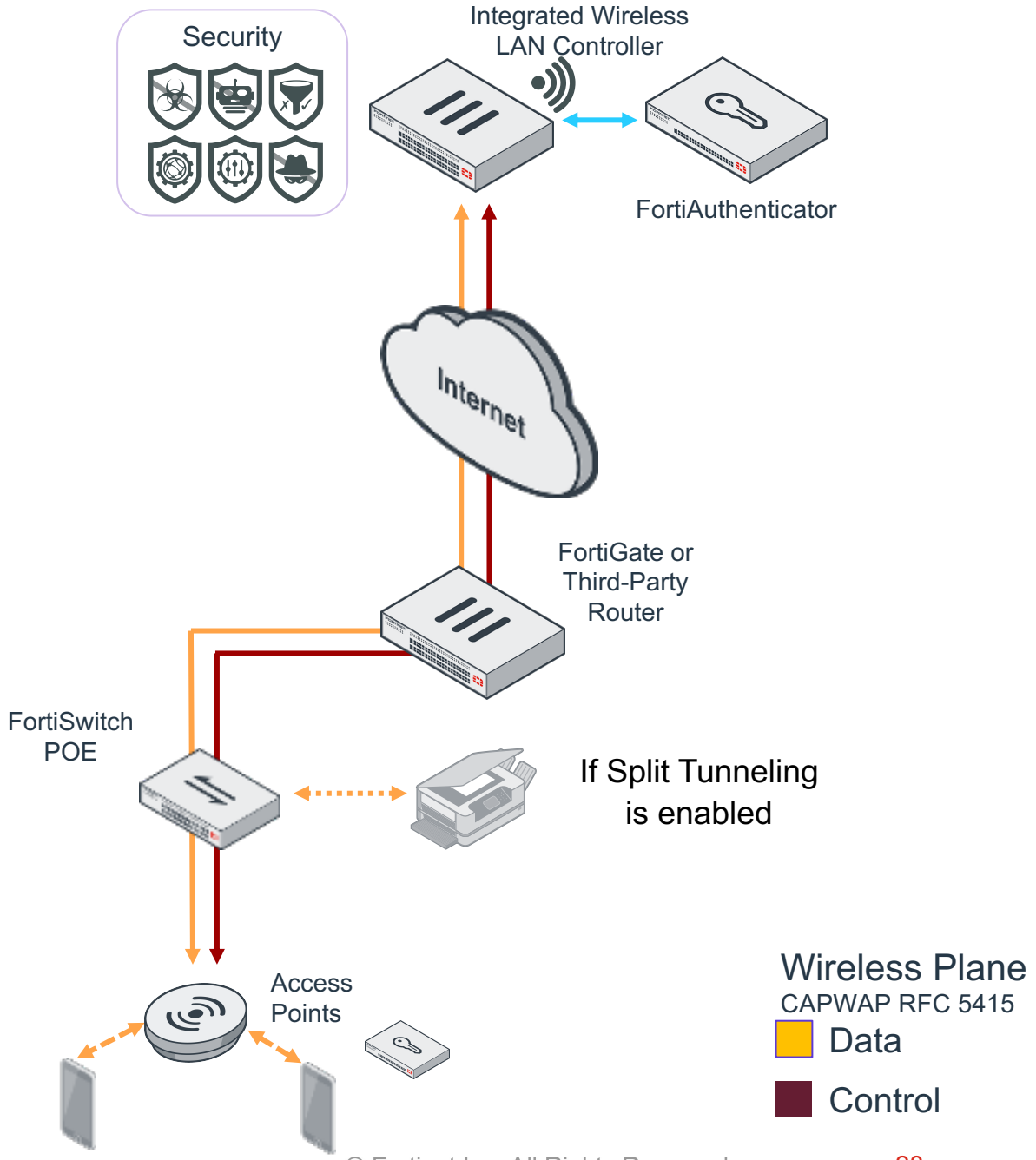
Cloud

FortiAP

Tunnel Mode

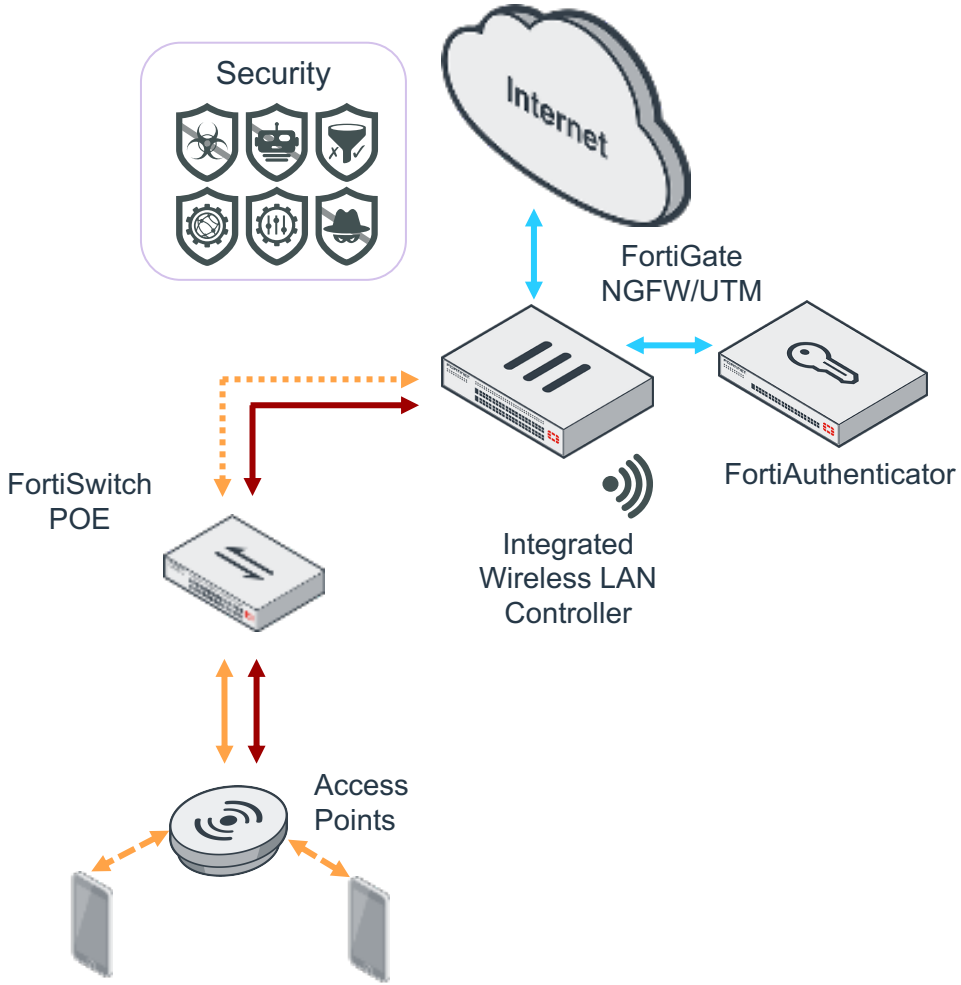
Сценарии применения

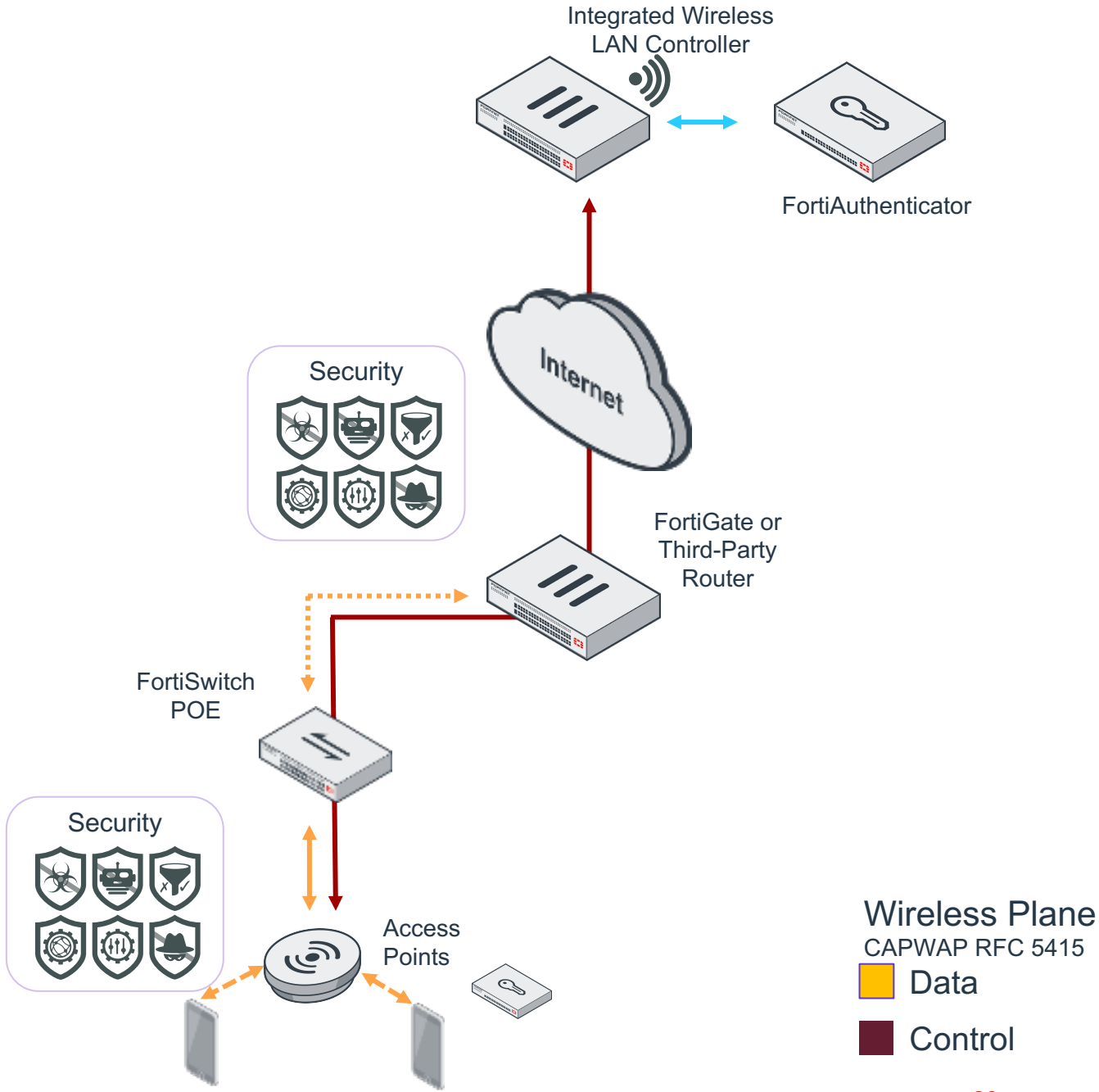




Local Bridge Mode

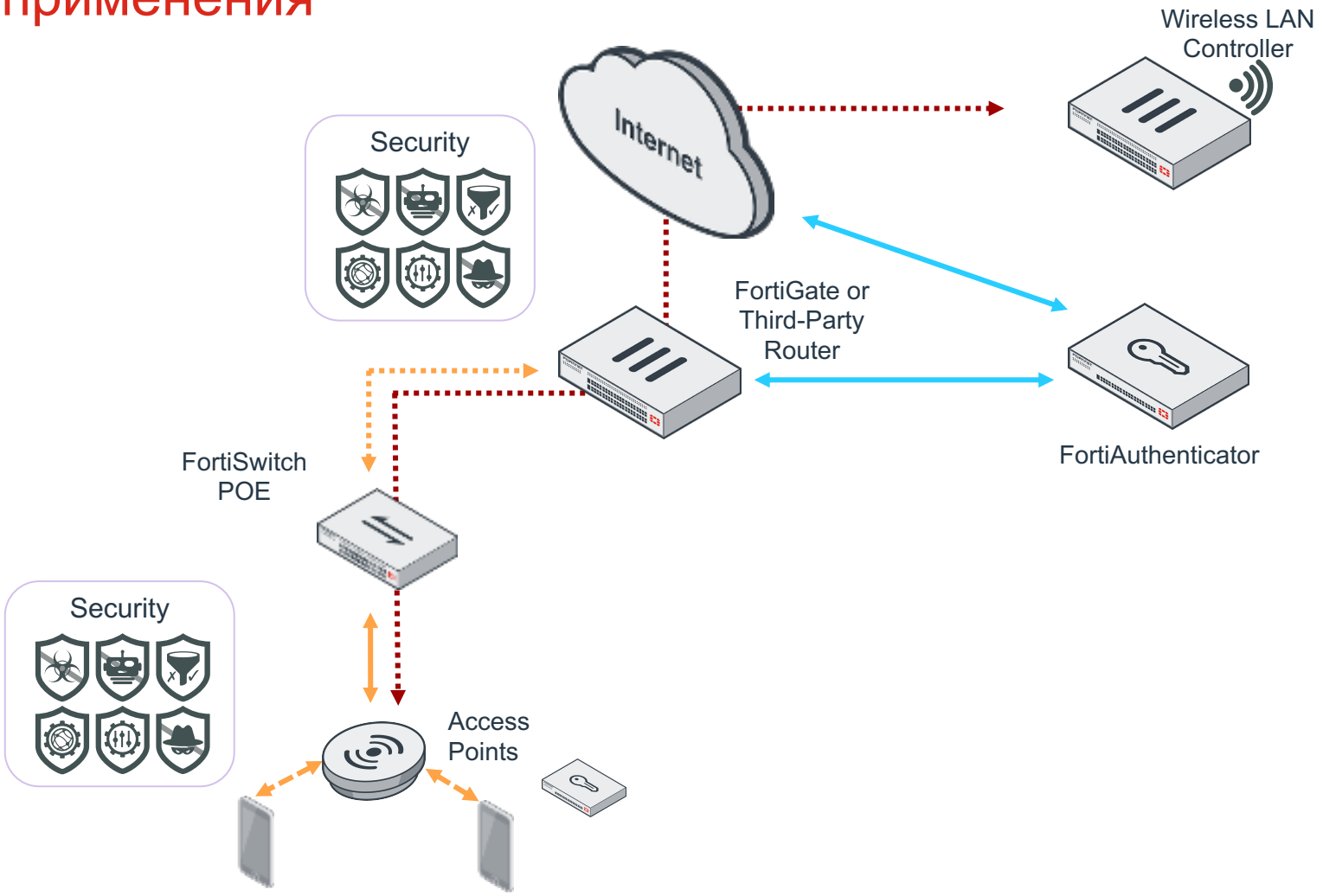
Сценарии применения





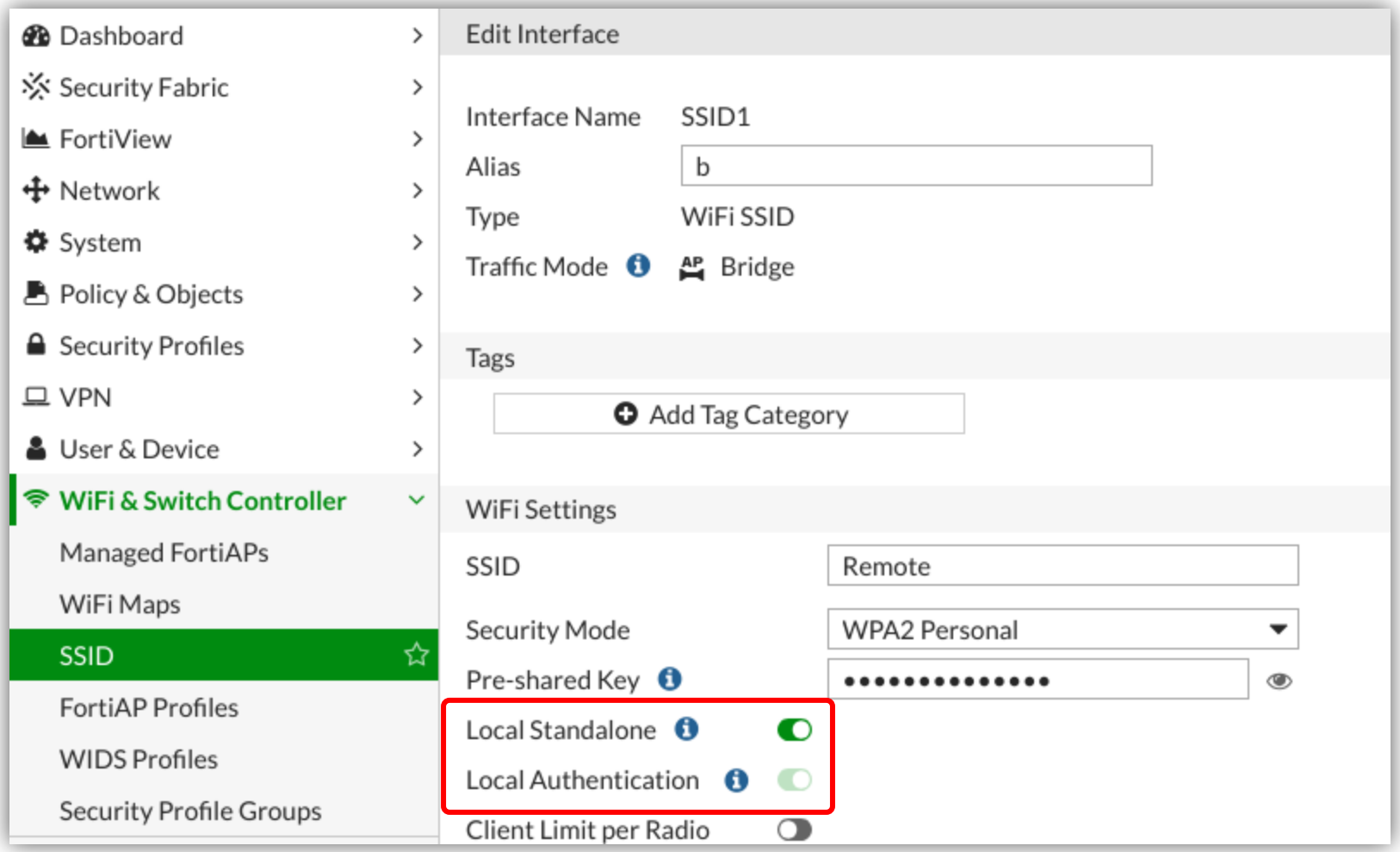
Local Standalone

Сценарии применения



Local Standalone

Configuration



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

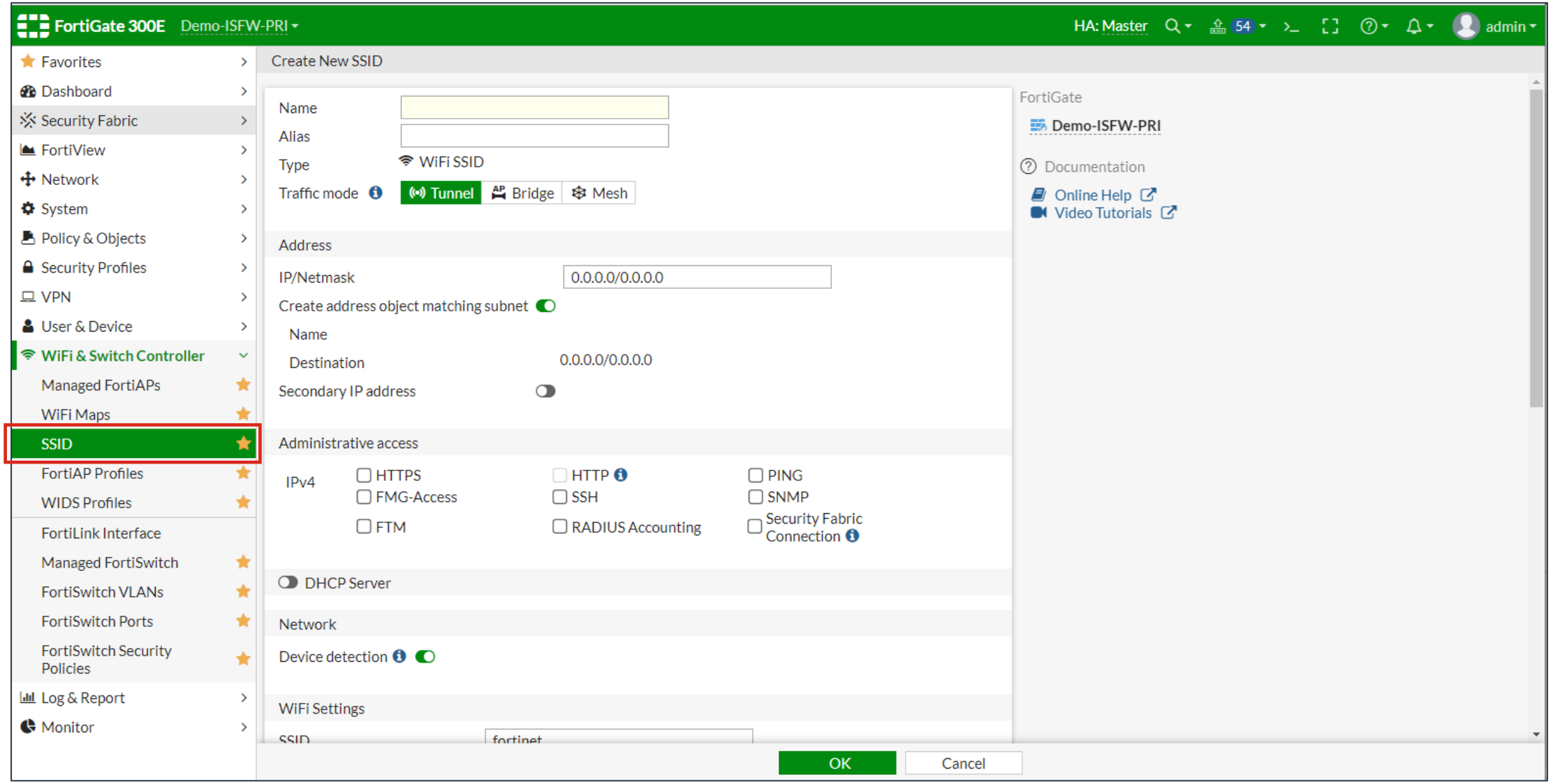
Feature	Tunnel	Local Bridge	Local Standalone
	Authentication		
Captive Portal	Yes	No	No
MAC-Auth Captive portal bypass	Yes	No	No
RADIUS Authentication	Yes	Yes	Yes
RADIUS Accounting	Yes	Yes	Yes
RADIUS CoA	Yes	Yes	Yes
RADIUS Dynamic VLAN	Yes	Yes	Yes
RADIUS User Group	Yes	Yes	Yes
	Wireless		
Probe response 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
	Deployments		
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
	Security		
Client Quarantine	Yes	No	No
UTM On FAP	No	Yes	Yes

