

**MARVEL**  
Дистрибуция

**FORTINET®**

# Все начинается с FortiGate и FortiOS

NEW



Mobile Security



App Control



Antivirus



Anti-spam



IPS



Web App



Database



Web Filtering



Vulnerability Management



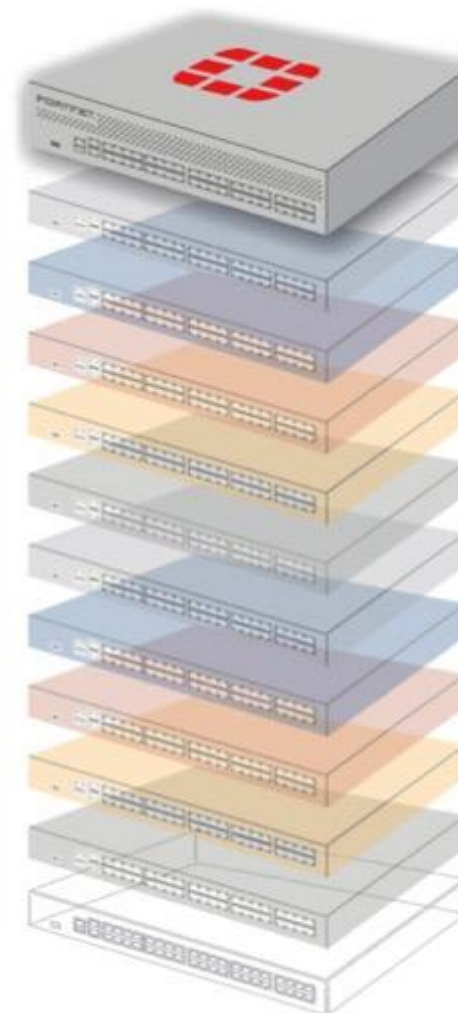
IP Reputation



SECURED BY  
FORTIGUARD®

**SD-WAN от Fortinet**

Firewall  
VPN  
Application Control  
IPS  
Web Filtering  
Anti-malware  
WAN Acceleration  
Data Leakage Protection  
Wi-Fi Controller  
Advanced Threat Protection



# Решения Security Fabric

- FortiGate
- FortiAnalyzer
- FortiManager
- FortiAP
- **FortiWiFi**
- FortiMail
- FortiSandbox
- FortiNAC
- FortiSOAR
- FortiClient
- FortiWeb
- FortiSIEM
- FortiAuthenticator
- FortiADC
- FortiCache/FortiProxy
- FortiFone
- FortiDDoS
- FortiDeceptor
- FortiRecorder & FortiCamera
- FortiTester
- FortiToken
- FortiAI
- FortiWLC
- FortiExtender
- FortiEDR

# Межсетевые экраны

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)

# Безопасная инфраструктура филиалов (SD-Branch)

Figure 1. Magic Quadrant for WAN Edge Infrastructure



Source: Gartner (September 2020)

# Wired and Wireless LAN Access (Апрель 2019)

Figure 1. Magic Quadrant for the Wired and Wireless LAN Access Infrastructure



# Wired and Wireless LAN Access (Апрель 2020)

Figure 1. Magic Quadrant for Wired and Wireless LAN Access Infrastructure



# Fortinet Security Fabric

Архитектура безопасности, которая обеспечивает :

## Широта

Видимость и защита от всех векторов атак

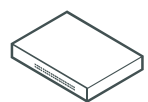
## Интеграция

Обнаружение атак и защита от сложных угроз

## Автоматизация

Автоматическая реакция на инциденты & Непрерывное оценка состояния защиты устройств

Поставляются как:



Appliance



Virtual Machine



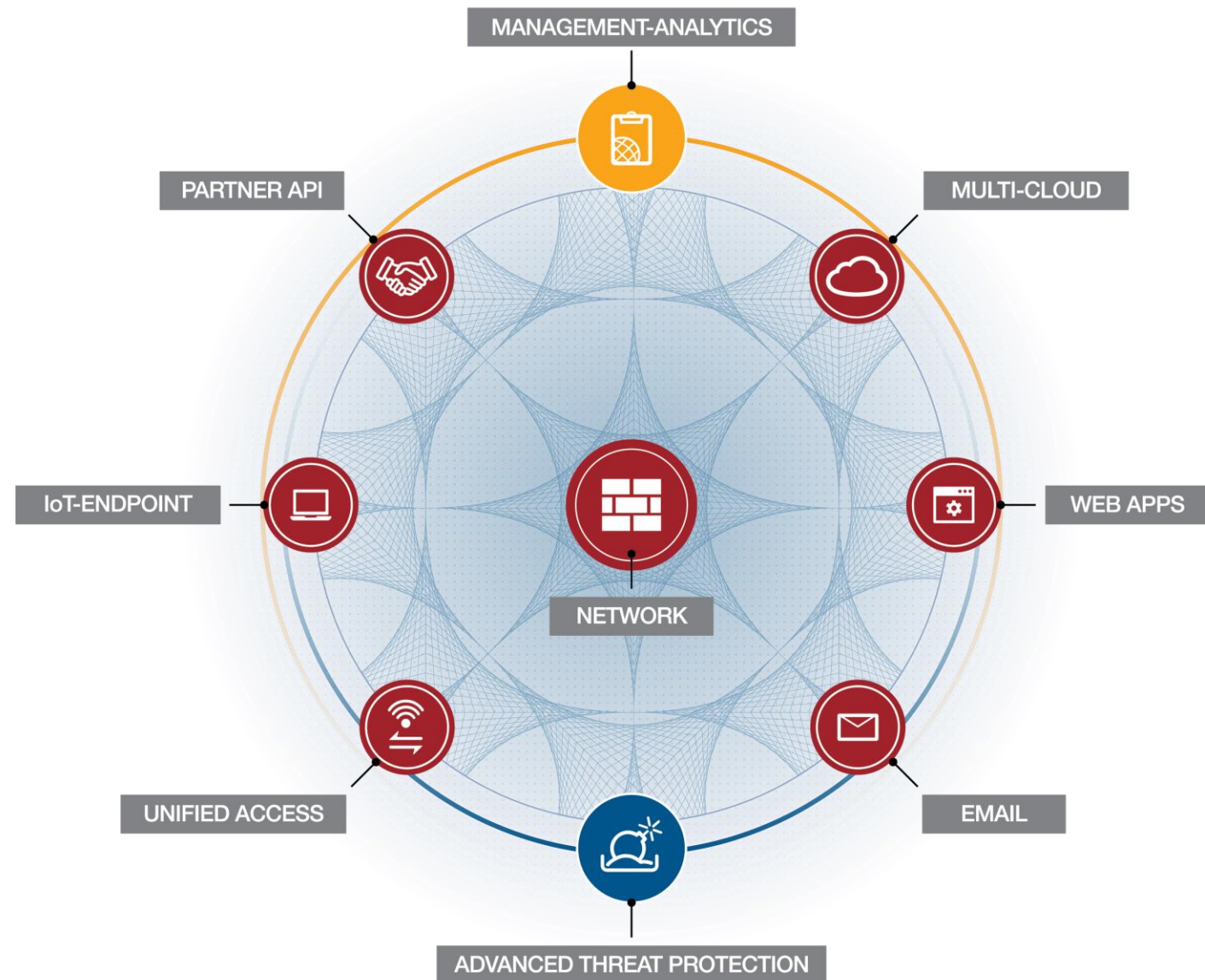
Hosted



Cloud



Software



# Fortinet Security Fabric Безопасный унифицированный доступ



Продукты и услуги, необходимые для обеспечения безопасного сетевого подключения, для проводных и/или беспроводных, пользователей Fortinet Security Fabric



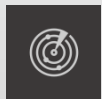
**FortiAP, FortiWLC, FortiWLM**  
Wireless Infrastructure



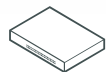
**FortiSwitch**  
Switching Infrastructure



