FORTINET®

VIRTUAL

SECURITY DAY

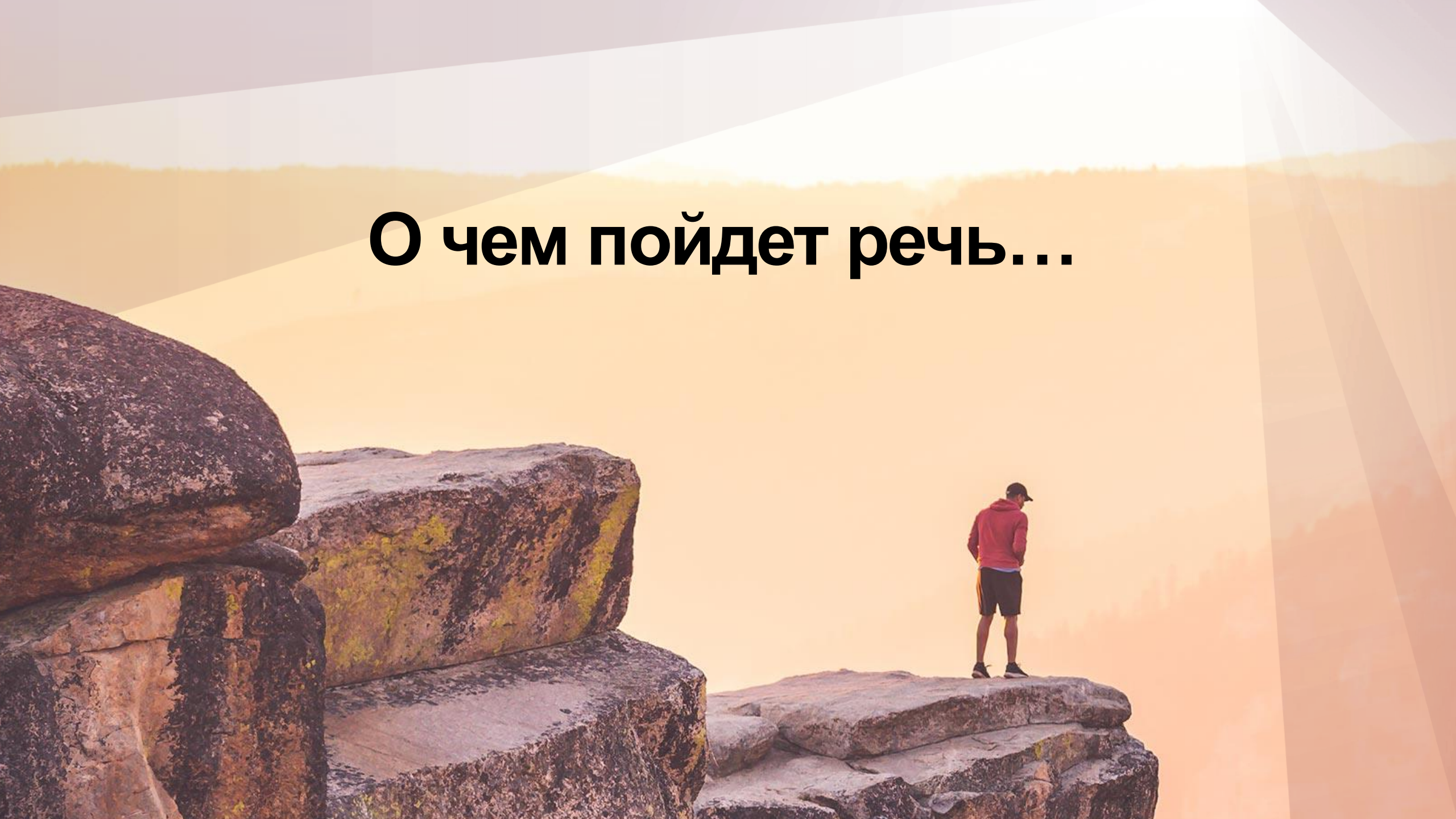
Современная инфраструктура доступа компании с встроенной безопасностью

Юрий Захаров

Системный инженер

yzakharov@fortinet.com

О чем пойдет речь…



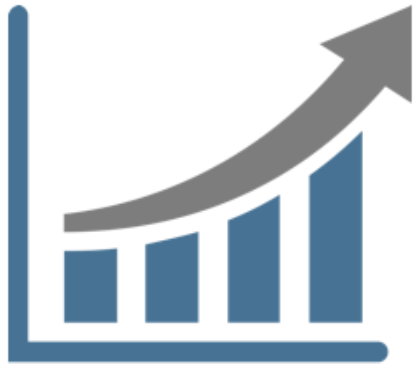
О чем пойдет речь…

- ✓ 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 точек доступа
- ✓ Обеспечение безопасности на уровне доступа
  - ❑ Решение для контроля доступа FortiNAC

FORTINET

Вызовы для уровня доступа

Количество устройств



- **30 млрд устройств к 2020**
- **Нехватка производительности средств защиты**

Безопасность

- **Угрозы становятся более продвинутыми**
- **Сложность при интеграции с устройствами безопасности**

Управление

- **Возрастают затраты на персонал**
- **Увеличивается время на решение инцидентов**

FORTINET

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

Коммутаторы уровня доступа и контроллер коммутаторов

в операционной системе FortiOS

Безопасность уровня доступа компании

Коммутаторы FortiSwitch

FORTINET SECURITY FABRIC

Простое управление

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

Интегрированная безопасность

Самый защищенный коммутатор доступа (интеграция с FortiGate)

Интеграция с Fortinet Security Fabric расширяет возможности безопасности покрывая все виды угроз