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

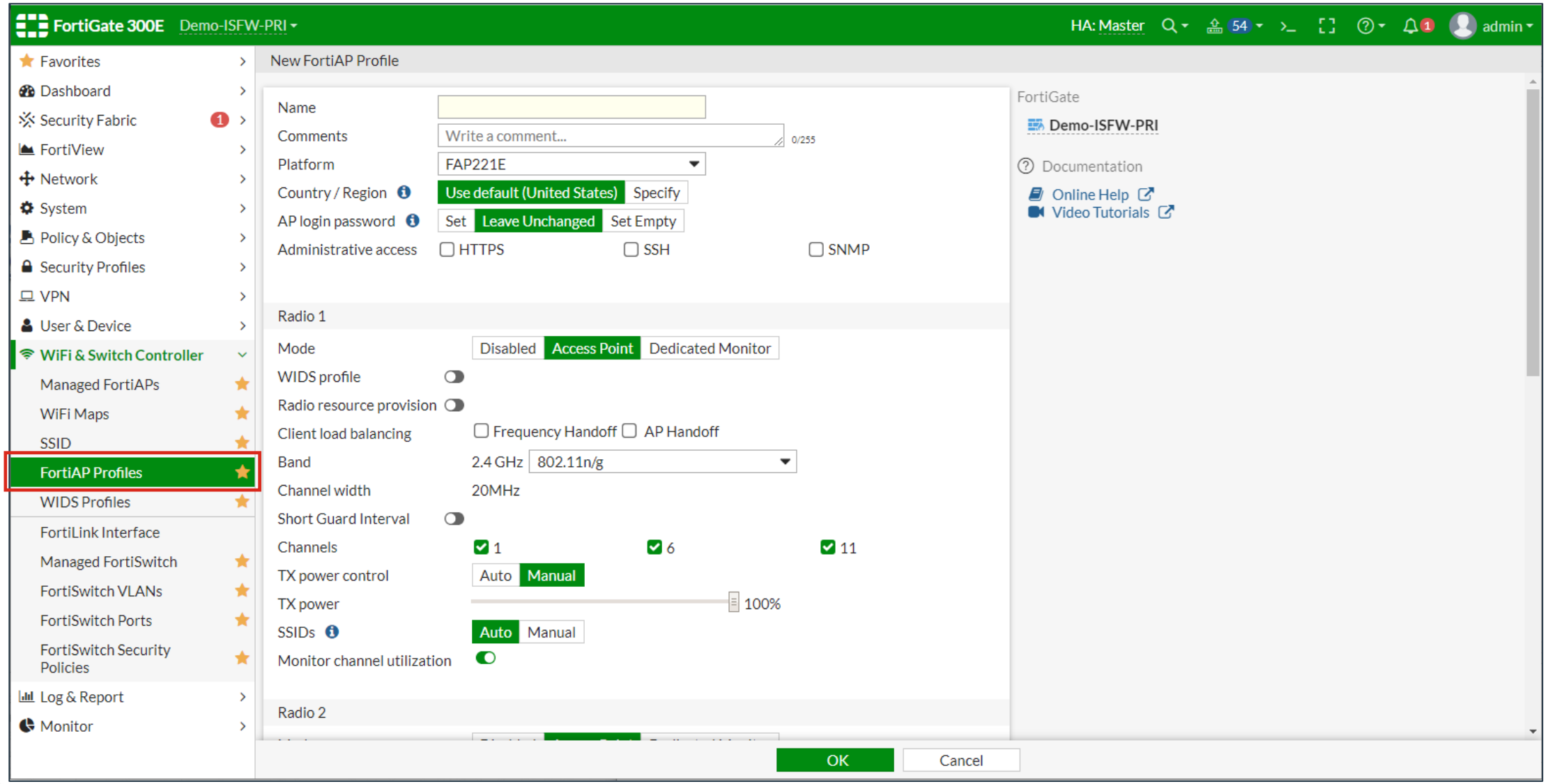
FortiOS Wireless Controller

Примеры настройки

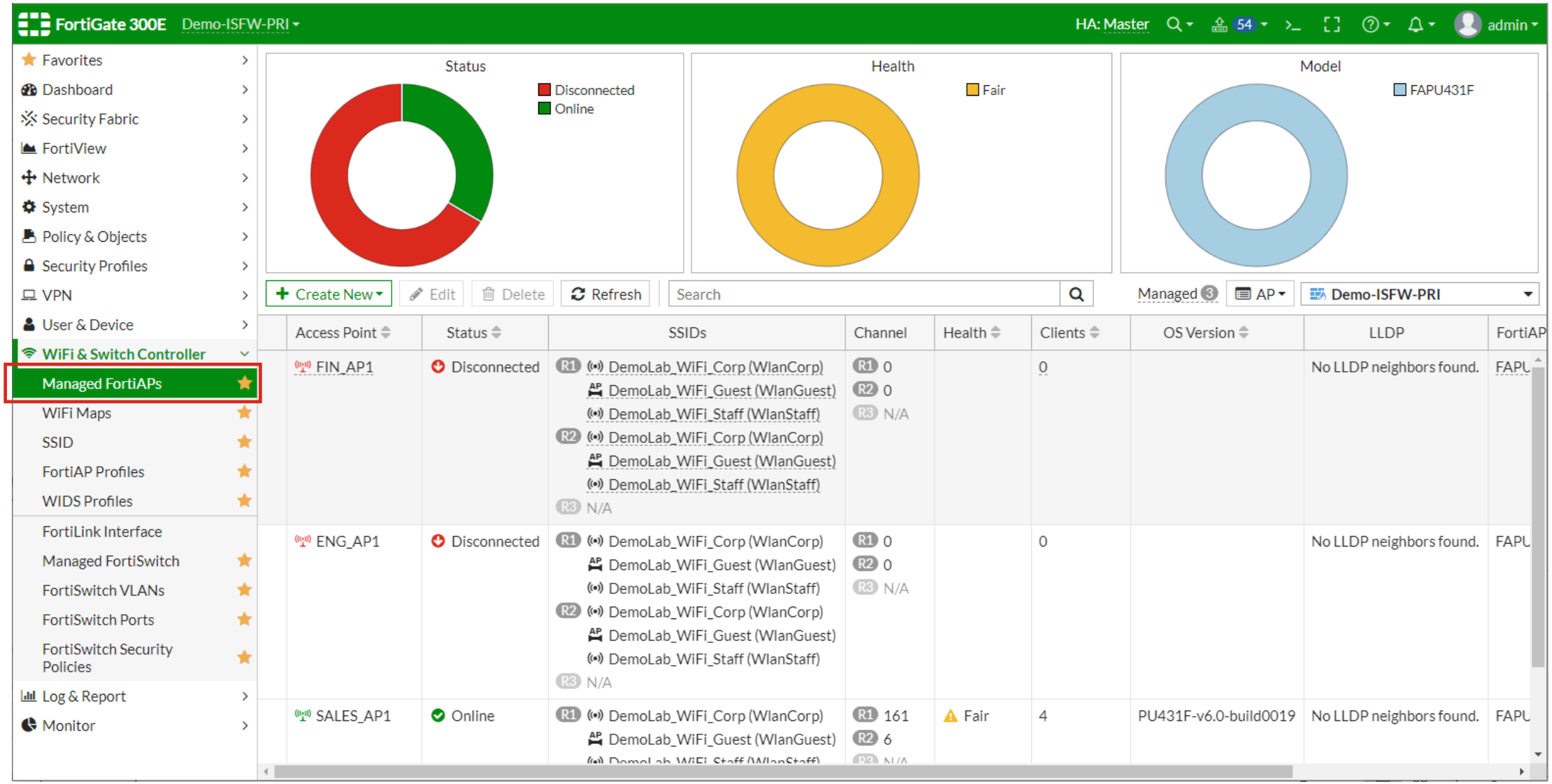