**FortiAuthenticator, FortiToken**  
Identity and Access Management



**FortiNAC**  
IoT and Access Control



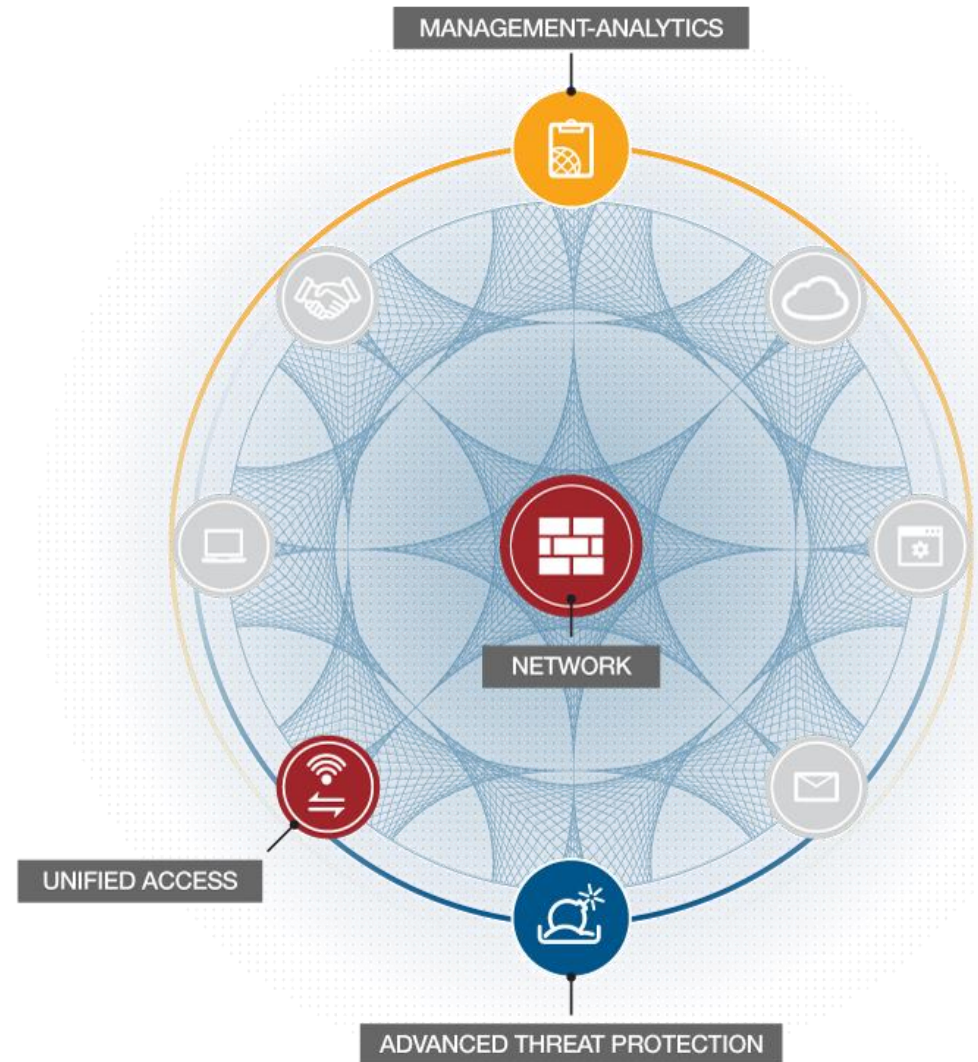
Appliance



Virtual Machine

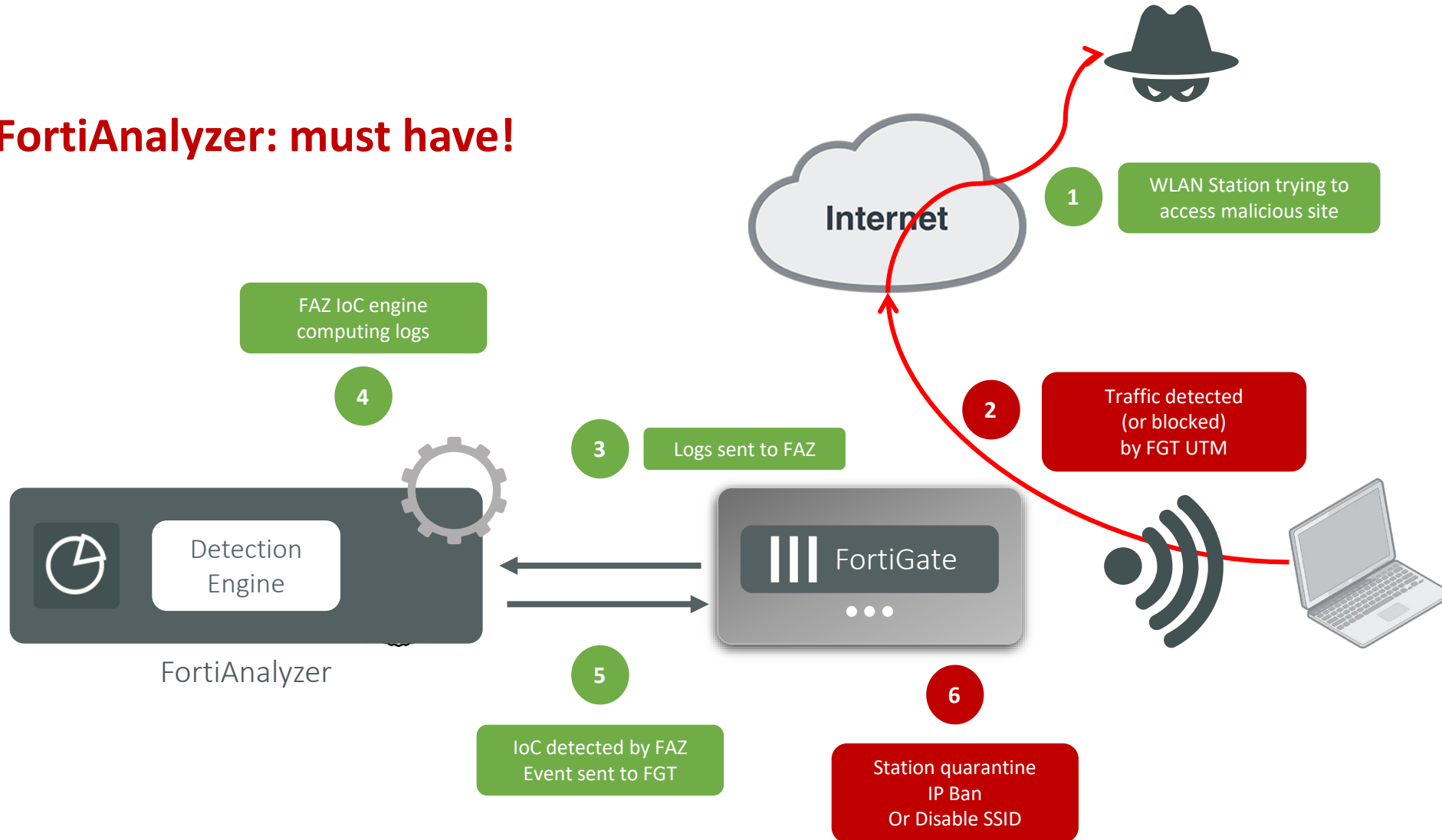


Hosted



# Fortinet Security Fabric : integrated wireless quarantine

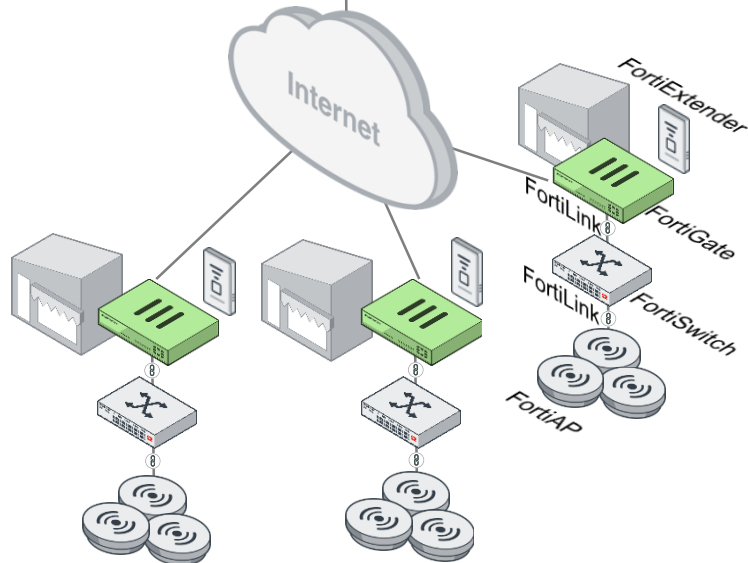
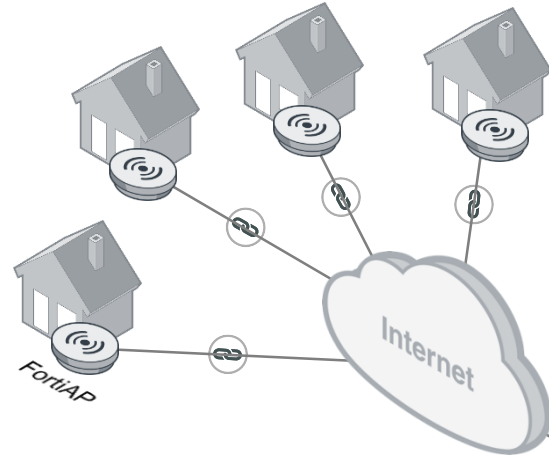
**FortiAnalyzer: must have!**