Масштабируемость

Широкий модельный ряд оборудования

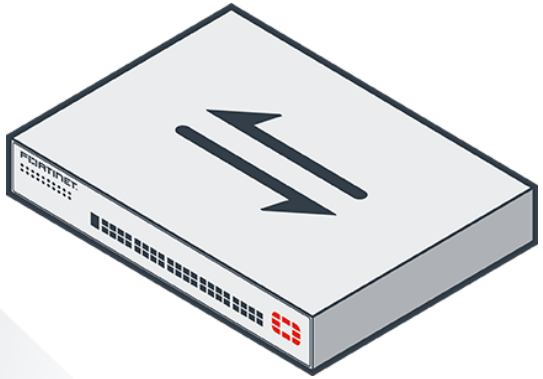
Стекирование коммутаторов

Аппаратная акселерация и коммутация без переподписки

Централизованное управление

Поддержка MCLAG

Встроенная безопасность



FORTINET

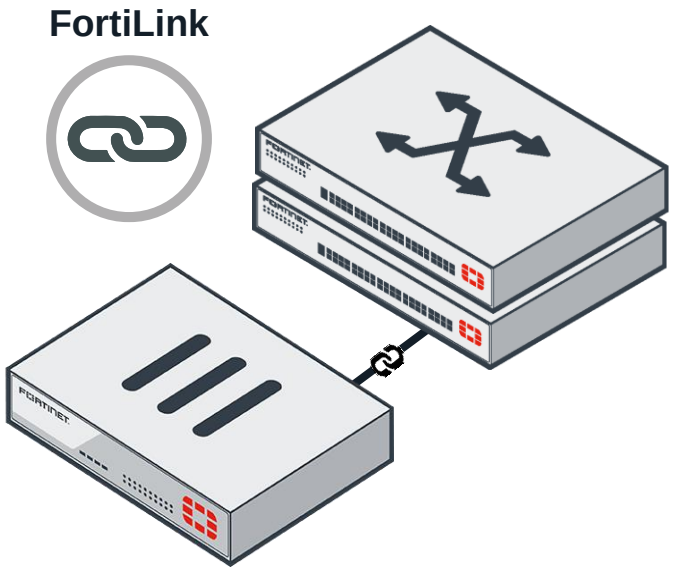
Варианты развертывания FortiSwitch

FortiLink

Управление с FortiGate

Расширение Security Fabric на коммутаторы

Наиболее распространенная модель развертывания



Stand Alone

Стандартная модель развертывания

Распространена в средах без FortiGate

Реализация безопасного доступа

с помощью протокола FortiLink

Простота

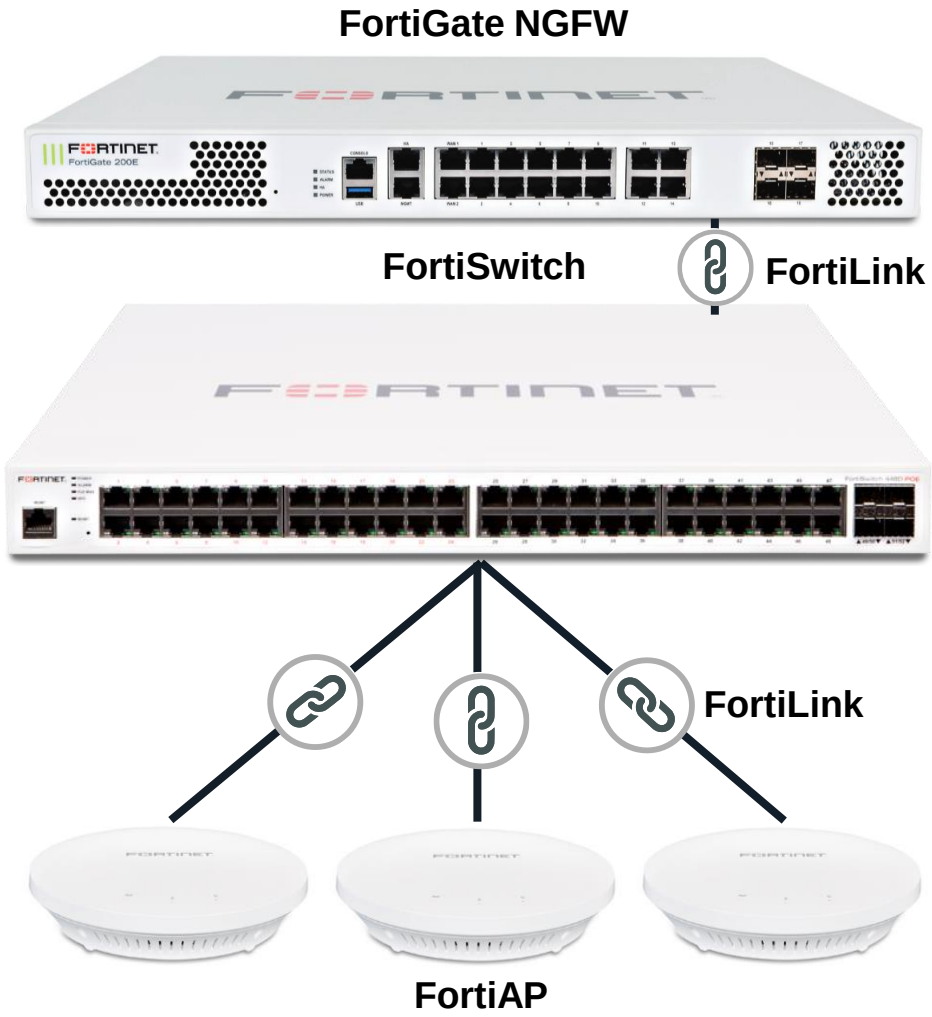
- Гибкая архитектура, масштабирование и удобство управления
- Видимость всего, что происходит в инфраструктуре (проводной и беспроводной)

Безопасность

- Расширение функций NGFW на уровень доступа (на порты коммутатора)
- Контроль трафика БЛВС (SSID) с NGFW
- Глобальные политики безопасности применяются к проводной и беспроводной среде

Низкая стоимость владения

- Не требует дополнительного лицензирования и сторонних систем



Fortilink – протокол управления коммутаторами

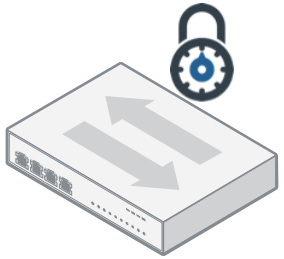
Ключевые преимущества

ZERO-TOUCH PROVISIONING

АВТОМАТИЗАЦИЯ УСТАНОВКИ И НАСТРОЙКИ

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

БЕЗОПАСНОЕ И ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

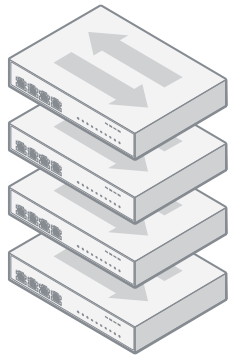


- FortiGate является единой точкой управления
- Централизованное управление VLAN и других функций провижининга

ИНТЕГРАЦИЯ КОММУТАТОРОВ С SECURITY FABRIC

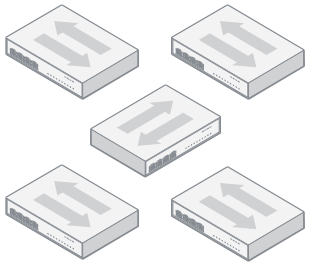
- Обнаружение подключаемых устройств
- Централизованная аутентификация
- Карантин на порту
- Динамическое назначение VLAN
- Логирование процессов