Create SSID



AP Profile

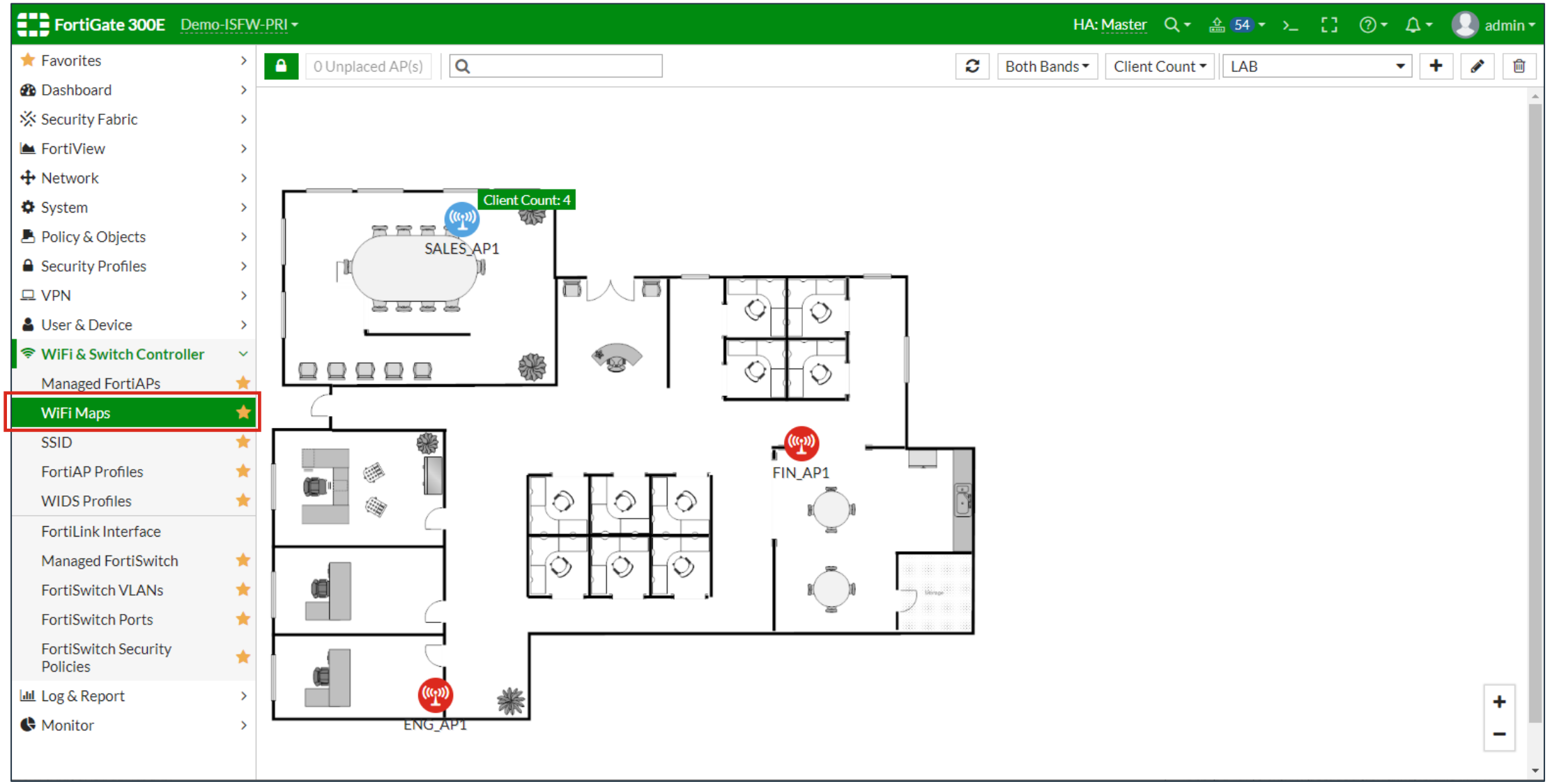


Managed APs

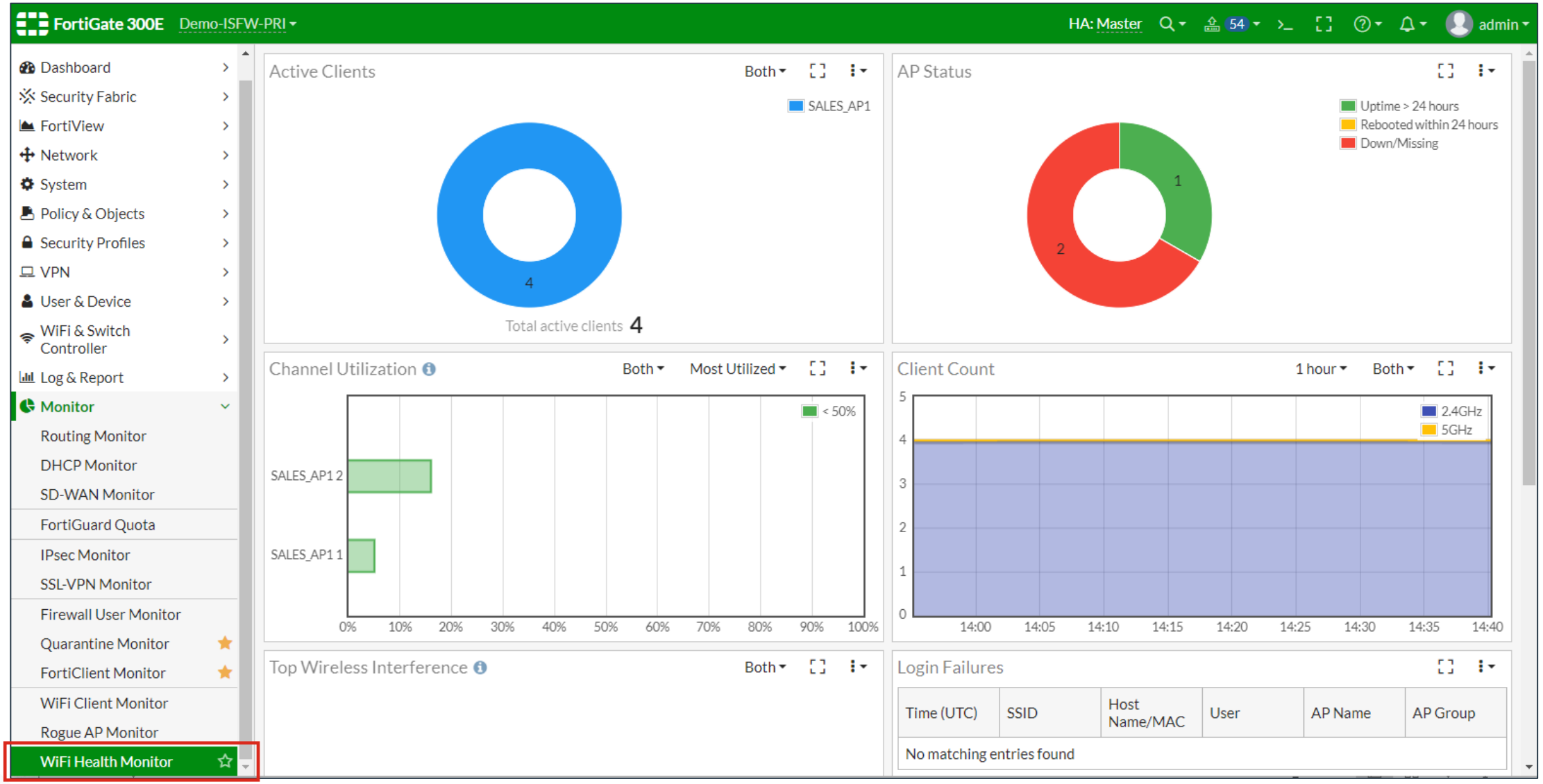


AP Details (w/ Spectrum)