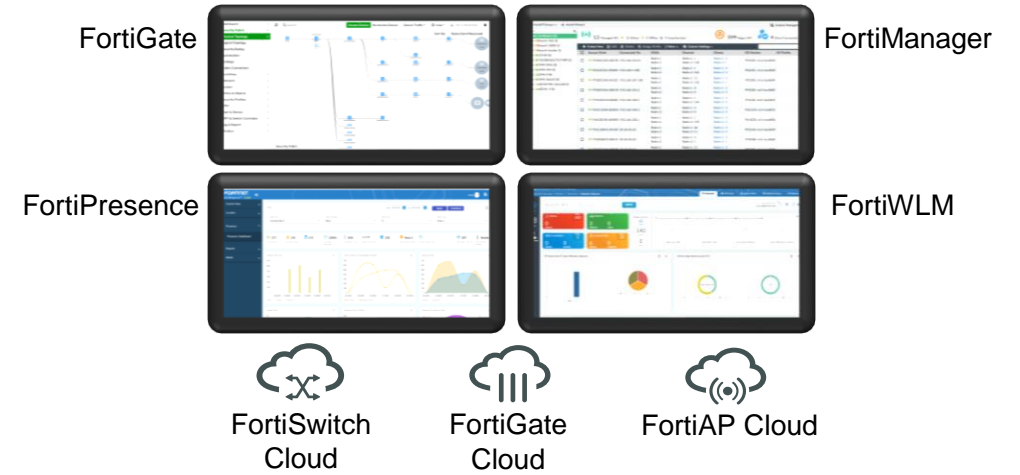
# Secure Access Solution

## Teleworker

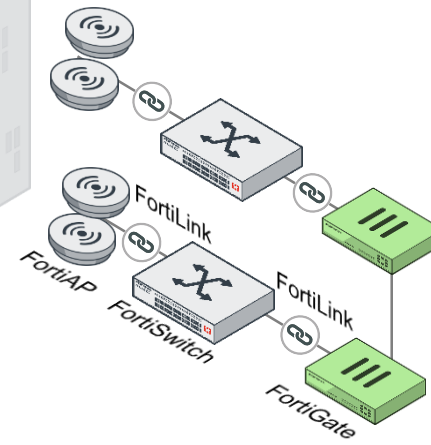


## SD-Branch

## Management and Analytics

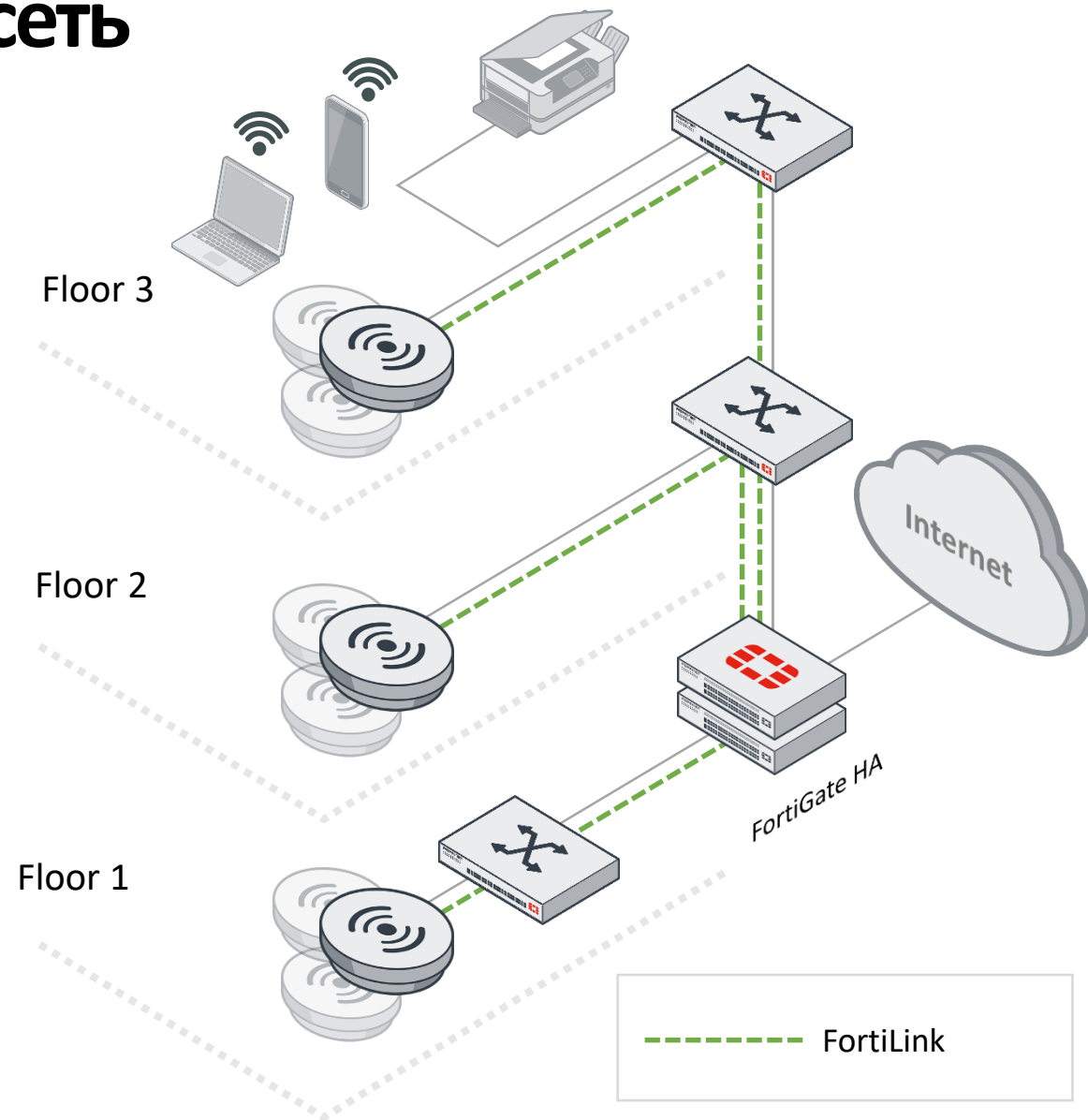


## Campus



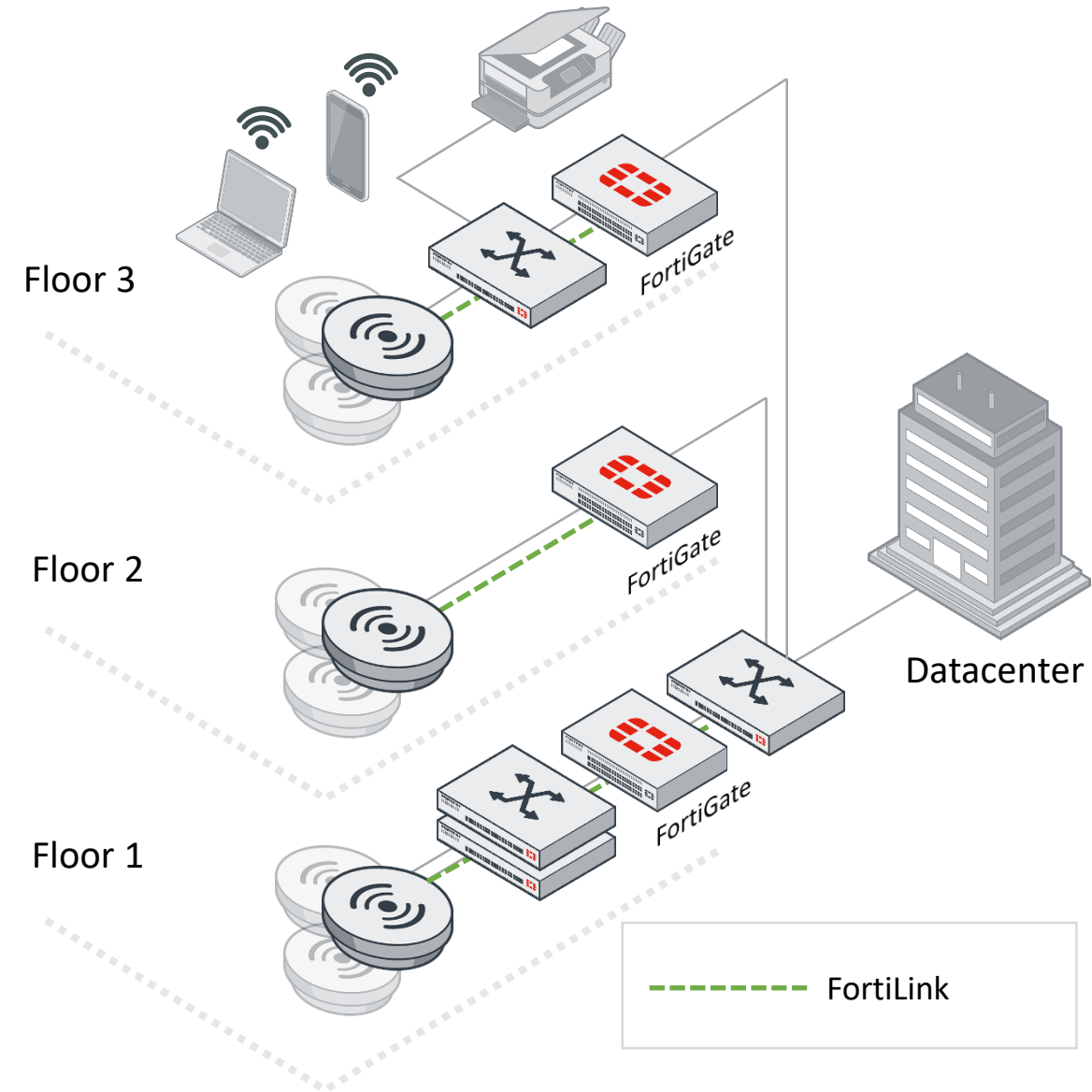
# Кампусная сеть

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

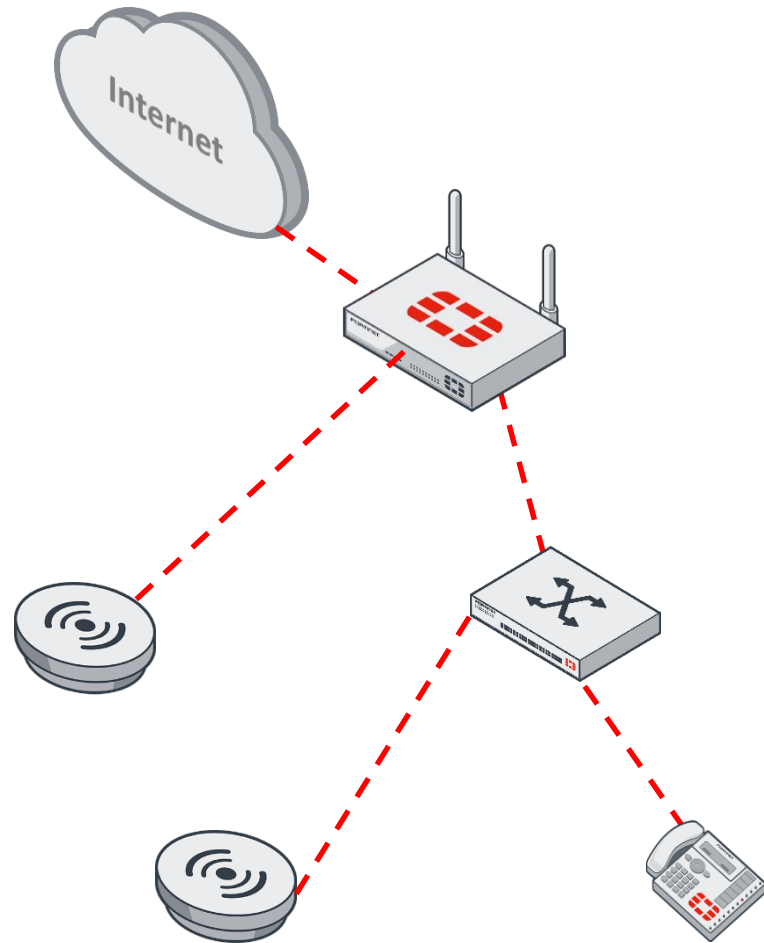


# Кампусная сеть

- 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



# SMB сектор – небольшие предприятия или филиалы



Малое предприятие/офис/Филиал

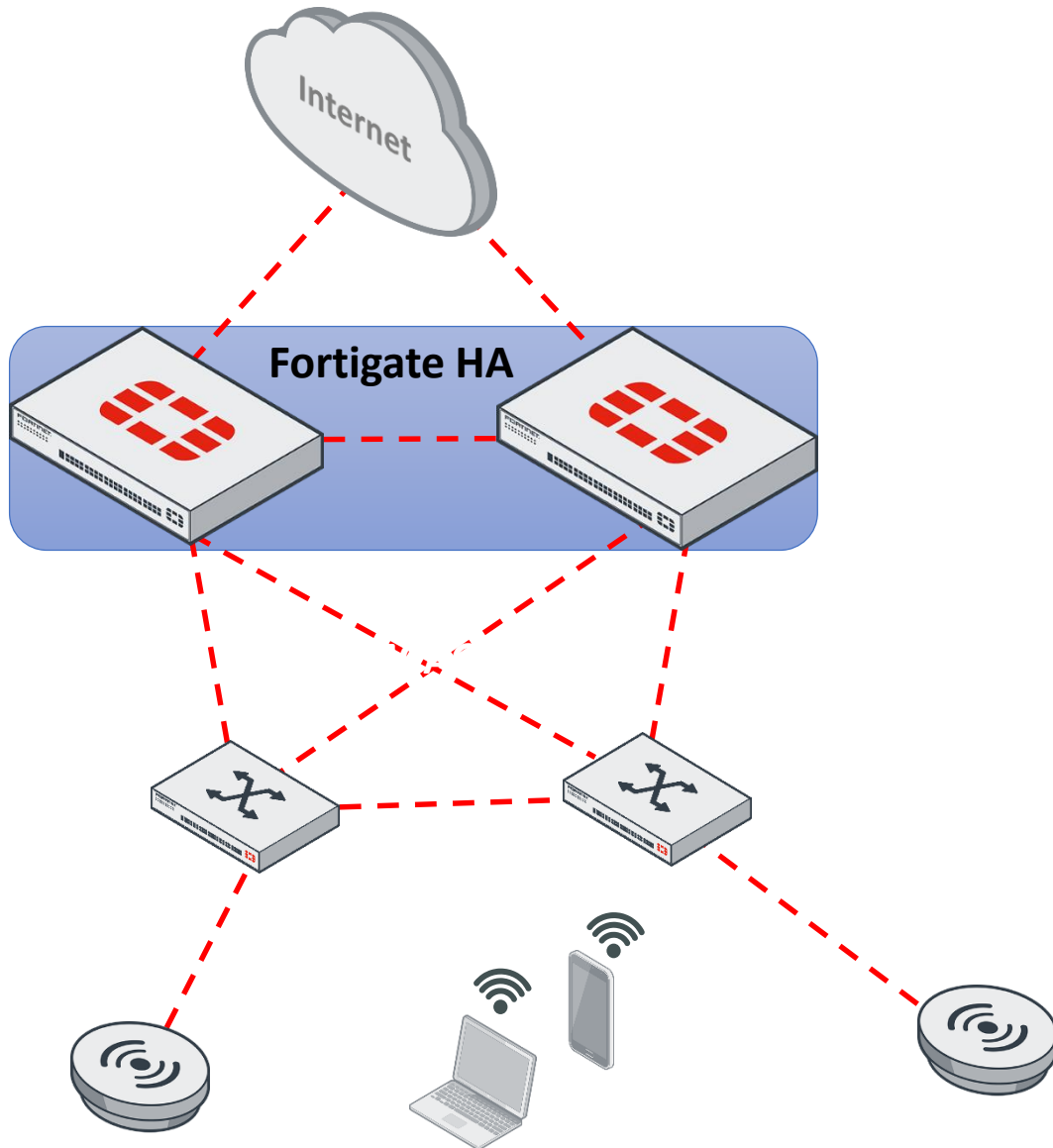
## Примеры использования:

- Ограниченный IT бюджет.
- Поддержка ограничена или отсутствует.
- Обязательная безопасность.
- Обязательные требования PCI, ИСПДн, ГИС и т.д.
- Постоянные изменения
- Требования быстро меняются, новые пользователи и изменения в инфраструктуре, появление новых систем

## Преимущества Fortinet:

- Удобное управление
- Управляемая безопасность, контроль доступа, и WAN через единый интерфейс
- Простой провижининг
- Эффективная система безопасности
- Просто масштабируется

# SMB сектор – небольшие предприятия или филиалы



## Примеры использования:

- Постоянное изменение.
- Требования меняются быстро, новые пользователи и системы постоянно пересматриваются
- Уменьшает сложность управления
- Ограничивает количество экранов
- Простая установка и снижение затрат на эксплуатацию

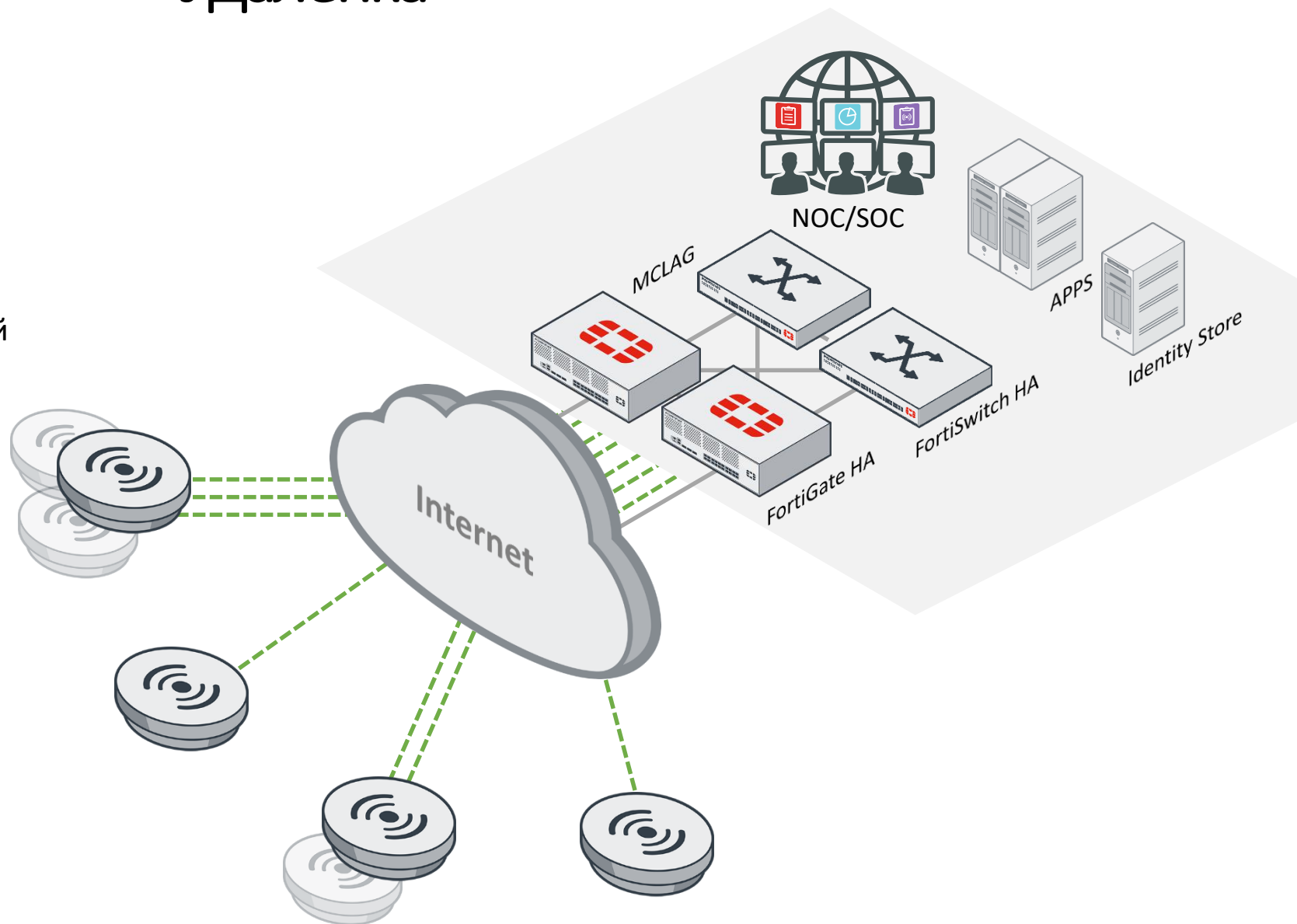
## Почему Fortinet:

- Архитектура способна надежно и быстро масштабироваться.
- Удобство управления
- Управление безопасностью, доступом и глобальной сетью из одного интерфейса.