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

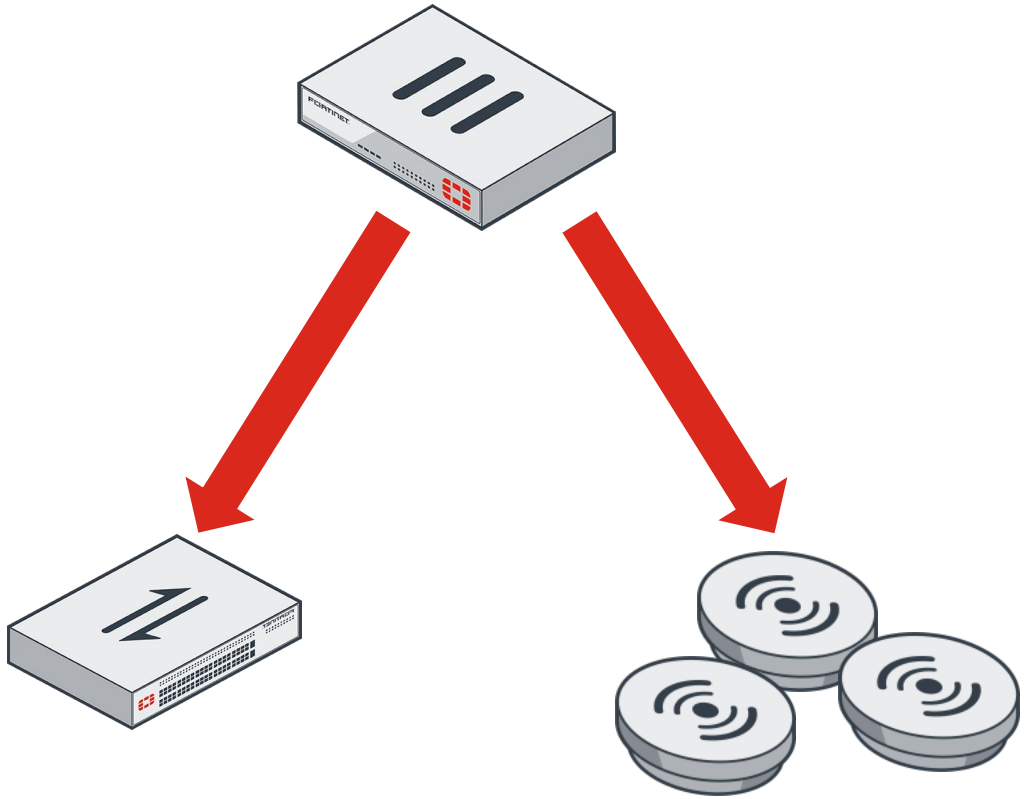
FORTINET

Сеть с интегрированной безопасностью

- 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

Сеть с интегрированной безопасностью

- 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



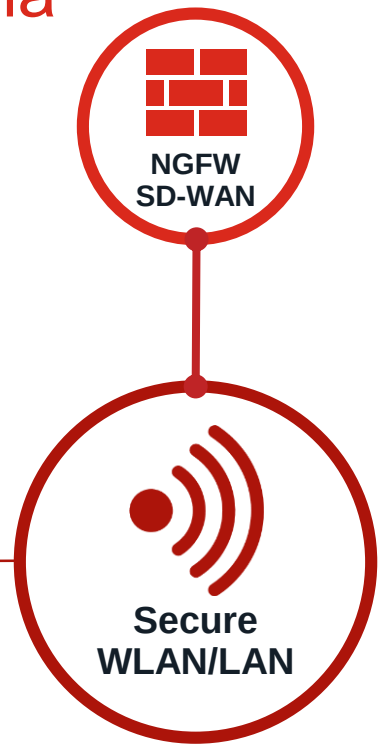
Уровень доступа Fortinet