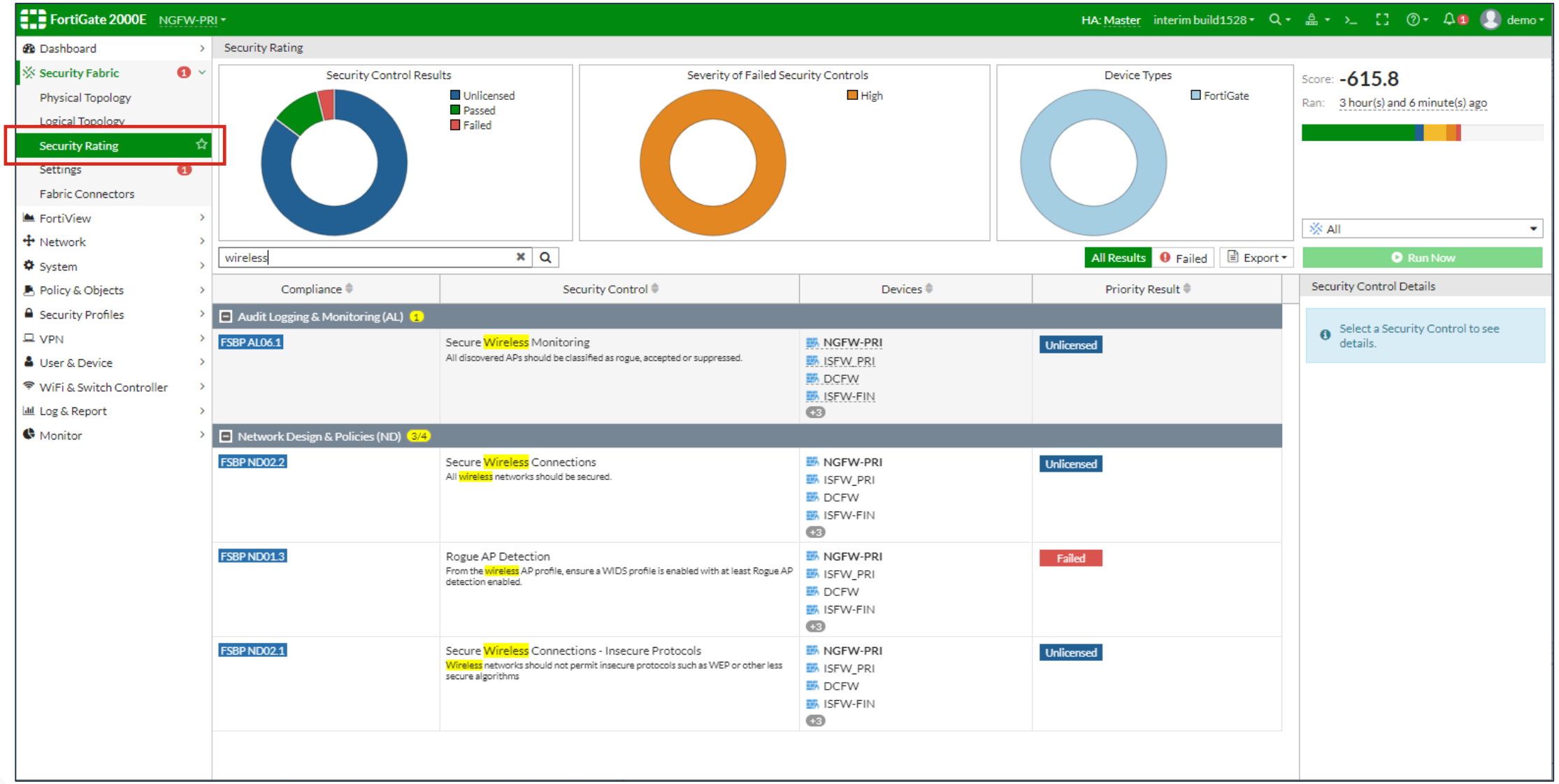
MAP



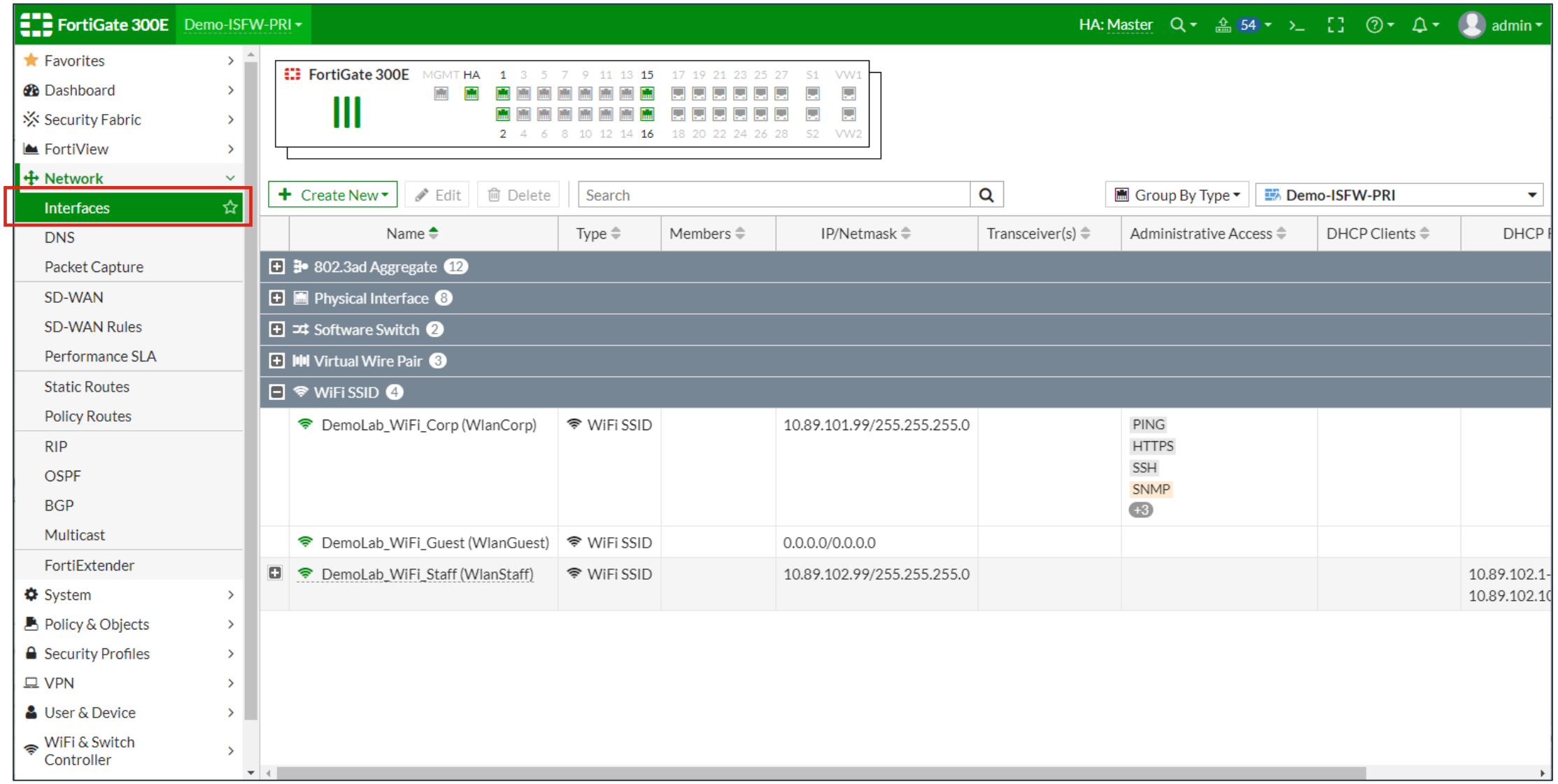
Wi-Fi Overview



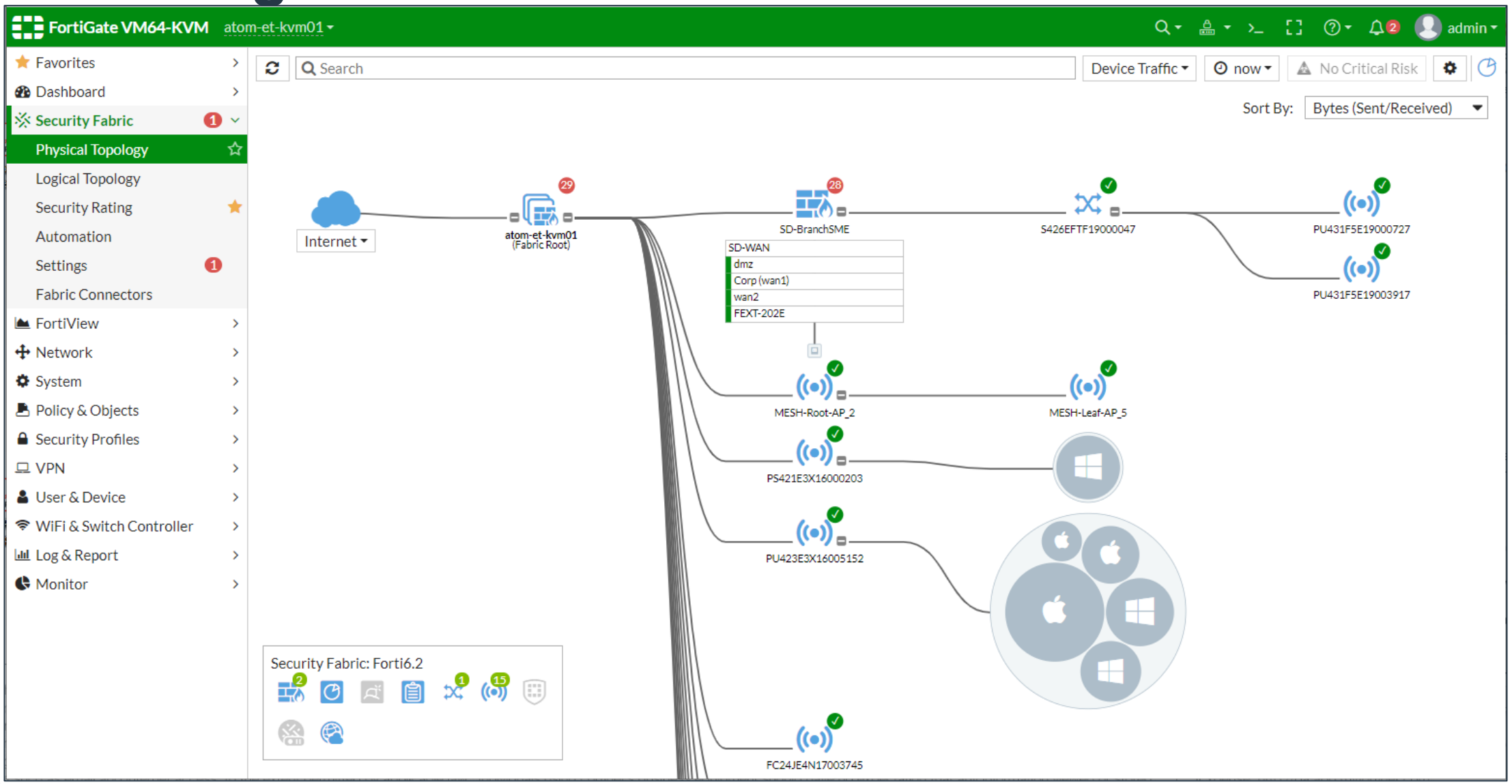
Security Rating



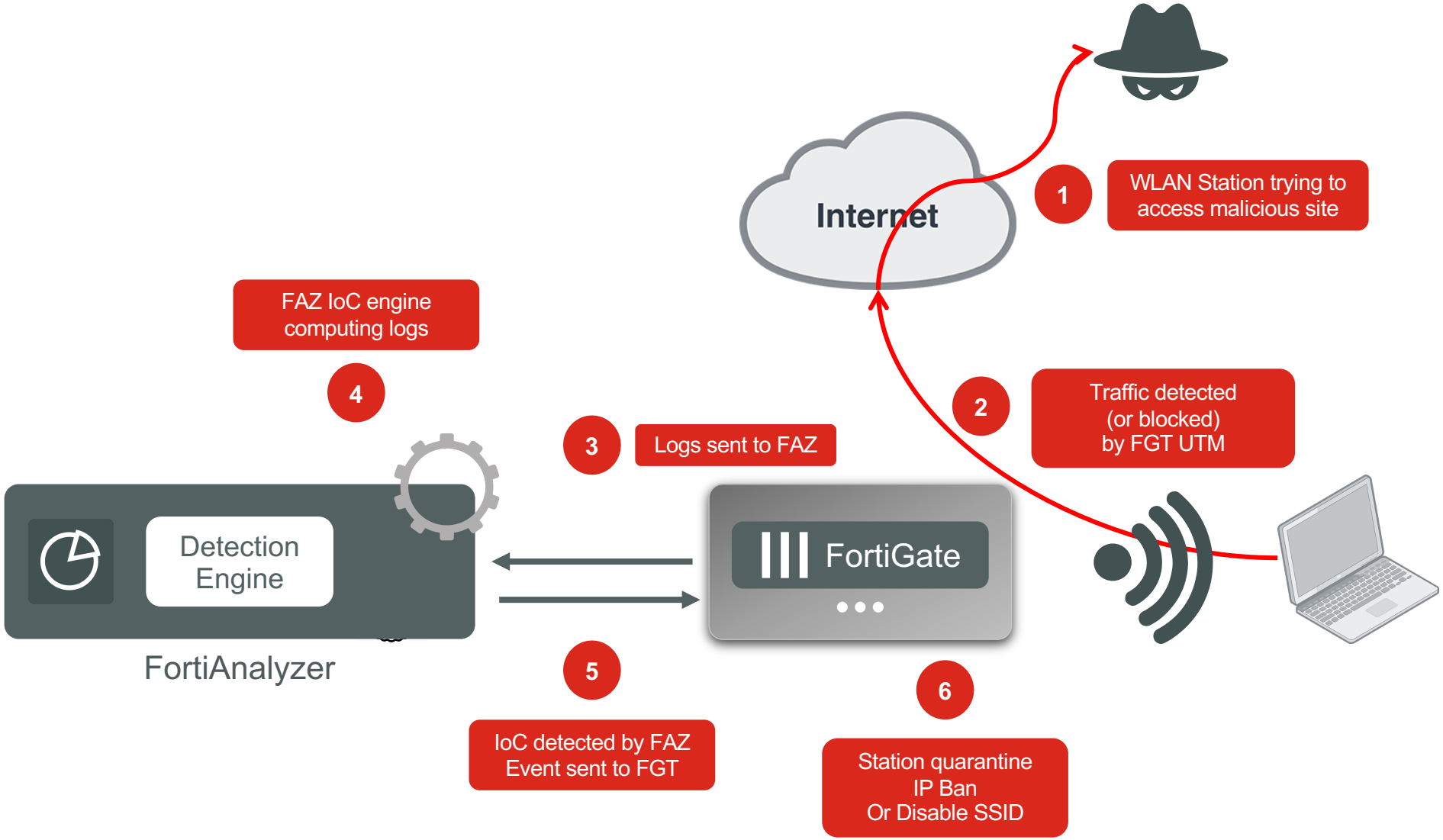
Интерфейсы (в том числе SSIDs)



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