# «Удалёнка»

## 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



# Ключевые преимущества

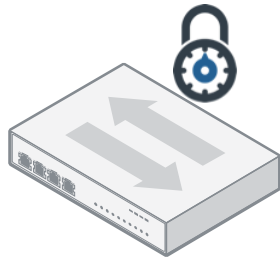
## ZERO-TOUCH PROVISIONING

### АВТОМАТИЗАЦИЯ УСТАНОВКИ И НАСТРОЙКИ



- Простое развертывание большого количества
- Централизованное управление
- Автообнаружение, авторизация и настройка

## БЕЗОПАСНОЕ И ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ



- FortiGate является единой точкой управления
- Централизованное управление конфигурацией

## ИНТЕГРАЦИЯ С SECURITY FABRIC



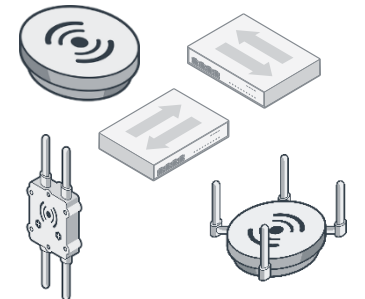
- Обнаружение подключаемых устройств
- Централизованная аутентификация
- Карантин устройства
- Динамическое политик
- Логирование процессов

## ОБЩИЕ ПОЛИТИКИ NGFW+WIFI



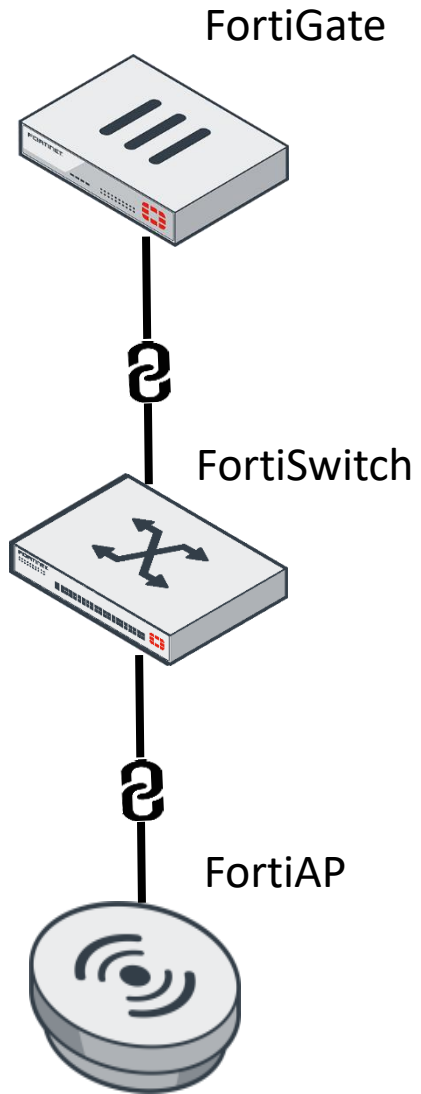
- Одно место для проверки, логирования и применения
- Wireless policy видны как политики FortiGate

## БОЛЬШОЙ МОДЕЛЬНЫЙ РЯД



- Широкая линейка FortiWiFi:
  - » Внутренние и внешние модели
  - » Compact form factor
  - » Уличное исполнение
  - » BLE/BT
  - » Выделенное радио для сенсора

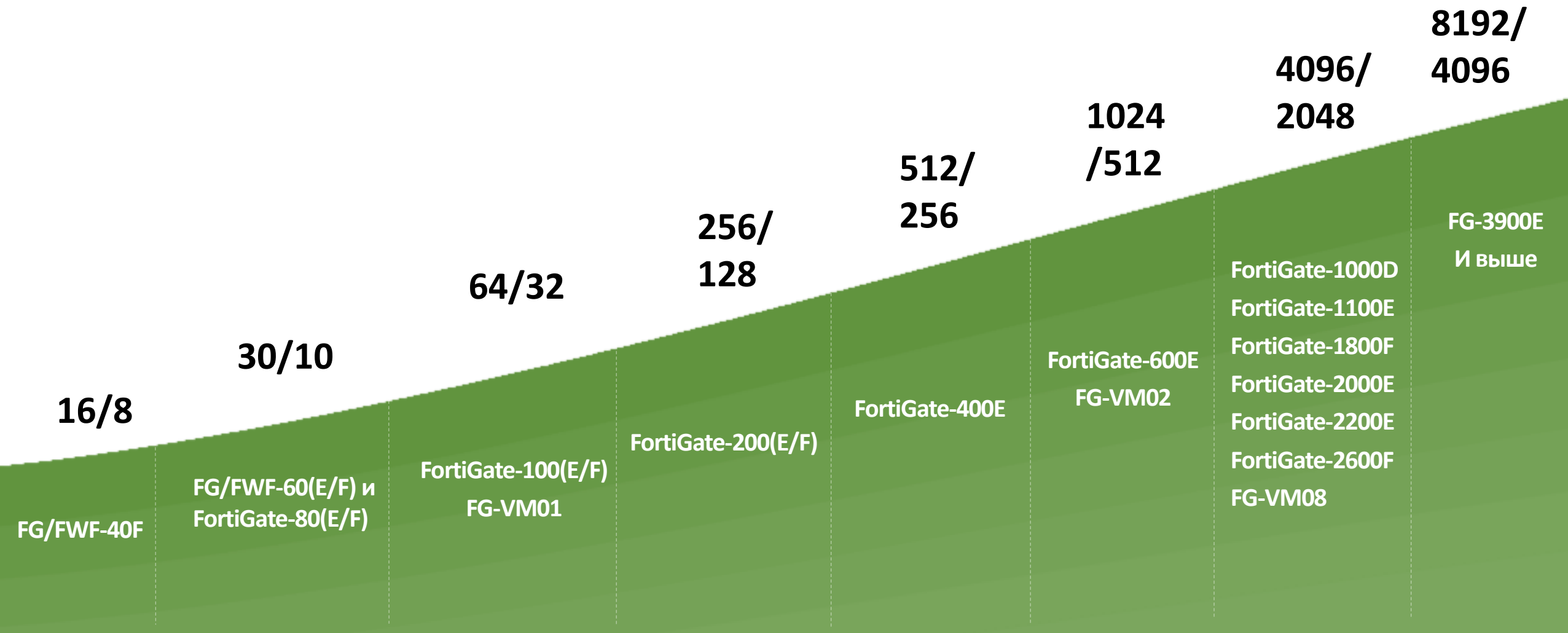
# Развертывание и управление сетью с Security Fabric + FortiLink



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 (highlighted), Physical Topology (highlighted with a star), 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 the Physical Topology of the Security Fabric. It 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 access switches: 'FAC\_ACC\_SW', 'ENG\_ACC\_SW', 'FIN\_ACC\_SW', 'SALES\_ACC\_SW', 'IT\_ACC\_SW', and 'HR\_ACC\_SW'. These access switches are further connected to various devices: 'Demo-ISFW-ENG', 'Demo-ISFW-FIN', 'Demo-ISFW-SALES', 'FIN\_ACC\_SW1', and 'SALES\_SW1'. On the right side, there are two circular nodes representing FortiLink devices with traffic statistics: 'FP22E3H000802' (39.96 GB) and 'FP22E3H000895' (54.34 GB). At the bottom right, there is a 'FP221E1F18025895' device. The interface also includes a search bar, 'Access Device' and 'No Access Device' buttons, 'Device Traffic' dropdown, and a 'Sort By: Bytes (Sent/Received)' dropdown.



# Количество поддерживаемых точек доступа в зависимости от модели FortiGate



# Продуктовая линейка FortiWiFi

Ссылка на обновляемую версию:

<https://drive.google.com/file/d/1fTAPVWfyfwKkqc9u-jDOmmBnEp6t3hiU>

# FortiWiFi подбор моделей через конфигуратор

<https://www.fortinet.com/products/product-compare>

**SECURITY-DRIVEN NETWORKING**

**ADAPTIVE CLOUD SECURITY**

**AI-DRIVEN SECURITY OPERATIONS**

**ZERO TRUST ACCESS**

Select up to 3 models to Compare

Compare Models →

## Categories:

- Next Generation Firewall (39)
- Secure SD-WAN (15)
- VPN (37)
- SWG (15)
- Access Point (23)
- Analytics (8)
- Application Delivery Controller (8)
- Distributed Denial of Service (5)
- Email Security (7)
- Management (6)
- Sandbox (4)
- Security Information & Event Management (3)
- Switching (44)

Wi-Fi Technology

Wi-Fi 6 (802.11ax)

Performance

Any

Number of Radios

Any

Antenna Type (Internal or External)

Any

BLE Enabled

Any

Dual 5GHz Capable

Any

### FortiAP U433F



Wi-Fi Technology : WiFi 6

Performance : 4x4

Number of Radios : 3

### FortiAP 433F



Wi-Fi Technology : WiFi 6

Performance : 4x4

Number of Radios : 3

### FortiAP 432F



Wi-Fi Technology : WiFi 6

Performance : 4x4

Number of Radios : 3

# Продуктовая линейка FortiWiFi

	Model	Outdoor	Antenna: internal external	# radios	802.11	Radio №1	Radio №2	Radio №3	BLE/BT dedicated	PoE budget	Gig interfaces	Max clients	Console USB
FAP-	<b>221E</b>		i	2	n/ac	2.4	5 2*2:2			802.3af	1	512	
FAP-	<b>222E</b>	√	e*4	2	n/ac	2.4	5 2*2:2		√	802.3af	1	512	
FAP-	<b>223E</b>		e*4	2	n/ac	2.4	5 2*2:2			802.3af	1	512	
FAP-	<b>224E</b>	√	i	2	n/ac	2.4	5 2*2:2		√	802.3af	2+SFP	512	
FAP-	<b>231E</b>		i	3	n/ac w2	2.4/5ac	5 2*2:2	2.4/5n	√	802.3at	2	512/128	√
FAP-	<b>321E</b>		i	2	n/ac	2.4	5 3*3:3		√	802.3at	1	512	√
FAP-	<b>421E</b>		i	2	n/ac w2	2.4	5 4*4:4			802.3at	2	512	√ √
FAP-	<b>423E</b>		e*8	2	n/ac w2	2.4	5 4*4:4			802.3at	2	512	√ √
FAP-	<b>431F</b>		i	3	ax	2.4	5 2*2:2	2.4/5 scanner	√	802.3at	2/multigig	512	√
FAP-	<b>433F</b>		e*5	3	ax	2.4	5 2*2:2	2.4/5 scanner	√	802.3at	2/multigig	512	√
FAP-	<b>C24JE</b>		i	2	n/ac	2.4	5 2*2:2			802.3at	2+6	64	√
FAP-	<b>U24JEV</b>		i	2	n/ac	2.4	2/5 2*2:2		√*	802.3at	2+4	128	√
FAP-	<b>U221E</b>		i	2	n/ac	2.4	5 2*2:2		√	802.3af	1	128	√
FAP-	<b>U223EV</b>		e*4	2	n/ac	2.4	5 2*2:2		√	802.3af	1	128	√
FAP-	<b>U321EV</b>		i	2	n/ac w2	2.4	5 3*3:3		√	802.3at*	2	256	√ √
FAP-	<b>U323EV</b>		e*6	2	n/ac w2	2.4	5 3*3:3		√	802.3at*	2	256	√ √
FAP-	<b>U421EV</b>		i	2	n/ac w2	2.4	5 4*4:4		√	802.3at	2	256	√ √
FAP-	<b>U422EV</b>	√	e*8	2	n/ac w2	2.4	5 4*4:4		√	802.3at	2	256	√
FAP-	<b>U423EV</b>		e*8	2	n/ac w2	2.4	5 4*4:4		√	802.3at	2	256	√ √
FAP-	<b>U431F</b>		i	3	ax	2.4	5 4*4:4	2.4/5 scanner	√	802.3at	2/multigig	512	√
FAP-	<b>U433F</b>		e*5	3	ax	2.4	5 4*4:4	2.4/5 scanner	√	802.3at	2/multigig	512	√

# Начальный уровень доступа: цена!



**FAP-221E**



**FAP-223E**

Технические характеристики	
Use Case	Mid Density Indoor AP
Form Factor	Wall/Ceiling Mount
Rx / Tx	2x2
Radio 1	2.4 GHz 802.11b/g/n 2x2, 2 stream (300 Mbps)
Radio 2	5 GHz 802.11a/n/ac 2x2 MU-MIMO 2x2, 2 stream (866 Mbps)
Radio 3	-
BLE	-
PoE	802.3 af
Antennas	221: 4x Internal 223: 4x External
Ethernet Interfaces	1 x GE RJ45



**FAP-U221EV**



**FAP-U223EV**

# Wallplate



**FAP-C24JE**

Технические характеристики	
Use Case	Wallplate Indoor AP
Form Factor	Wallplate Mount
Rx / Tx	2x2 or 1x1
Radio 1 (U24JEV)	2.4 GHz 802.11b/g/n (or 5 GHz 802.11a/n/ac Configurable as 1 2x2, or 2 1x1 radios)
Radio 2 (C24JE)	5 GHz 802.11a/n/ac 2x2 MU-MIMO 2x2, 2 stream (866 Mbps)
Radio 3	-
BLE (U24JEV)	Bluetooth scanning and iBeacon advertisement
PoE	802.3 at
Antennas	4/2x Internal
Ethernet Interfaces	6 x GE RJ45: <ul style="list-style-type: none"><li>• 1 x GE RJ45 (PD 802.3at)</li><li>• 1 x GE RJ45 (PSE 802.3af)</li><li>• 2 x GE RJ45</li><li>• 1 x GE RJ45 (Pass Through In)</li><li>• 1 x GE RJ45 (Pass Through Out)</li></ul>



**FAP-U24JEV** 

# Outdoor High Performance



**FAP-U422EV**

## Технические характеристики

Use Case	High Density, High Performance Outdoor AP
Form Factor	IP67, Wall/Pole Mount
Rx / Tx	4x4
Radio 1	2.4 GHz 802.11b/g/n 4x4, 4 stream (600 Mbps)
Radio 2	5 GHz 802.11a/n/ac 4x4 MU-MIMO 4x4, 4 stream (1,733 Mbps)
Radio 3	-
BLE	Bluetooth scanning and iBeacon advertisement
PoE	802.3 at
Antennas	FAP-U422EV: 8x External
Ethernet Interfaces	2 x GE RJ45