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



Комплексное решение

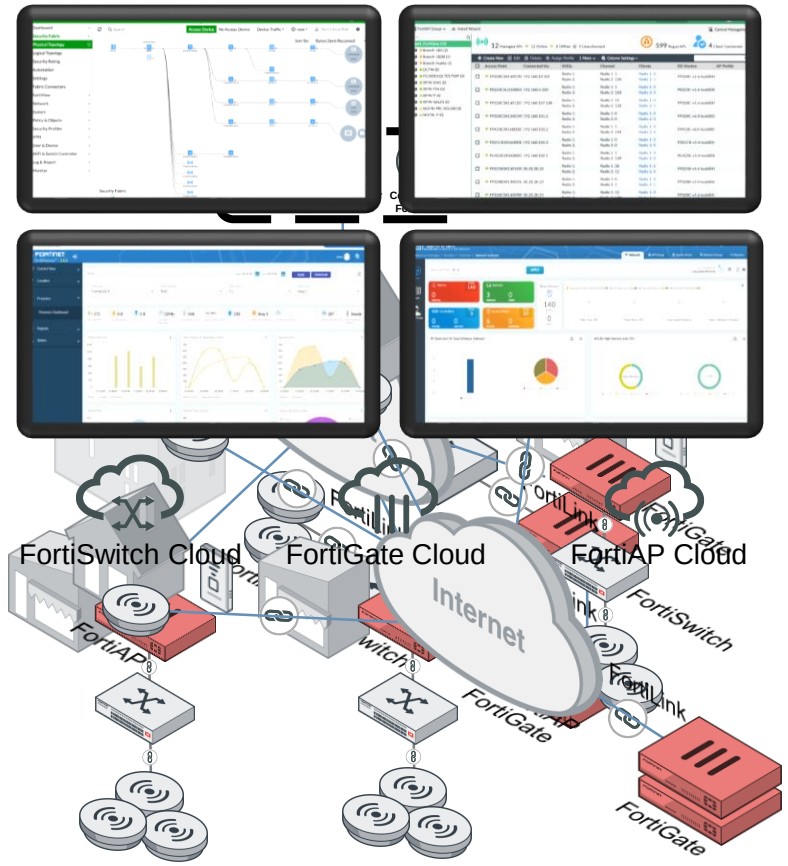
Управление и аналитика

FortiGate

FortiManager

FortiPresence

FortiWLM



Кампус

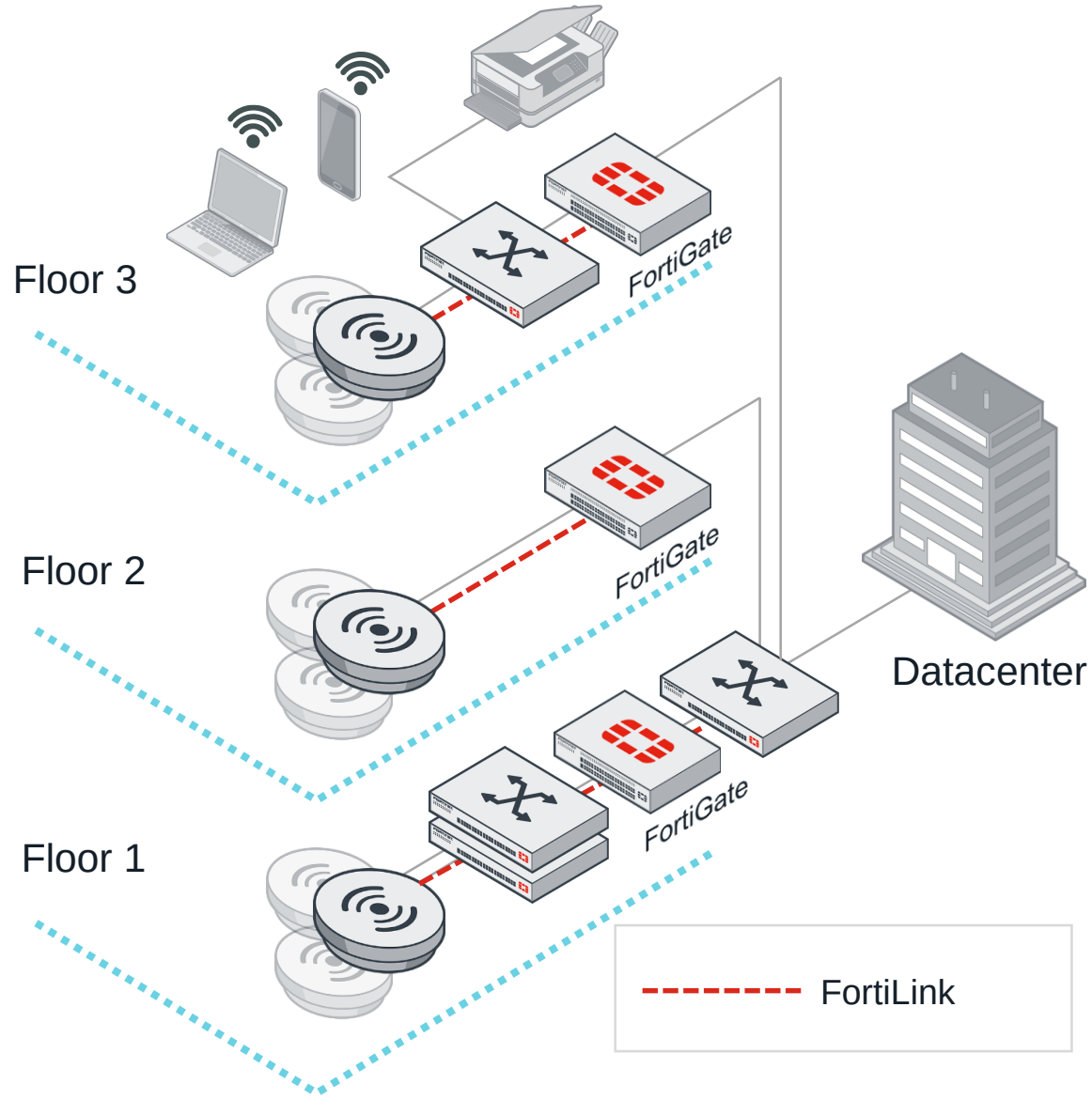
Филиал

Удаленный работник

Сценарии применения

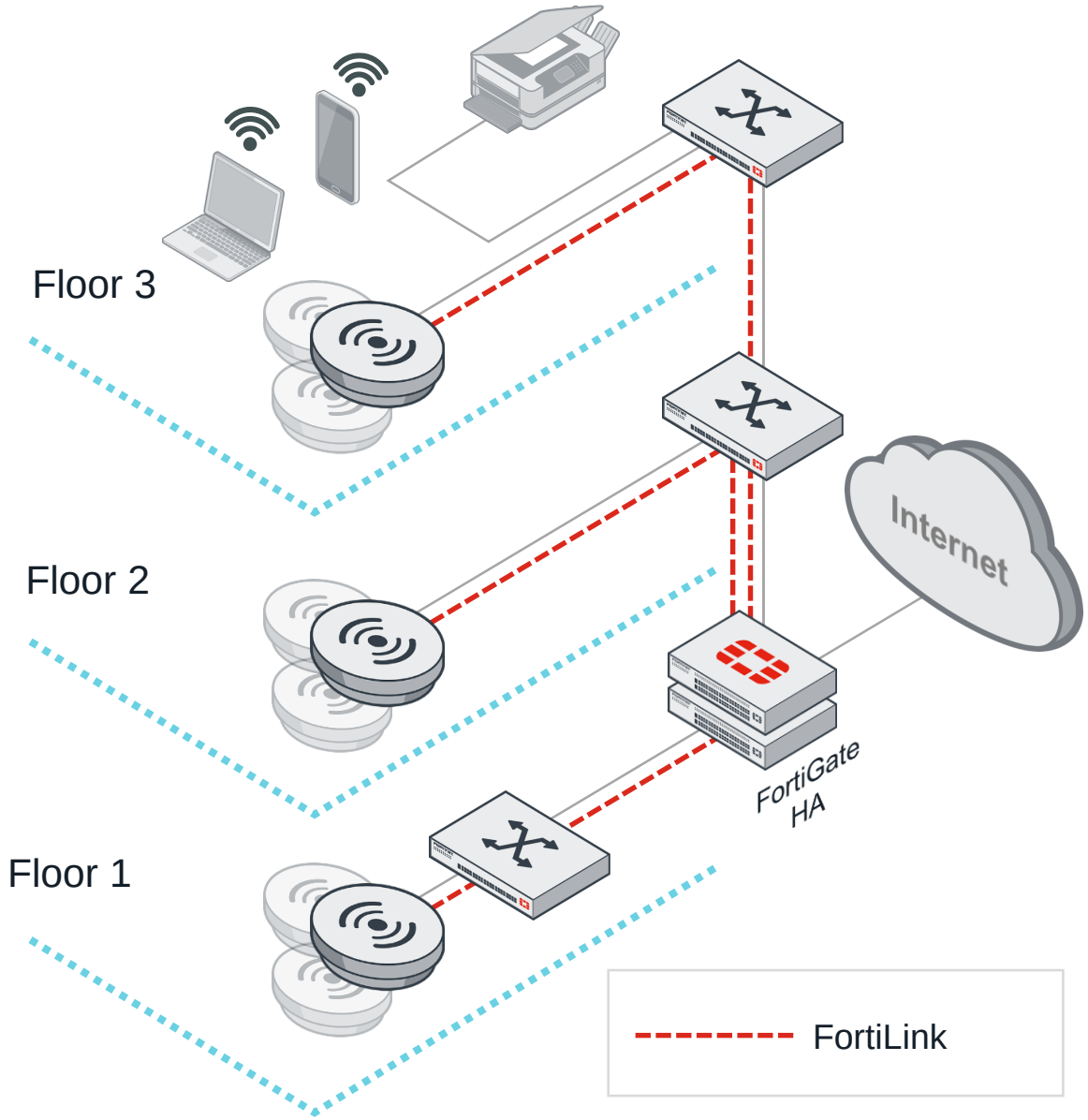
Кампусная сеть

- NGFW 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