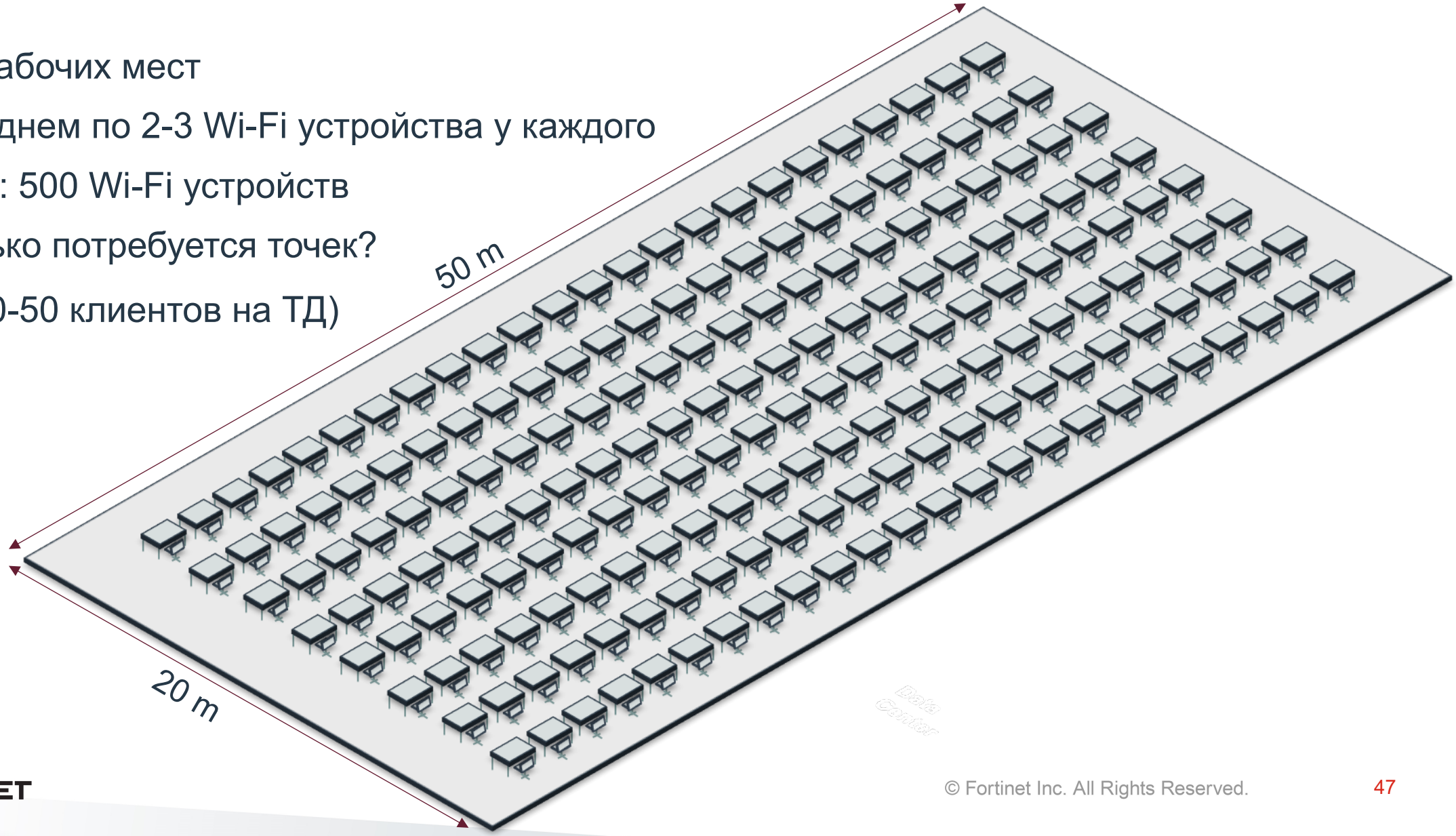
FWC-3000D
3000 точек доступа
45К клиентов

✓ Не нужны лицензии на точки для новых FWC

В чем основные сложности при строительстве современных БЛВС?

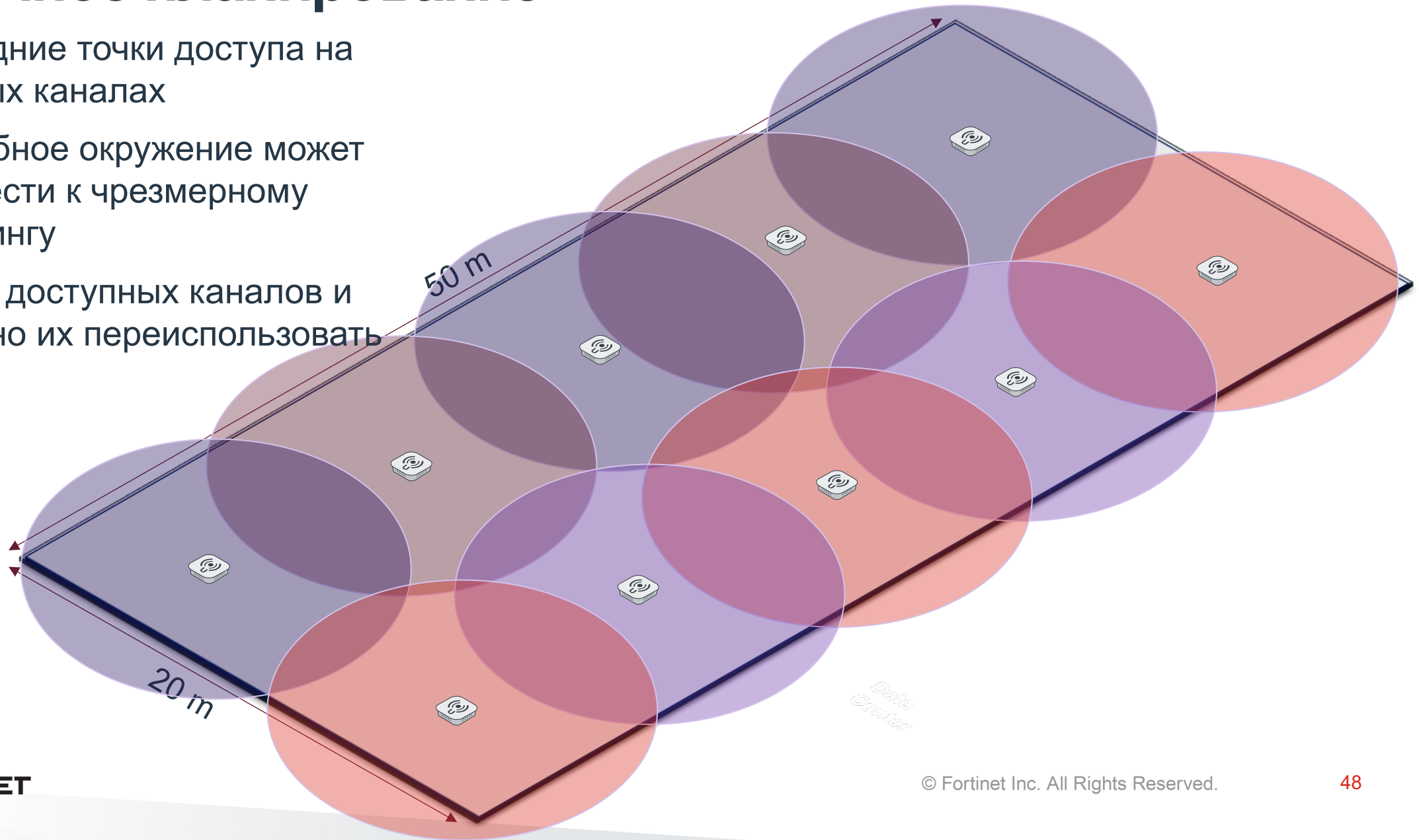
Обычный офис

- 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)