# Точки доступа 802.11ax WiFi6



 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



# Indoor High Performance



**FAP-431F**

Технические характеристики	
Use Case	High Density Indoor 802.11ax APs
Form Factor	Wall/T-Rail/Ceiling Mount
Rx / Tx	4x4
Radio 1	2.4 GHz 802.11b/g/n/ac/ax 4x4
Radio 2	5 GHz 802.11a/n/ac/ax 4x4
Radio 3	2.4/5 GHz scanner
BLE	+
PoE	802.3 af (2*2, no USB) 802.3 at
Antennas	431: 5x Internal + internal BLE 433: 5x External omni + internal BLE
Ethernet Interfaces	1 x 2.5/1 GE RJ45 1 x GE RJ45



**FAP-433F**

# **FortiAP: варианты использования**

# Варианты развертывания FortiWiFi

## Integrated

- Управляется с FortiGate. Расширение Security Fabric на коммутаторы.
- Наиболее распространенная модель развертывания
- От 16(8) до 8000(4000) AP
- Управление сетью: Security Fabric, FortiManager

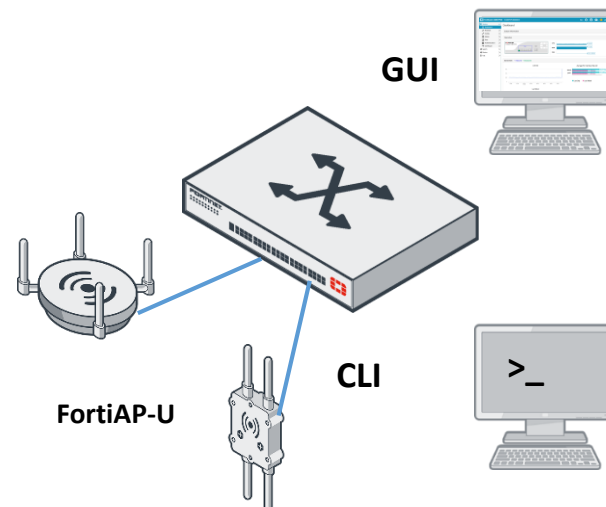
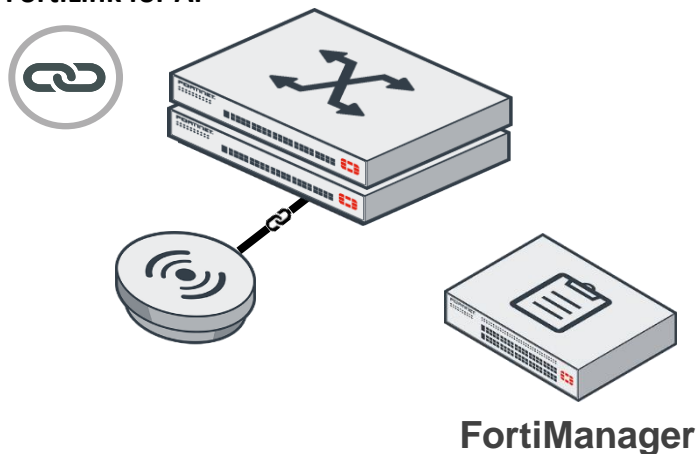
## WLC WLM

- Традиционная модель развертывания с физическим или VM контроллером
- Распространена в средах без FortiGate
- Свой CLI / GUI
- До 15000 AP
- Только для U(niversal) точек

## Cloud

- Управление сетью с веб-портала
- Простое конфигурирование и обновление ПО Firmware
- Мониторинг устройств, интерфейсов, событий ...

FortiLink for AP



# Что такое FortiLink?



**FortiLink**

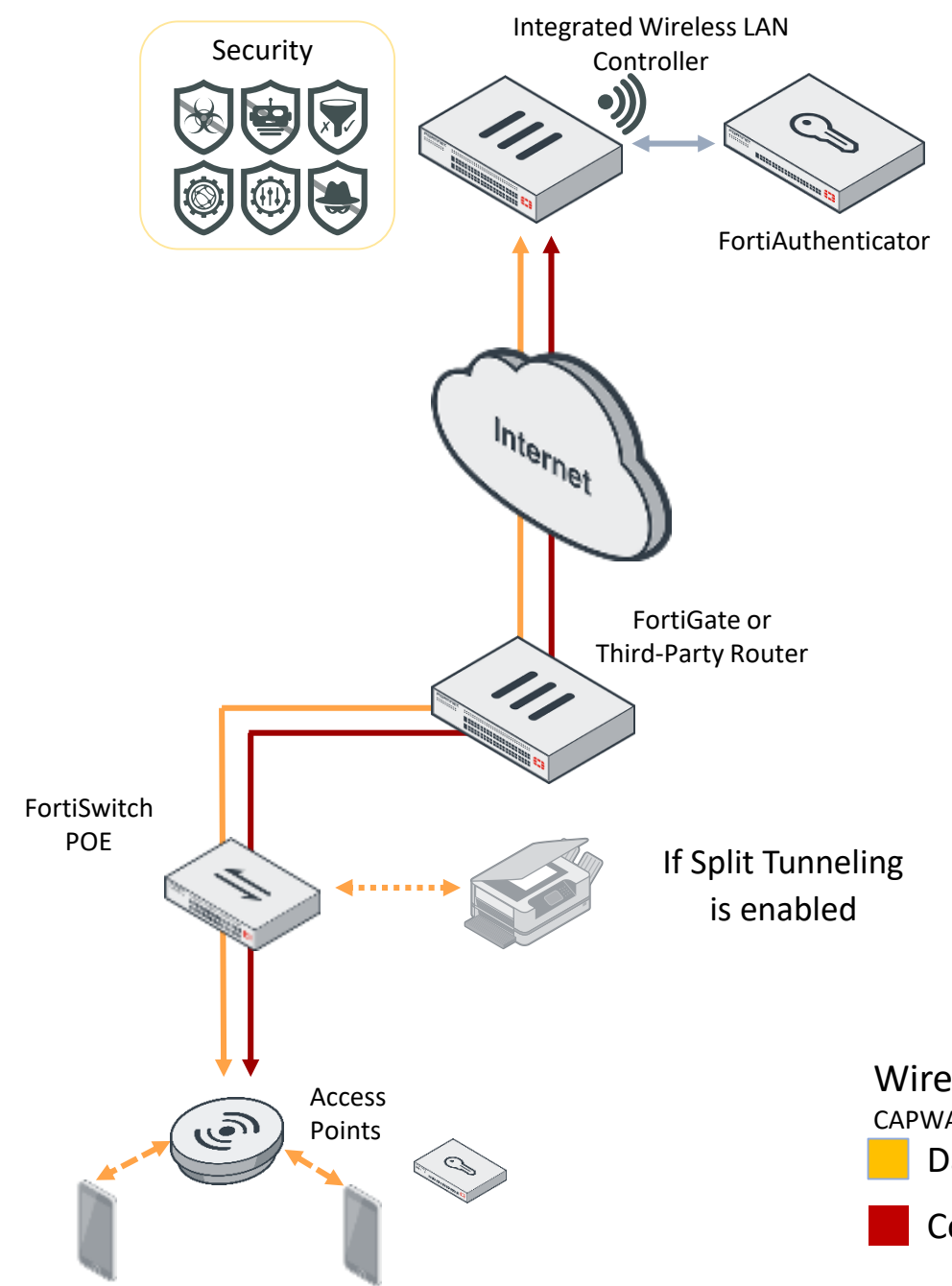
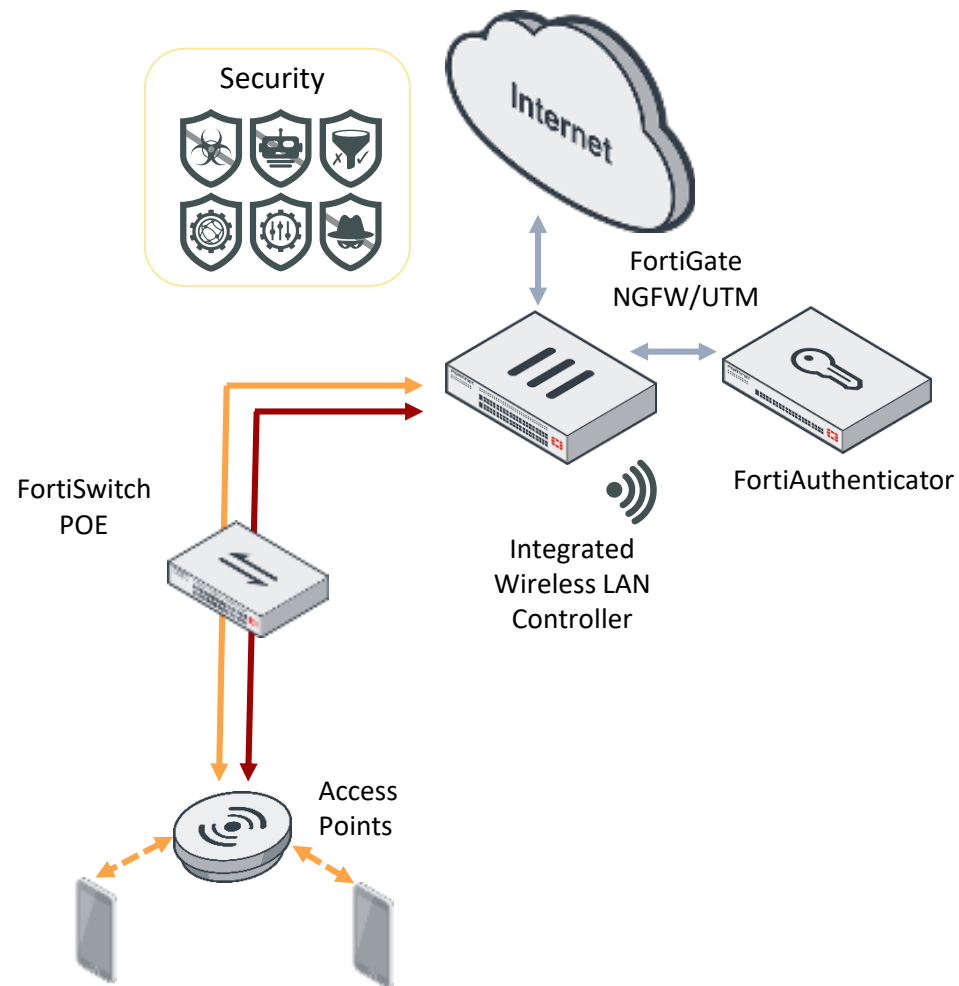
FortiLink представляет собой набор протоколов, которые позволяют FortiOS управлять коммутаторами и точками доступа

**FortiLink обеспечивает:**

- FortiLink Heartbeat
- LLDP -> обнаружение
- CAPWAP -> конфигурационные команды, обновление ПО
- NTP -> синхронизация времени с FGT
- HTTPS -> config и diag команды через REST API