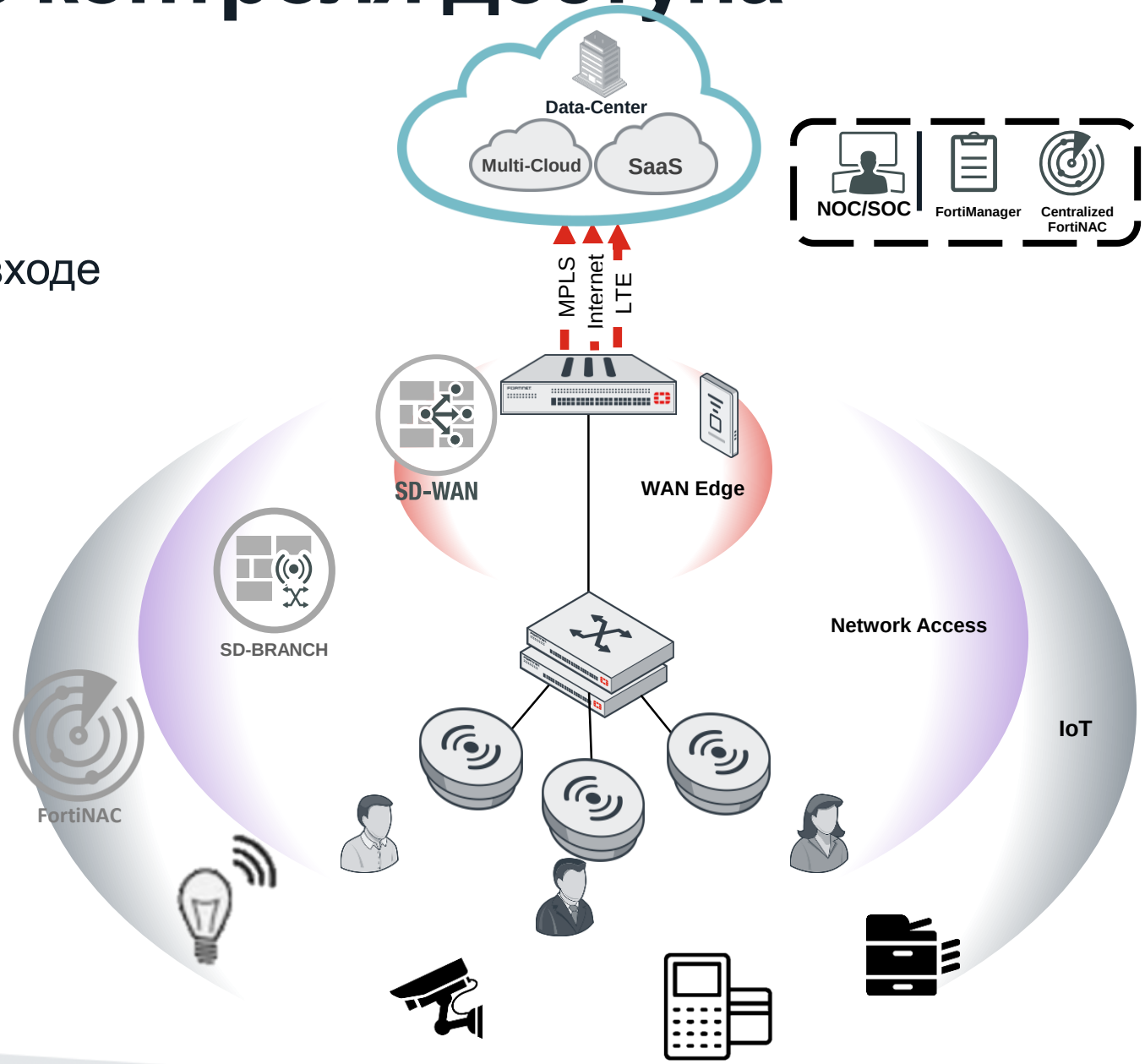


Интеллект на уровне контроля доступа

FortiNAC

FortiNAC защита на уровне устройств

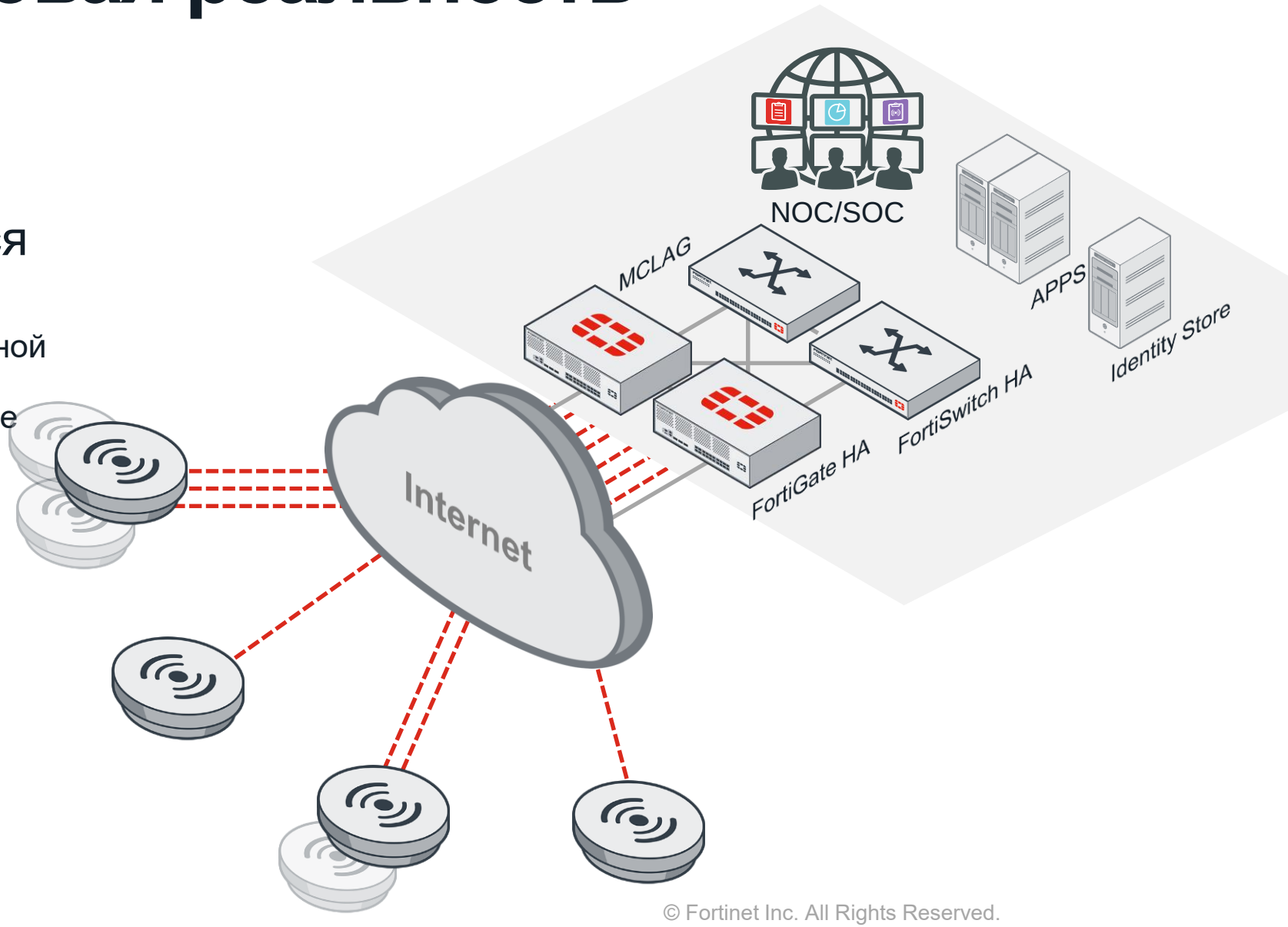
- Обнаружение, классификация, контроль, профилирование, оценка состояния при входе устройств в сеть
- Увеличение видимости и обнаружение аномалий
- FortiGate как сенсор, не нужны дополнительные устройства