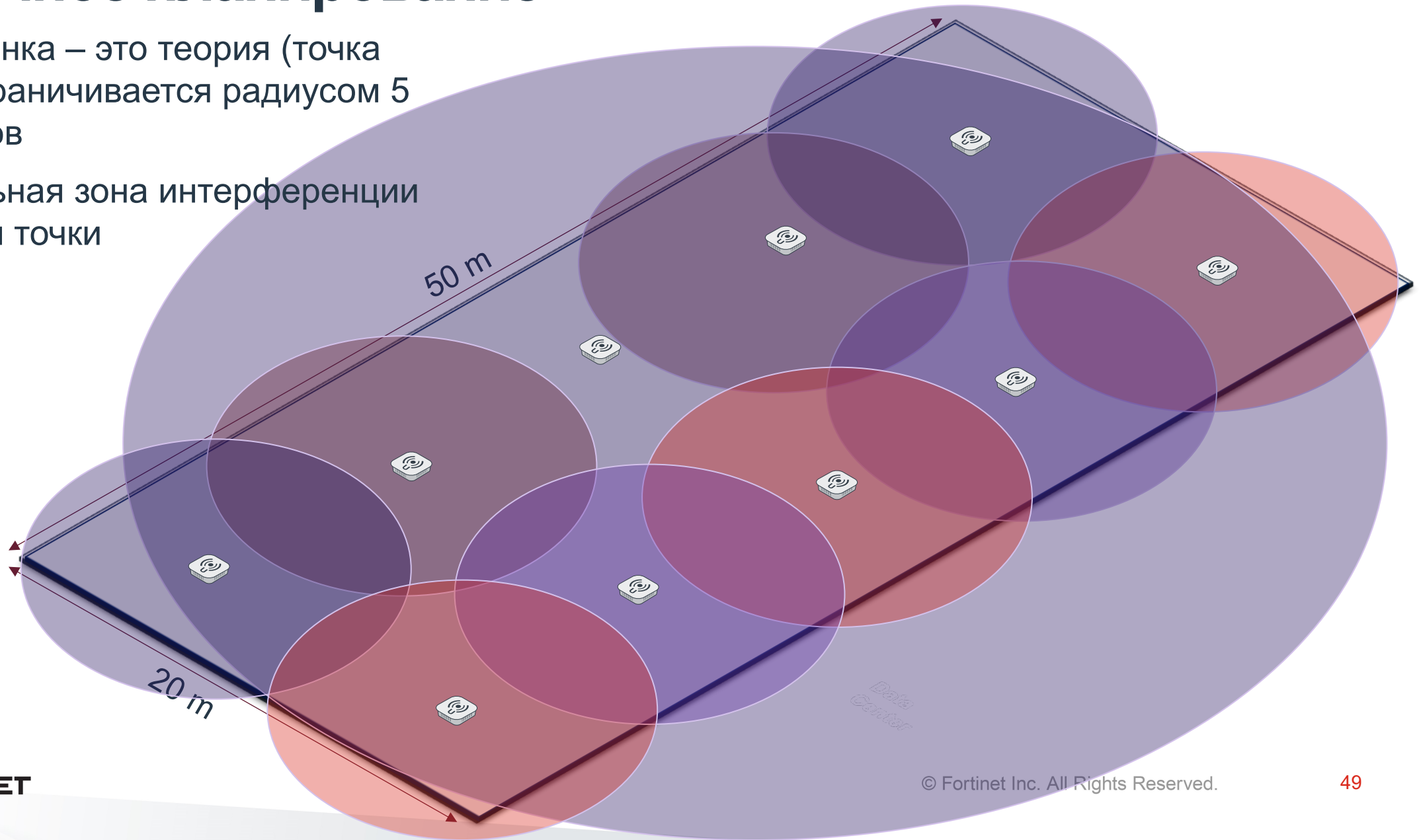
Обычное планирование

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



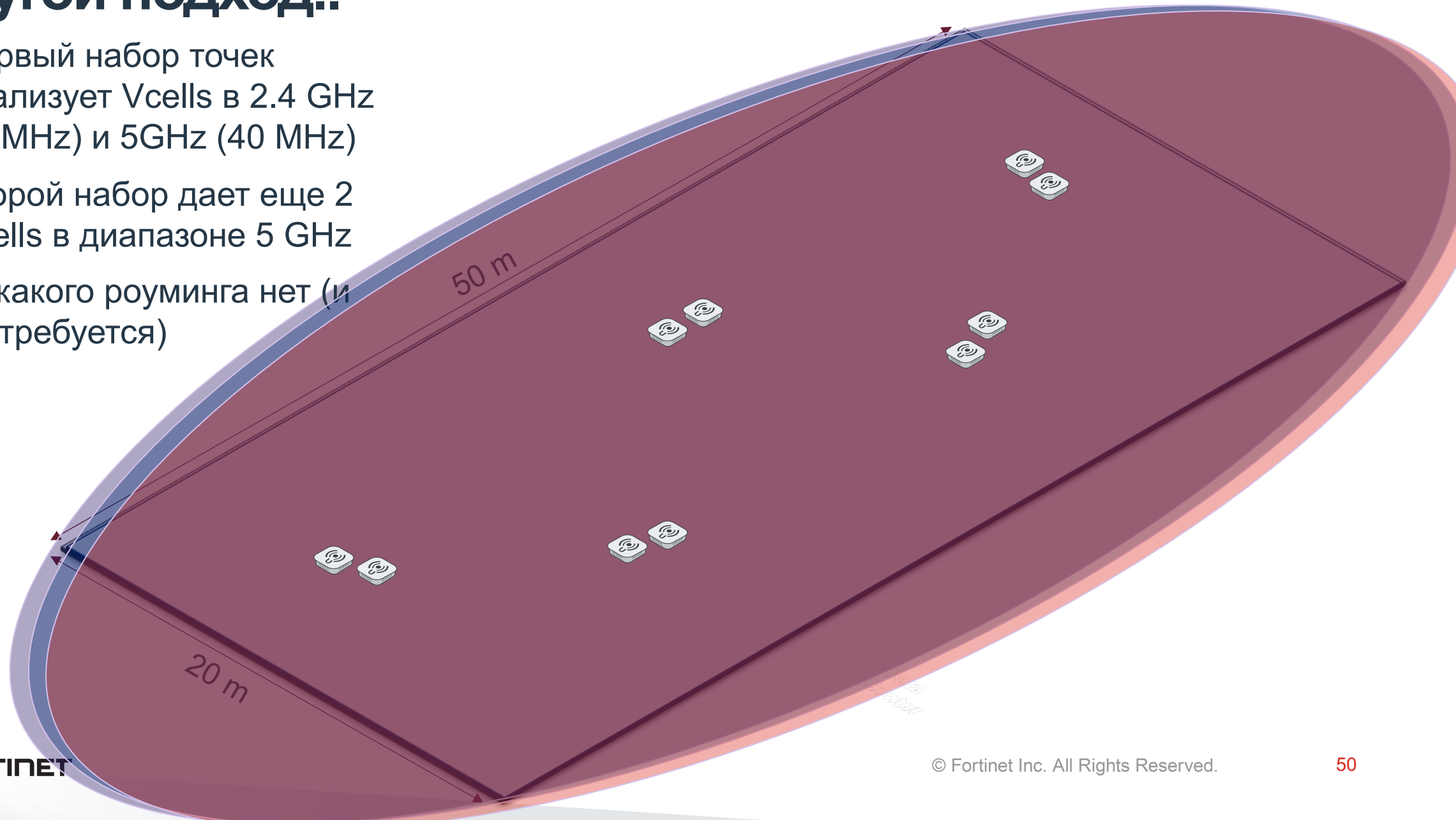
Обычное планирование

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



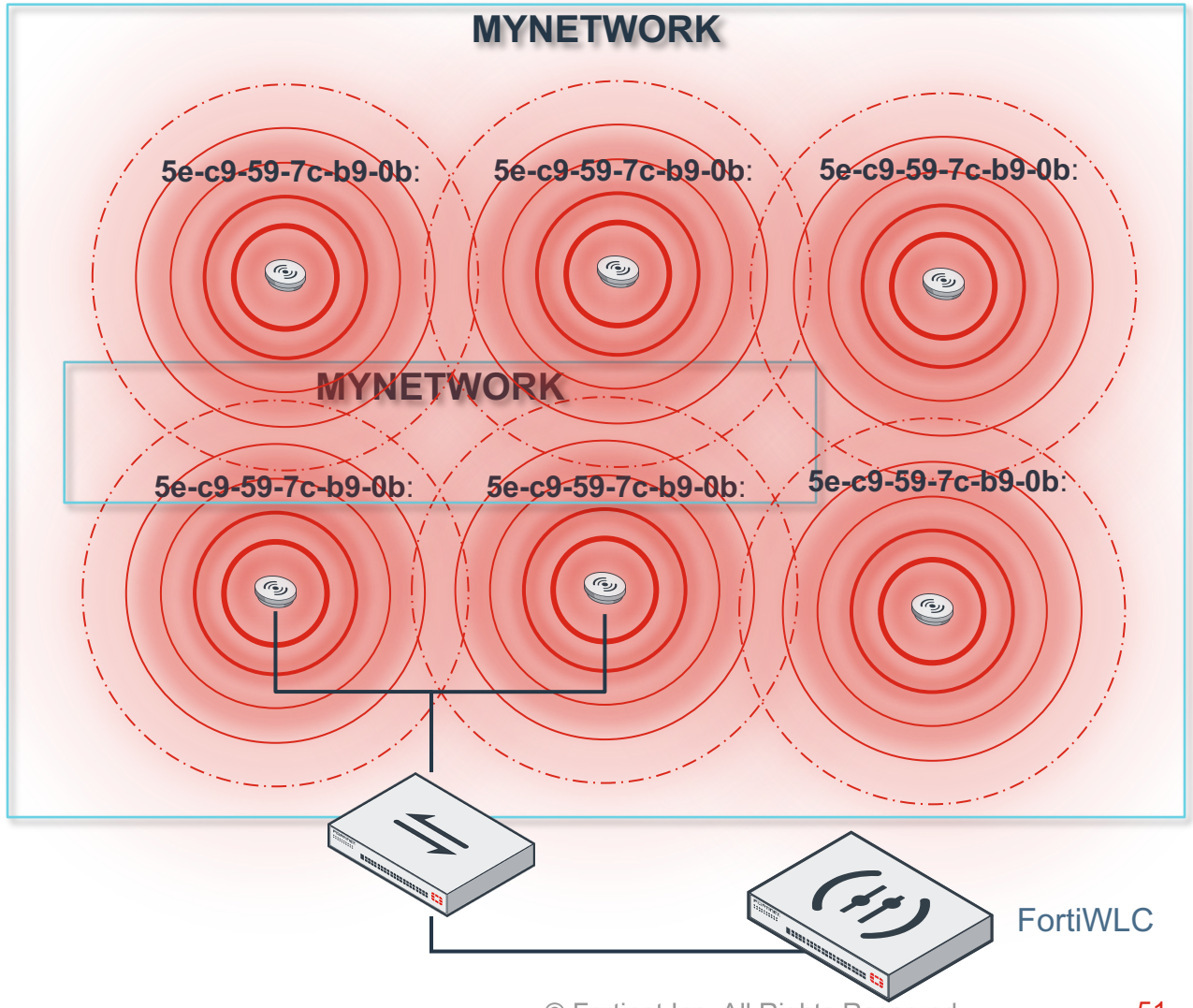
Другой подход..