# Tunnel Mode

## Сценарии применения

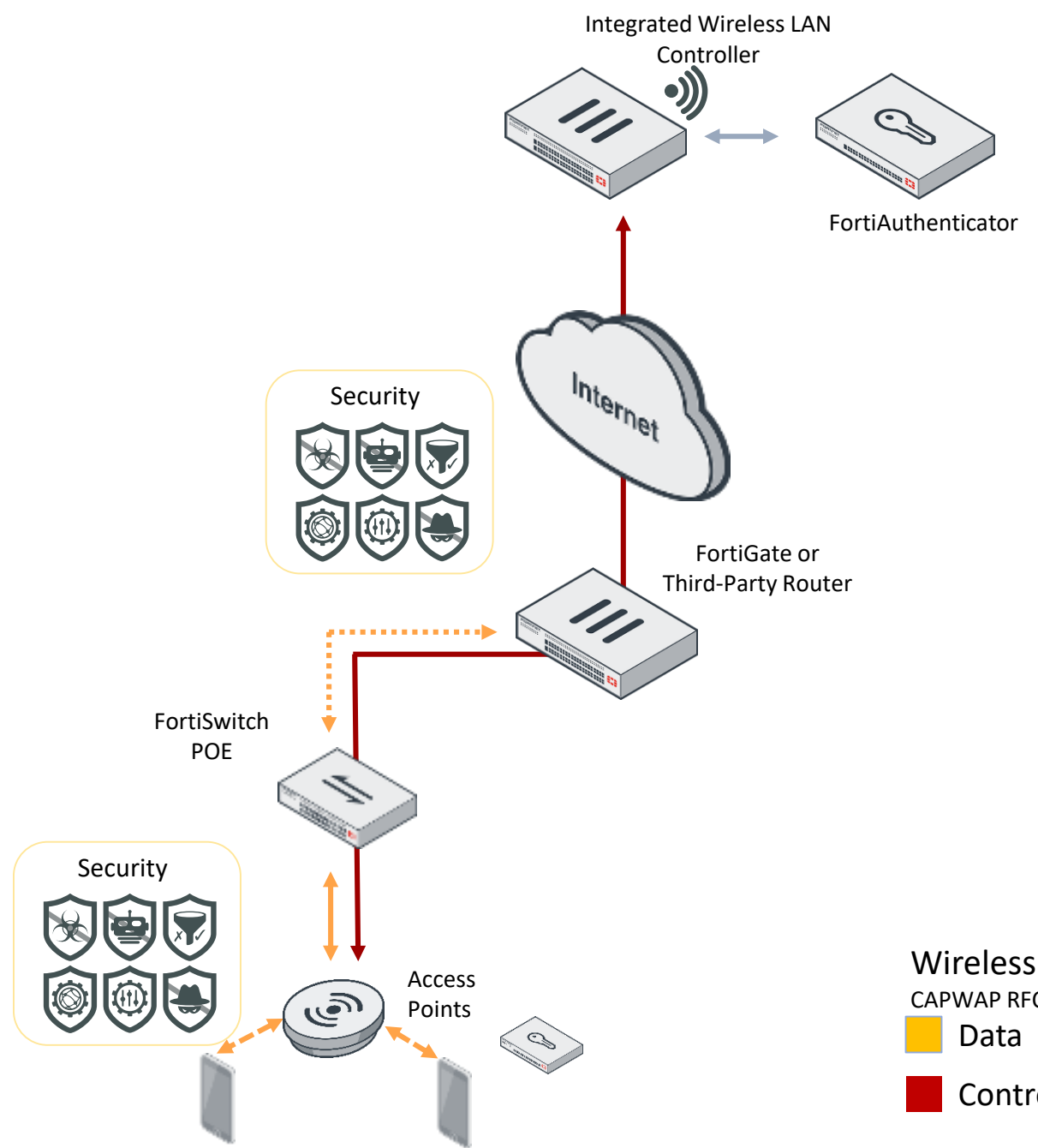
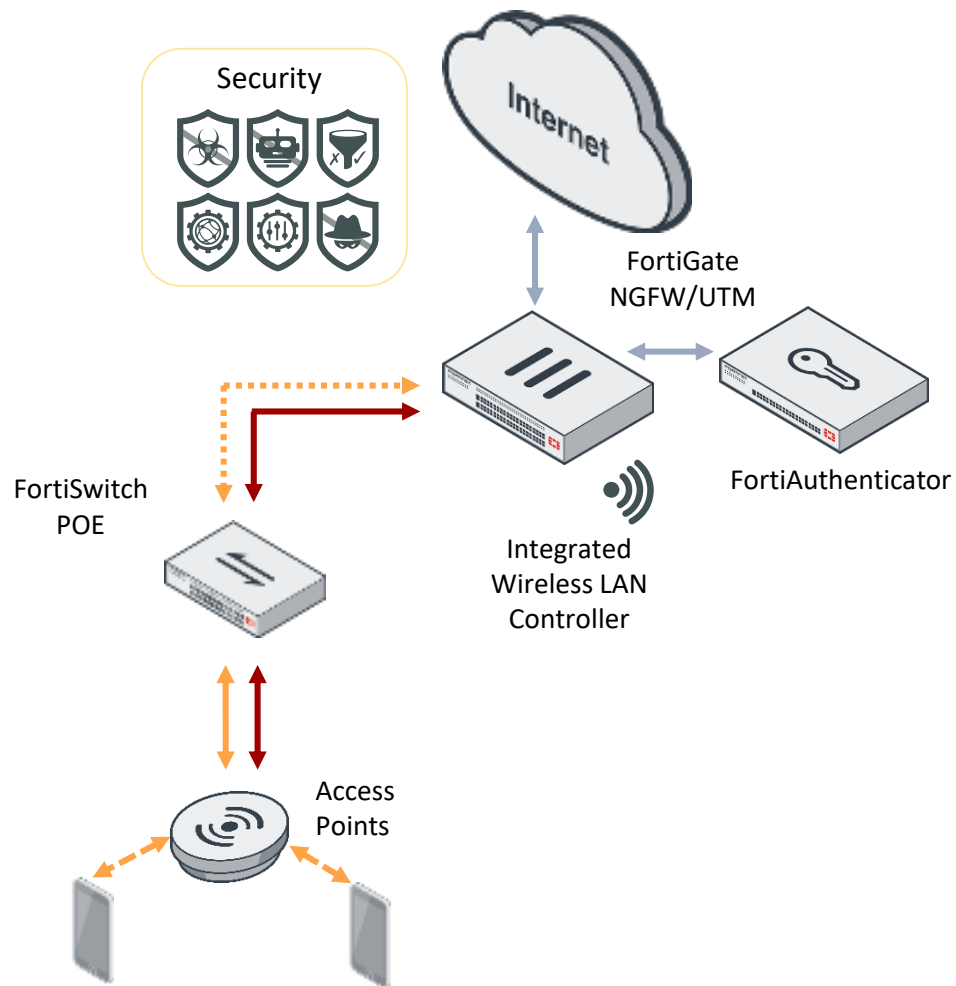


If Split Tunneling is enabled

Wireless Plane  
CAPWAP RFC 5415  
Data  
Control

# Local Bridge Mode

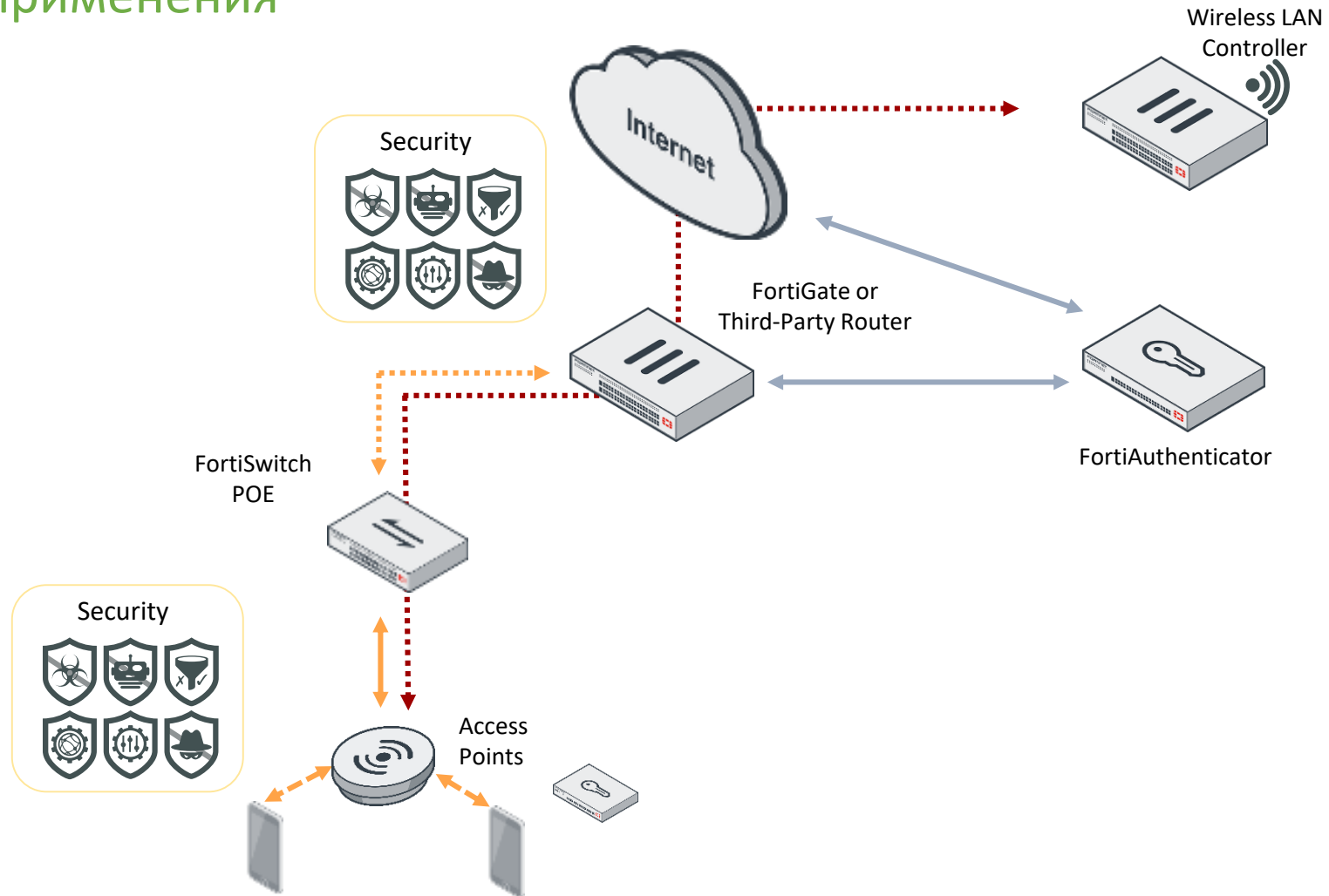
## Сценарии применения



Wireless Plane  
CAPWAP RFC 5415  
Data  
Control

# Local Standalone

## Сценарии применения



### Wireless Plane

CAPWAP RFC 5415

■ Data

■ Control

■ Internet

# 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



# Совместимость FortiOS и FortiAP firmware

FortiOS 6.2.x compatibility

FortiAP-U	FortiOS Versions							
	6.2.0	6.2.1	6.2.2	6.2.3	6.2.4	6.2.5	6.2.6	6.2.7
FAP-U24JEV	5.4.6	5.4.6	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U221EV	5.4.6	5.4.6	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U223EV	5.4.6	5.4.6	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U321EV	5.4.6	5.4.6	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U323EV	5.4.6	5.4.6	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U421EV	5.4.6	5.4.6	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U422EV	5.4.6	5.4.6	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U423EV	5.4.6	5.4.6	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U431F	N/A	N/A	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4
FAP-U433F	N/A	N/A	6.0.2	6.0.2	6.0.4	6.0.4	6.0.4	6.0.4

FortiOS 6.2.x compatibility

FortiAP	FortiOS Versions							
	6.2.0	6.2.1	6.2.2	6.2.3	6.2.4	6.2.5	6.2.6	6.2.7
Legacy Models								
FAP-221C	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6
FAP-320C	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6
FAP-321C	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6	6.0.6
Wi-Fi 6 Models								
FAP-23JF	N/A	N/A	N/A	N/A	N/A	6.4.4	6.4.4	6.4.4
FAP-231F	N/A	N/A	N/A	N/A	N/A	6.4.3	6.4.3	6.4.3
FAP-234F	N/A	N/A	N/A	N/A	N/A	6.4.4	6.4.4	6.4.4
FAP-431F	N/A	N/A	N/A	N/A	6.4.3	6.4.3	6.4.3	6.4.3
FAP-432F	N/A	N/A	N/A	N/A	N/A	6.4.4	6.4.4	6.4.4
FAP-433F	N/A	N/A	N/A	N/A	6.4.3	6.4.3	6.4.3	6.4.3

- **Всегда**, перед началом настроек проверяйте совместимость FSW-OS и FAP-OS
- **Внимательно читайте гайды** по настройке оборудования
- Таблица совместимости с FortiOS:

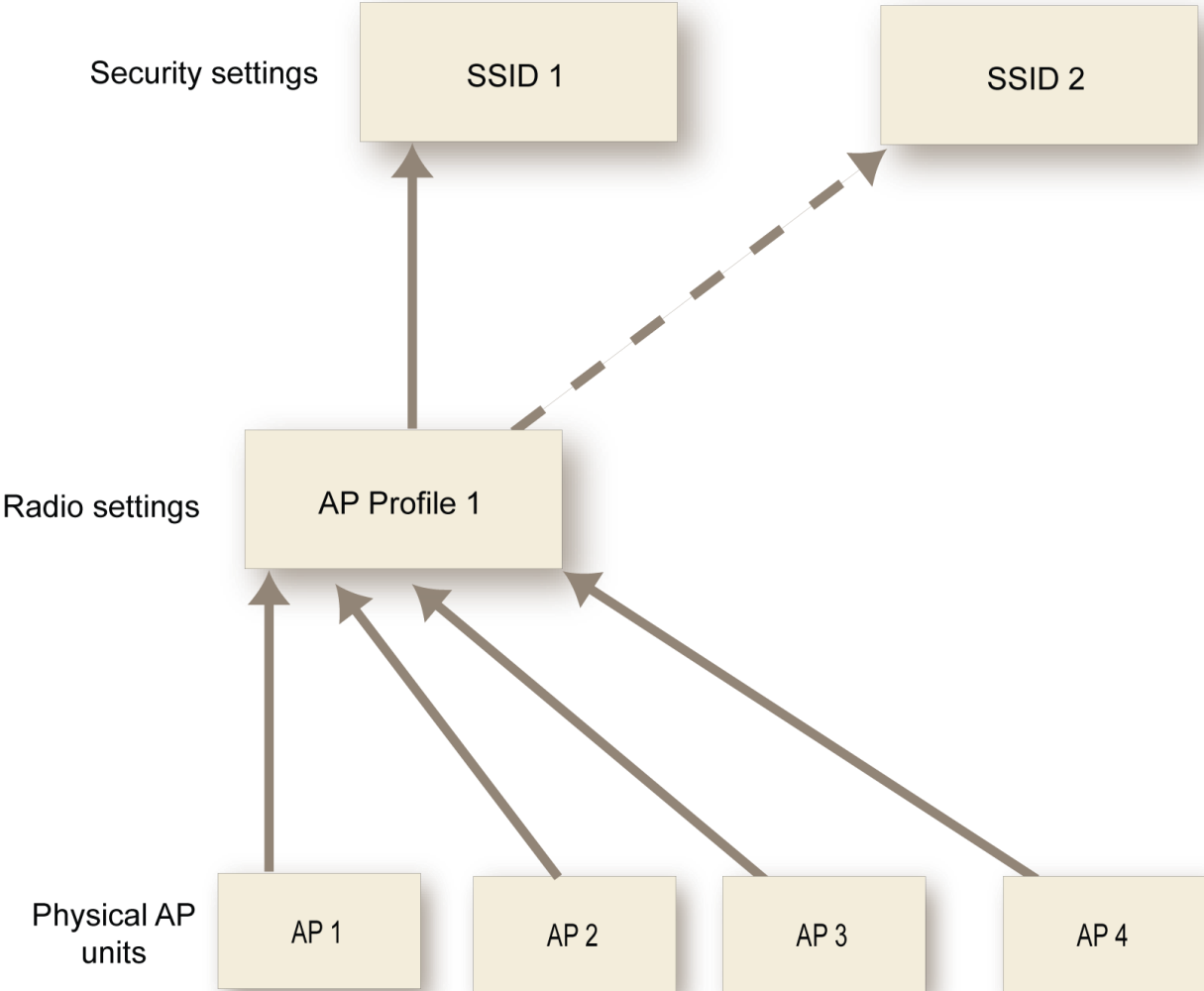
<https://docs.fortinet.com/document/fortiap/6.4.5/fortiap-and-fortios-compatibility-matrix/495193/fortiap-and-fortios-compatibility-matrix>

# FortiAP open ports and protocols

Outgoing ports		
Purpose		Protocol/Port
FortiAnalyzer	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246*
FortiCloud	Initial Discovery	TCP/443
	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246*
FortiGate	Syslog, Registration, Quarantine, Log & Report	TCP/443
	CAPWAP	UDP/5246*, UDP/5247*
FortiGuard	FortiGuard Queries	UDP/53, UDP/8888
	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246*

Reserved VLANS IDs: ~~97,98,898,899~~

# Conceptual view of FortiGate WiFi controller configuration



# AP profile

The screenshot shows the FortiGate 300E configuration interface for a new FortiAP profile. The interface is divided into a left sidebar, a main configuration area, and a right sidebar.