«Удалёнка» - новая реальность

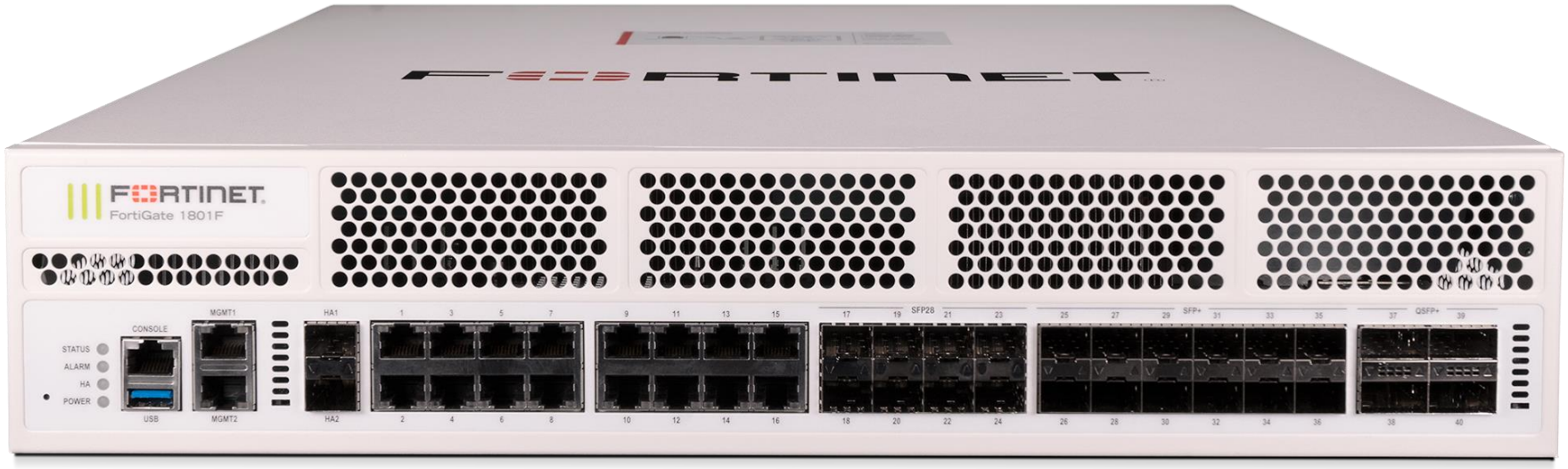
Remote AP

- 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

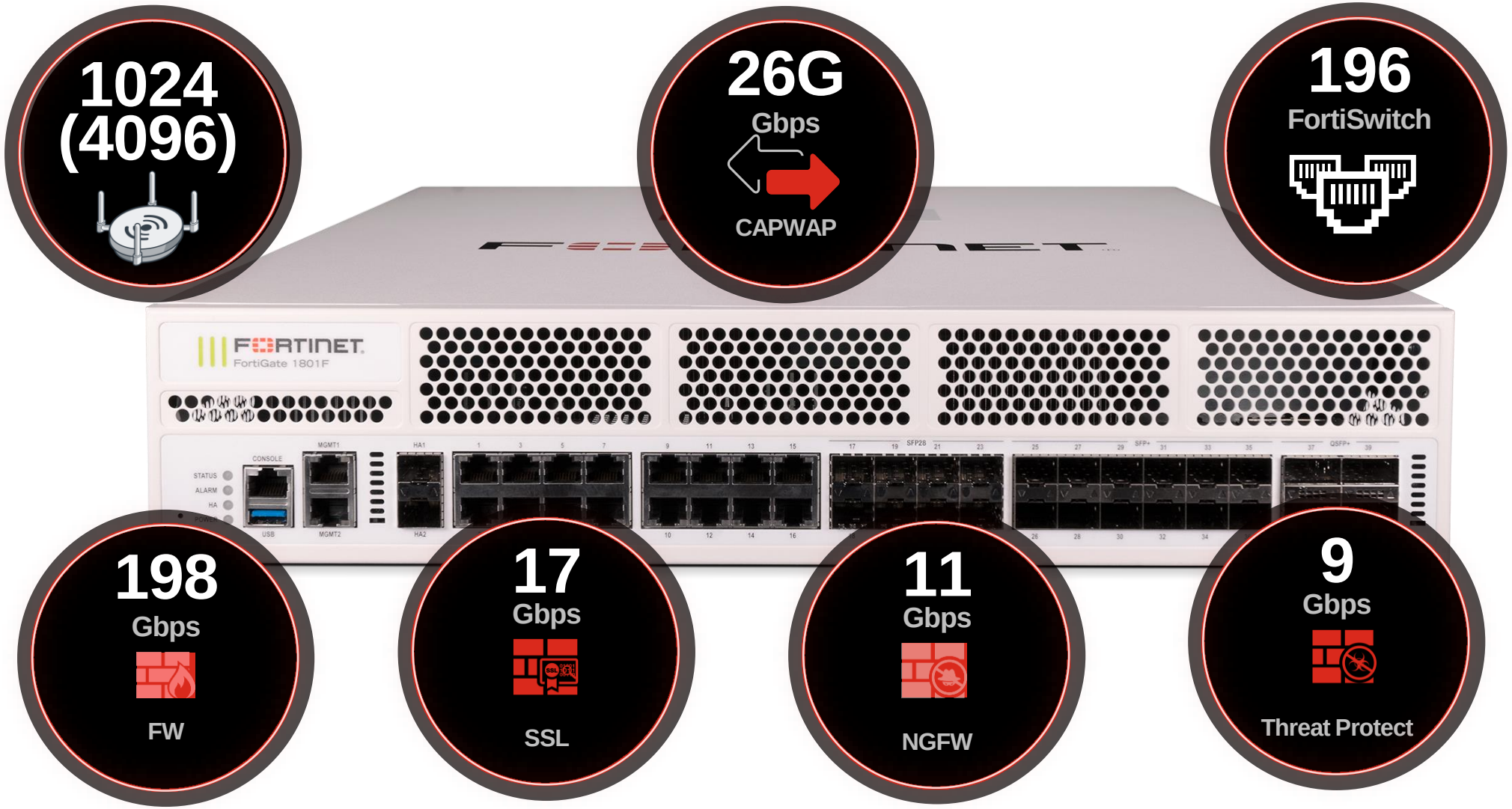


Беспроводной доступ (Wi-Fi)