- 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)



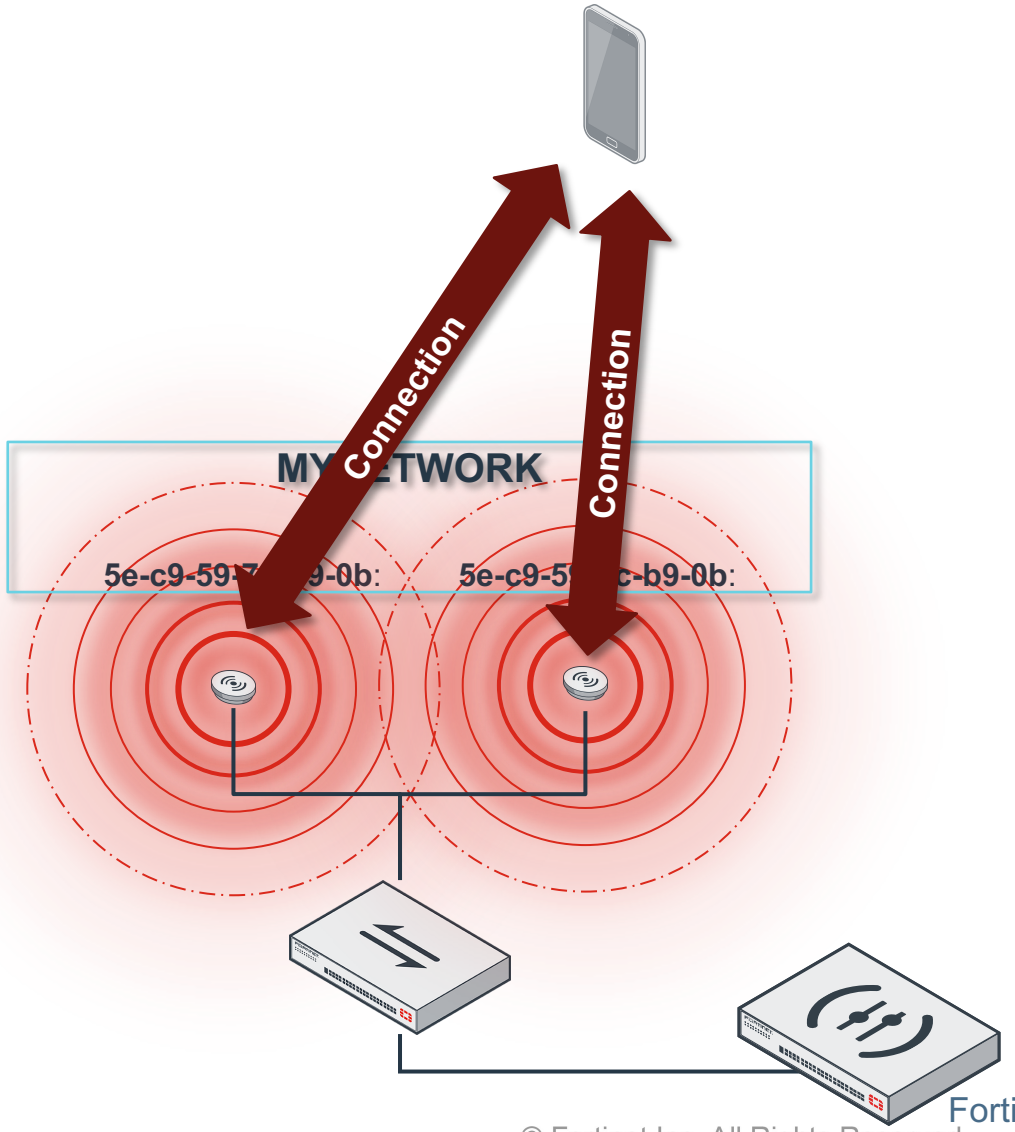
Virtual Cell – виртуализация Wi-Fi сети

- 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

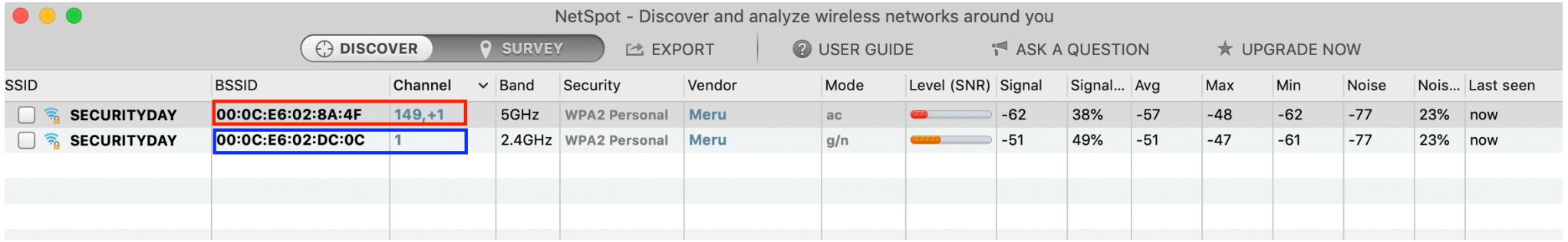


Virtual Cell – процесс роуминга

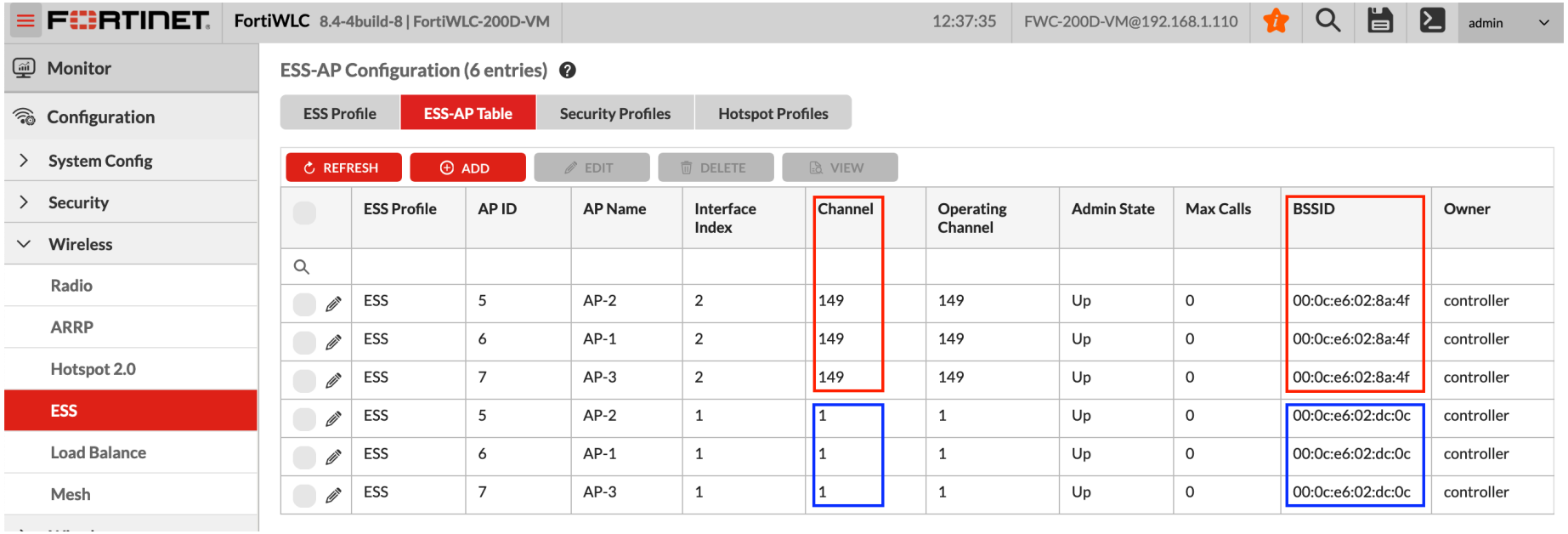
- Когда клиент перемещается…
  - Он видит только одну «точку доступа»
  - Контроллер отслеживает SNR клиента
  - .. и когда это необходимо, переключает его на соседнюю точку доступа в рамках того же vcell
  - Клиент продолжает работу и не осведомлен, что теперь он работает физически с другой точкой доступа



Virtual Cell – виртуализация Wi-Fi сети



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



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

Различия между MCA 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


GEORGIA WORLD CONGRESS CENTER


ADELAIDE CONVENTION CENTRE


99
Koosier


FORTINET