**Left Sidebar (Navigation):**

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

**Main Configuration Area (New FortiAP Profile):**

**General Settings:**

- 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 Settings:**

- 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 Settings:**

- [Empty text box]

**Right Sidebar (FortiGate Info):**

- FortiGate Demo-ISFW-PRI
- Documentation
- Online Help
- Video Tutorials

**Bottom Buttons:** OK, Cancel

# FortiAP local configuration via Web GUI

The screenshot displays the FortiAP S221E Web GUI configuration interface. The top navigation bar shows the device name 'FortiAP-S221E' and the user 'admin'. The left sidebar contains navigation options: Information, System Status, WTP Configuration, Radio Configuration, Settings, and Local Configuration (highlighted). The main configuration area is divided into sections: System, Network, Connectivity, and WTP Configuration. The 'System' section includes fields for Host Name, Login Password, FortiAP Location, and Idle Timeout (5 minutes). The 'Network' section includes Address Mode (DHCP), Management VLAN ID (0), DNS Server IP (208.91.112.53), Local IP Address (192.168.1.2), Local Network Mask (255.255.255.0), Gateway IP (192.168.1.1), and various access control options. The 'WTP Configuration' section includes AC Discovery Type (Auto), AC IP Address 1 (192.168.1.1), AC Host Name 1 (\_capwap-control\_udp.example.com), Multicast Address (224.0.1.140), DHCP Option Code (138), FortiAP Cloud Server, FortiAP Cloud Account, FortiAP Cloud Password, AC Control Port (5246), and AP Data Channel Security (Clear text, DTLS enabled, IPsec enabled). A dropdown menu is open on the right, listing actions: Backup Configuration, Restore Configuration, Upgrade Image, Reboot (highlighted with a red box), Download, and Logout. At the bottom, there are 'OK' and 'Cancel' buttons, and a status bar indicating 'CONFIG MODE (reboot to exit config mode)'.

FortiAP-S221E admin

**Information**

- Dashboard
- System Status
- WTP Configuration
- Radio Configuration

**Settings**

- Local Configuration

**System**

- Host Name
- Login Password
- FortiAP Location
- Idle Timeout (minute): 5
- Baud Rate:  9600  19200  38400  57600  115200
- LED State:  Enabled  Disabled  Controlled by AC
- WANLAN Mode:  WAN-ONLY  WAN-LAN  AGGREGATE
- Access Point Mode:  Thin AP  Site survey

**Network**

- Address Mode:  DHCP  STATIC
- Management VLAN ID: 0
- DNS Server IP (default): 208.91.112.53
- Local IP Address (default): 192.168.1.2
- Local Network Mask (default): 255.255.255.0
- Gateway IP (default): 192.168.1.1
- Allow HTTPS Access:  Disabled  Enabled  Controlled by AC
- Allow SSH Access:  Disabled  Enabled  Controlled by AC
- Spanning Tree Protocol Mode:  Disabled  Enabled  Disabled with blocked WAN port switch
- Bonjour Gateway:  Disabled  Enabled  Controlled by AC

**Connectivity**

- Uplink:  Ethernet  Mesh  Ethernet with mesh backup support

**WTP Configuration**

- AC Discovery Type:  Auto  Static  DHCP  DNS  Broadcast  Multicast  FortiAP Cloud
- AC IP Address 1: 192.168.1.1
- AC IP Address 2:
- AC IP Address 3:
- AC Host Name 1: \_capwap-control\_udp.example.com
- AC Host Name 2:
- AC Host Name 3:
- Multicast Address: 224.0.1.140
- DHCP Option Code: 138
- FortiAP Cloud Server:
- FortiAP Cloud Account:
- FortiAP Cloud Password:
- AC Control Port: 5246
- AP Data Channel Security:  Clear text  DTLS enabled  IPsec enabled

admin

- Backup Configuration
- Restore Configuration
- Upgrade Image
- Reboot
- Download
- Logout

OK Cancel

CONFIG MODE (reboot to exit config mode)

# FortiAP discovery for AP controller

WTP Configuration

AC Discovery Type	<input checked="" type="radio"/> Auto <input type="radio"/> Static <input type="radio"/> DHCP <input type="radio"/> DNS <input type="radio"/> FortiCloud <input type="radio"/> Broadcast <input type="radio"/> Multicast
AC IP Address 1	10.0.0.5
AC IP Address 2	
AC IP Address 3	
AC Host Name 1	_capwap-control._udp.exam
AC Host Name 2	
AC Host Name 3	
AC Discovery Multicast Address	224.0.1.140
AC Discovery DHCP Option Code	138
FortiCloud Account	
FortiCloud Password	
AP Data Channel Security	<input checked="" type="checkbox"/> Clear Text <input checked="" type="checkbox"/> IPsec Enabled <input checked="" type="checkbox"/> DTLS Enabled

\*Автоматическая авторизация:  
config system interface  
edit "lan"  
set auto-auth-extension-device enable  
next  
end

FortiWiFi 61E FortiWiFi-61E interim build0839 >\_ [?] [🔔] [👤 admin]

+ Create New Edit Delete Refresh **Authorize** Upgrade 1/10 Managed FortiAPs AP Radio Group

Access Point	Status	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Ref.
FP321C3X15001615	Online	10.0.99.152 - lan	Radio 1: FWF-61E-MESH (wifi-mesh) Radio 2: FWF-61E-MESH (wifi-mesh)	Radio1: 6 Radio2: 157	Radio 1: 1 Radio 2: 0	FP321C-v6.0-build0031	FAP321C-default (Overridden)	0
FP423E3X16000320	Waiting for Authorization	10.0.99.151 - FP321C3X15001615	Radio 1: CORP_WIFL_ACCESS (wifi-fake) Radio 2: FWF-61E-LOCAL (wifi)	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0	FP423E-v6.2-build0220	FAP423E-default	0

Edit  
> Edit in CLI  
Delete  
Drill Down to Details  
**Authorize**  
Deauthorize  
Restart  
Upgrade  
LED Blink  
Assign Profile  
> Connect to CLI

**Click on either "Authorize" to authorize the discovered FAP.**

Authorize or Deauthorize APs

# FortiAP configuration and details

The screenshot displays the FortiWiFi 51E configuration interface for a managed FortiAP. The top navigation bar shows the device name 'FortiWiFi 51E' and the user 'admin'. The left sidebar contains a menu with categories like Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, WiFi Maps, FortiLink Interface, Log & Report, and Monitor. The main content area is titled 'Edit Managed AP' and is divided into several sections:

- Serial Number:** FP423E3X16000320
- Name:** (empty text field)
- Comments:** Write a comment... (0/35)
- State:** Authorized ; WTP Mode: Normal
- Firmware:** Current: FP423E-v6.2-build0217; Upgrade button
- Wireless Settings:** FortiAP Profile: FAP423E-default
- Override Radio 1:** Band: 802.11n/g (2.4 GHz Band); Channels: 1, 6, 11; TX Power Control: 100%; SSIDs: QA-FWF-51E-SSID (QA-FWF-51E-SSID)
- Override Radio 2:** Band: 802.11ac (5 GHz Band); Channels: 36, 40, 44, 48, 149, 153, 157, 161; TX Power Control: 100%; SSIDs: FWF-51E-SSID (wifi)
- Override LAN Port:** Bridge to SSID: FWF-51E-SSID (wifi); Override:
- Override AP Login Password:**

The right-hand sidebar provides additional details:

- Status:** Connected
- Connected Via:** Ethernet (10.0.1.4)
- Base MAC Address:** 90:6c:ac:dc:62:28
- Join Time:** 2019/01/16 16:50:30
- Health:** Fair
- Radio 1:** Interfering APs, 1 Clients, 0% Channel Utilization
- Radio 2:** Interfering APs, 0 Clients, 0% Channel Utilization
- View More Details** button
- Documentation:** Online Help, Video Tutorials

At the bottom of the configuration area, there are 'OK' and 'Cancel' buttons.

# SSID

The screenshot displays the FortiGate 300E management console 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 to 'SSID'. The main content area is titled 'Create New SSID' and includes the following configuration sections:

- Name:** An empty text input field.
- Alias:** An empty text input field.
- Type:** A dropdown menu set to 'WiFi SSID'.
- Traffic mode:** Three radio buttons: 'Tunnel' (selected), 'Bridge', and 'Mesh'.
- Address:**
  - IP/Netmask:** A text input field containing '0.0.0.0/0.0.0.0'.
  - Create address object matching subnet:** A checked toggle switch.
  - Name:** An empty text input field.
  - Destination:** A text input field containing '0.0.0.0/0.0.0.0'.
  - Secondary IP address:** An unchecked toggle switch.
- Administrative access:** A grid of checkboxes for IPv4 access:
  - HTTPS, HTTP (with an info icon), PING
  - FMG-Access, SSH, SNMP
  - FTM, RADIUS Accounting, Security Fabric Connection (with an info icon)
- DHCP Server:** An unchecked toggle switch.
- Network:**
  - Device detection:** A checked toggle switch.
- WiFi Settings:**
  - SSID:** A text input field containing 'fortinet'.

At the bottom of the configuration window are 'OK' and 'Cancel' buttons. On the right side of the console, there is a 'FortiGate' sidebar with 'Demo-ISFW-PRI' and links for 'Documentation', 'Online Help', and 'Video Tutorials'.



# Local standalone SSID

The screenshot displays the FortiManager configuration interface for a Local Standalone SSID. The left sidebar shows the navigation menu with 'WiFi & Switch Controller' expanded and 'SSID' selected. The main content area is titled 'Edit Interface' and contains 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:**
- Local Authentication:**
- Client Limit per Radio:**

# FortiAP over MESH SSID uplink

FortiGate 80E-POE

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

Security Profile Groups

FortiLink Interface

Managed FortiSwitch

FortiSwitch VLANs

FortiSwitch Ports

FortiSwitch Security

Edit Managed AP

Override Radio 1

Band  802.11n (2.4 GHz Band)

Channels  1, 6, 11

TX Power Control  100%

SSIDs  MESH-UPLINK (mesh-uplink)

Auto Manual

MESH-UPLINK (mesh-uplink)

Override Radio 2

Band  802.11ac (5 GHz Band)

Channels  36, 40, 44, 48, 149, 153, 157, 161

TX Power Control  100%

SSIDs  MESH-UPLINK (mesh-uplink)

Auto Manual

MESH-UPLINK (mesh-uplink)

Override AP Login Password

Ethernet (10.180.101)

Base MAC Address  
90:6c:ac:03:9a:ee

Join Time  
2019/03/07 19:40:22

Radio 1

21 Interfering APs

0 Clients

23% Channel Utilization

Radio 2

0 Interfering APs

0 Clients

0% Channel Utilization

View More Details

WiFi Users

Setup guides

Learn how to configure guest WiFi accounts

Documentation

Online Help

Video Tutorials

OK Cancel

Connectivity

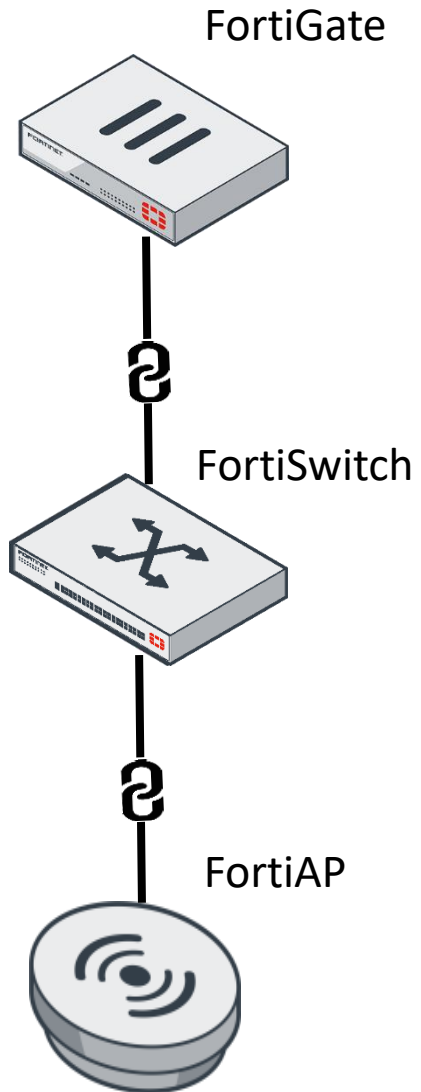
Uplink  Ethernet  Mesh  Ethernet with mesh backup support

Mesh AP SSID FWF-61E-MESH

Mesh AP Password .....