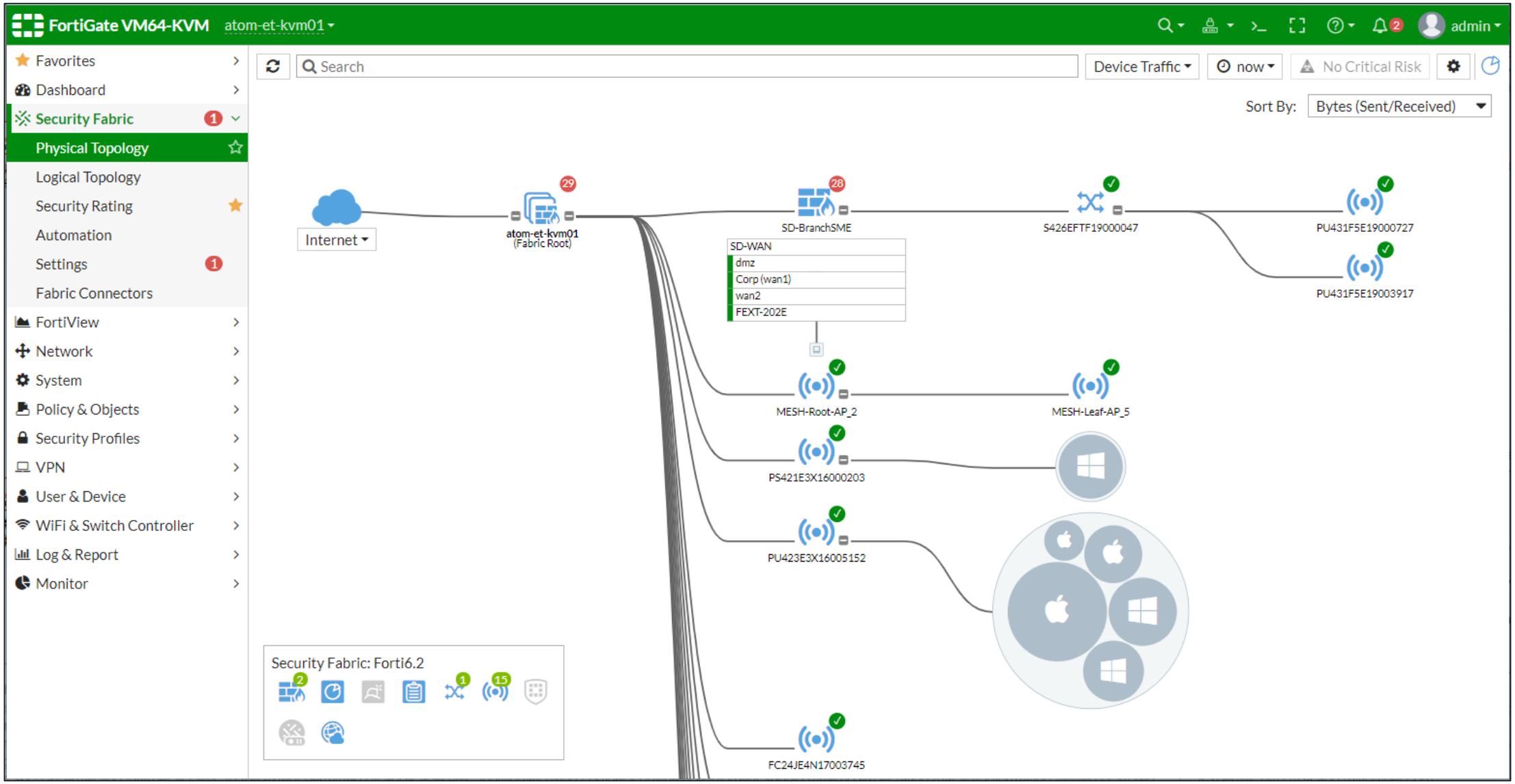
FortiGate в роли контроллера точек доступа



Новый FortiGate 1801F



Сетевые топологии



Анализатор спектра в FortiOS

Унифицированный уровень доступа с расширенными функциями безопасности

FortiGate

- Множество моделей
- Шлюз безопасности
- 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

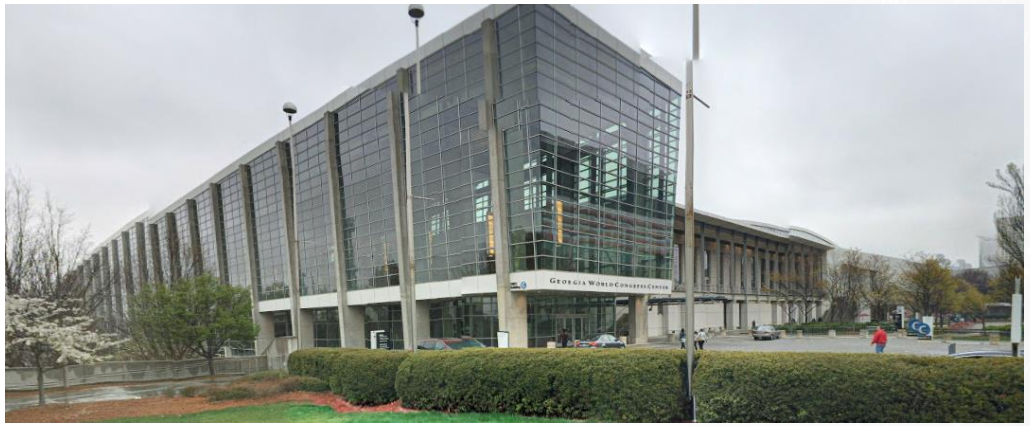
- Более 20 моделей
  - Коммутаторы доступа
  - Коммутаторы ЦОД
- Интеграция с FortiGate (FortiLink)
- L2/L3 + расширенные функции

FORTINET

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

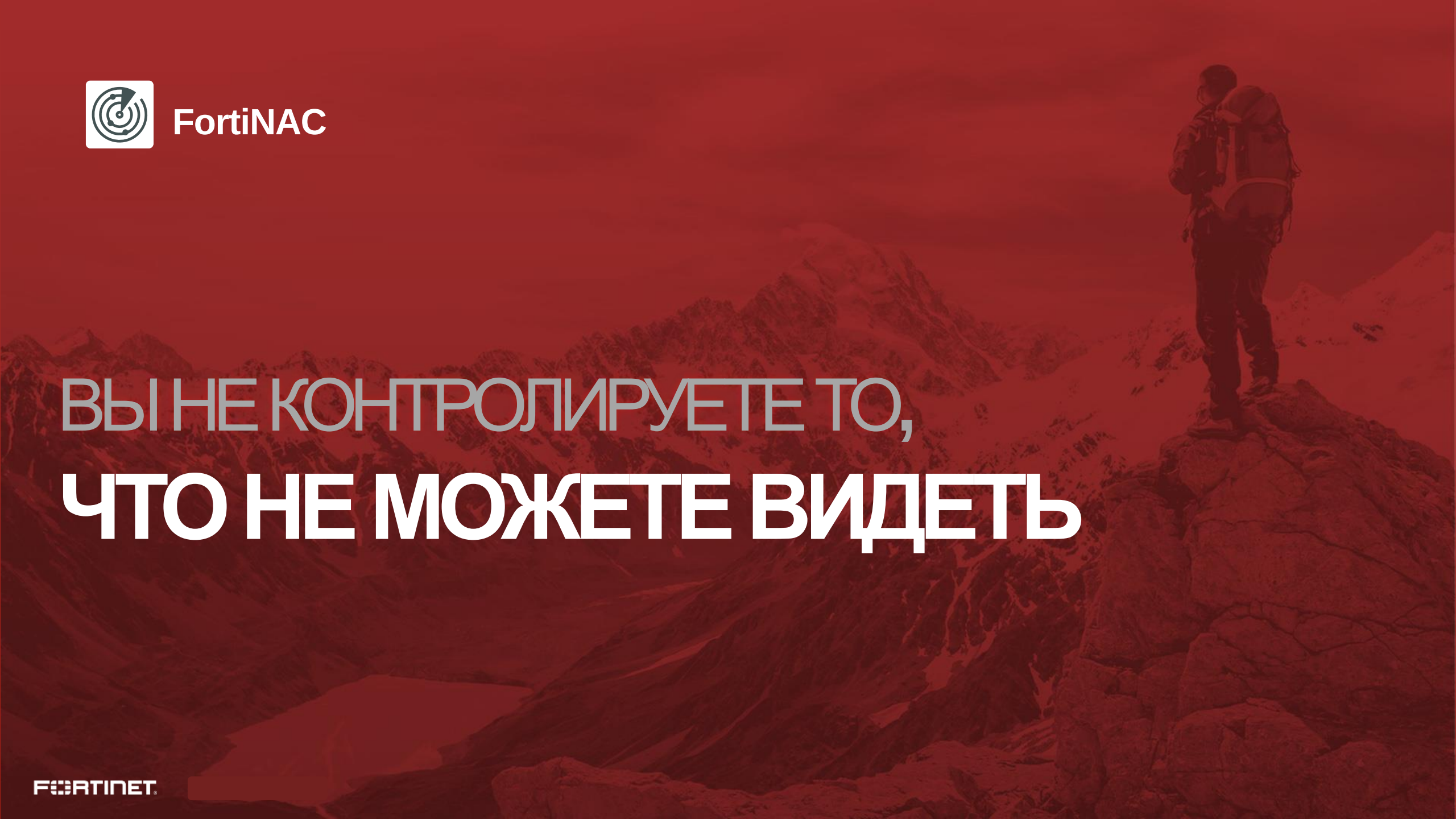

GEORGIA WORLD CONGRESS CENTER


ADELAIDE CONVENTION CENTRE


99
Koosier

Обеспечение безопасности на уровне доступа

Решение для контроля доступа FortiNAC


FortiNAC
ВЫ НЕ КОНТРОЛИРУЕТЕ ТО,
ЧТО НЕ МОЖЕТЕ ВИДЕТЬ
FORTINET

Что происходит в вашей сети ?

- 3 поколения Network Access Control

1950 - 2009 : Управление корпоративным доступом к сети

- Разрешение/Запрет/Ограничение для корпоративных устройств

2009 - 2014 : BYOD

- Упрощение и масштабирование процесса контроля подключений пользователей, устройств
- Проверка подключаемых устройств на соответствие политикам компании

2014 - 2050 : IoT

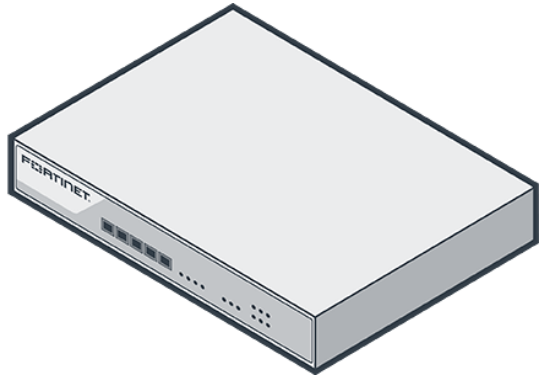
- Аутентификация устройств & Провижининг устройств
- Автоматические реакции на инциденты и события

Безопасность в мире IoT

контроль подключений к сети

FortiNAC

Network Access Control

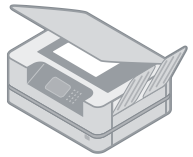


- Идентификация, профилирование всех конечных узлов, IoT устройств, пользователей, приложений
- Сегментация сети на основе характеристик конечных узлов и поведения
- Динамическая оценка риска и автоматическое применение мер противодействия, в том числе для устройств сторонних производителей

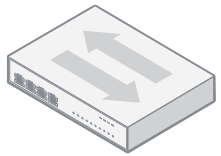
Отслеживает каждое устройство в сети

Сценарии применения NAC

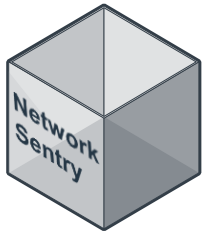
- **Динамическое профилирование устройств**



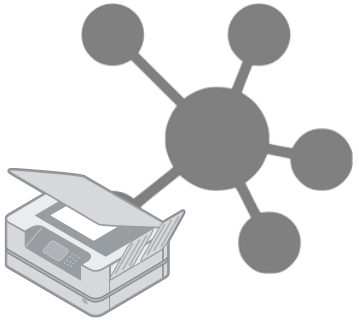
1. Принтер подключился к сети



2. На FortiNAC направлен MAC notification trap



3. FortiNAC Профилирует устройство как «принтер»

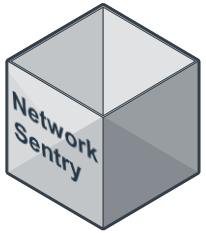


4. FortiNAC Информирует Фабрику о предоставлении соответствующего доступа

- **Сдерживание угроз на границе сети**

1. Пользователь подключает инфицированный ноутбук

2. FGT отправляет событие на FortiNAC



3. FortiNAC помещает узел в карантин на уровне доступа

4. Угроза сдержана на уровне коммутатора доступа

Зачем Вам NAC?

Знаете ли вы что происходит в вашей сети?

Беспокоит ли вас проблемы безопасности IoT устройств?

Сертификация, требования регулятора?


FORTINET