Ethernet Bridge

# Развертывание и управление сетью с Security Fabric + FortiLink



The screenshot shows the FortiGate 300E management interface for a device named 'Demo-ISFW-PRI'. The interface is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: Favorites, Dashboard, Security Fabric (highlighted), Physical Topology (highlighted with a star), 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 content area displays a network topology diagram. At the top left, there is a FortiGate device (FGT2KE391600421) connected to a central HA Active-Passive cluster of two FortiGate devices (Demo-ISFW-PRI and Demo-ISFW-BKP). This cluster is connected to a central switch (DISTR-B). From DISTR-B, multiple lines radiate out to various other devices: FAC\_ACC\_SW, ENG\_ACC\_SW, FIN\_ACC\_SW, SALES\_ACC\_SW, IT\_ACC\_SW, Demo-ISFW-ENG, Demo-ISFW-FIN, Demo-ISFW-SALES, HR\_ACC\_SW, SALES\_AP, FIN\_AP, and ENG\_AP. On the right side, there are two large circular nodes representing network segments, each with a traffic volume indicator (e.g., 39.96 GB and 54.34 GB). The interface also includes a search bar, a 'Sort By' dropdown set to 'Bytes (Sent/Received)', and various status indicators at the top right.

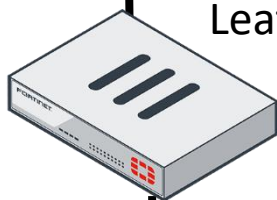


# Развертывание и управление сетью с Security Fabric + FortiLink

Root FortiGate



Leaf FortiGate



FortiAP



Access Device No Access Device Device Traffic now No Critical Risk

Sort By: Bytes (Sent/Received)

Internet

FG100D3G14823104

FG201E4Q17900485

FP320C3X17001889

FP321C3X16002600

PU421E3X16004993

FP320C3X17001889

FP321C3X16002600

PU421E3X16004993

Security Fabric: 100d\_csf

FortiGate Telemetry

Please authorize the highlighted devices below.

Group name: 100d\_csf

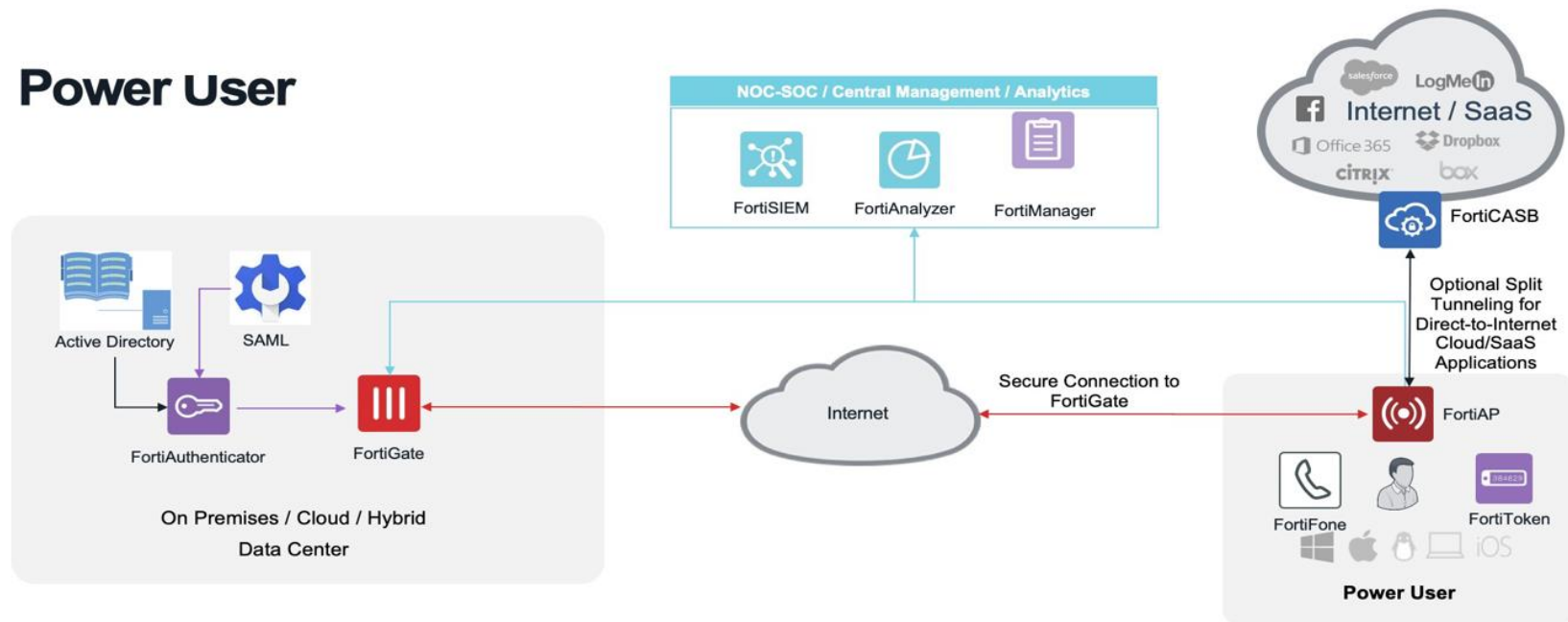
Group password: .....

Topology:

- FG100D3G14823104
  - FG201E4Q17900485
    - FP320C3X17001889
    - FP321C3X16002600
    - PU421E3X16004993
  - FP320C3X17001889
  - FP321C3X16002600
  - PU421E3X16004993

# Развертывание с Security Fabric + Remote AP

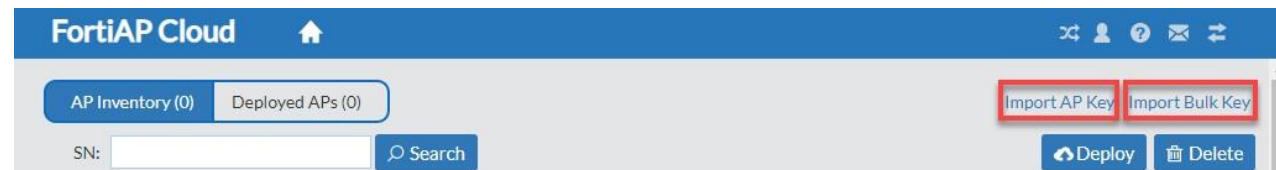
## Power User



## 1. Manual setting on AP FGate WAN IP

AC Discovery Type	<input checked="" type="radio"/> Auto <input type="radio"/> Static <input type="radio"/> DHCP <input type="radio"/> DNS <input type="radio"/> FortiCloud
AC IP Address 1	10.0.0.5
AC IP Address 2	
AC IP Address 3	
AC Host Name 1	_capwap-control_udp.exam
AC Host Name 2	
AC Host Name 3	

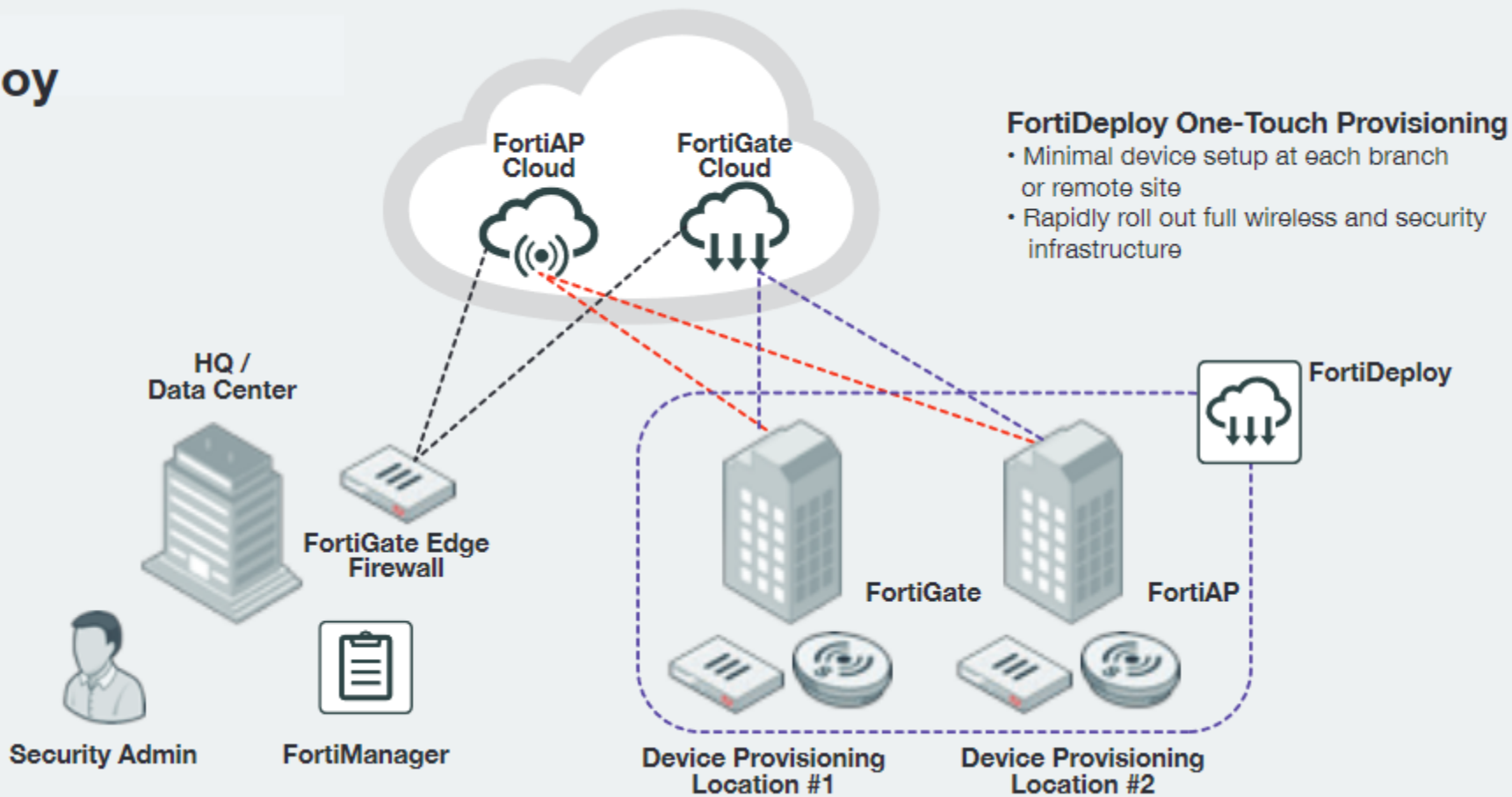
## 2. Deploy with FortiCloud



Deploy to External AC setting: FortiGate WAN IP

# Развертывание с FortiDeploy

## FortiDeploy



# Развертывание с Security Fabric + Remote AP

**Edit Interface**

Interface Name: wan1 (E8:1C:BA:BC:8C:13)  
Alias:   
Link Status: Up   
Type: Physical Interface  
Estimated Bandwidth: 0 kbps Upstream, 0 kbps Downstream

**Tags**

Role: WAN   
[Add Tag Category](#)

**Address**

Addressing mode: **Manual** DHCP PPPoE  
IP/Network Mask: 10.10.10.3/255.255.255.0

**Administrative Access**

IPv4:  HTTPS  HTTP  PING  FMG-Access  
 CAPWAP  DNP  SSH  SNMP  
 FTM  RADIUS Accounting  
 FortiTelemetry

**New FortiAP Profile**

Name:   
Comments: Write a comment...  
Platform: FAP221E  
Country / Region: **Use default (United States)** Specify  
AP login password: Set **Leave Unchanged**  
Administrative access:  HTTPS  SSH  
Client load balancing:  Frequency Handoff  AP Handoff

**Split Tunneling**

Include Local Subnet   
Split Tunneling Subnet(s)

Radio 1

**Security Fabric Settings**

FortiGate Telemetry 2

**Please authorize the highlighted devices below.**

Security Fabric role: **Serve as Fabric Root** Join Existing Fabric  
Fabric name: Fabric  
Topology:  
FGT60E (Fabric Root)  
FP221E5519064307  Authorize  
FG5H1E5818905207

# FortiWiFi monitoring: AP details/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

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

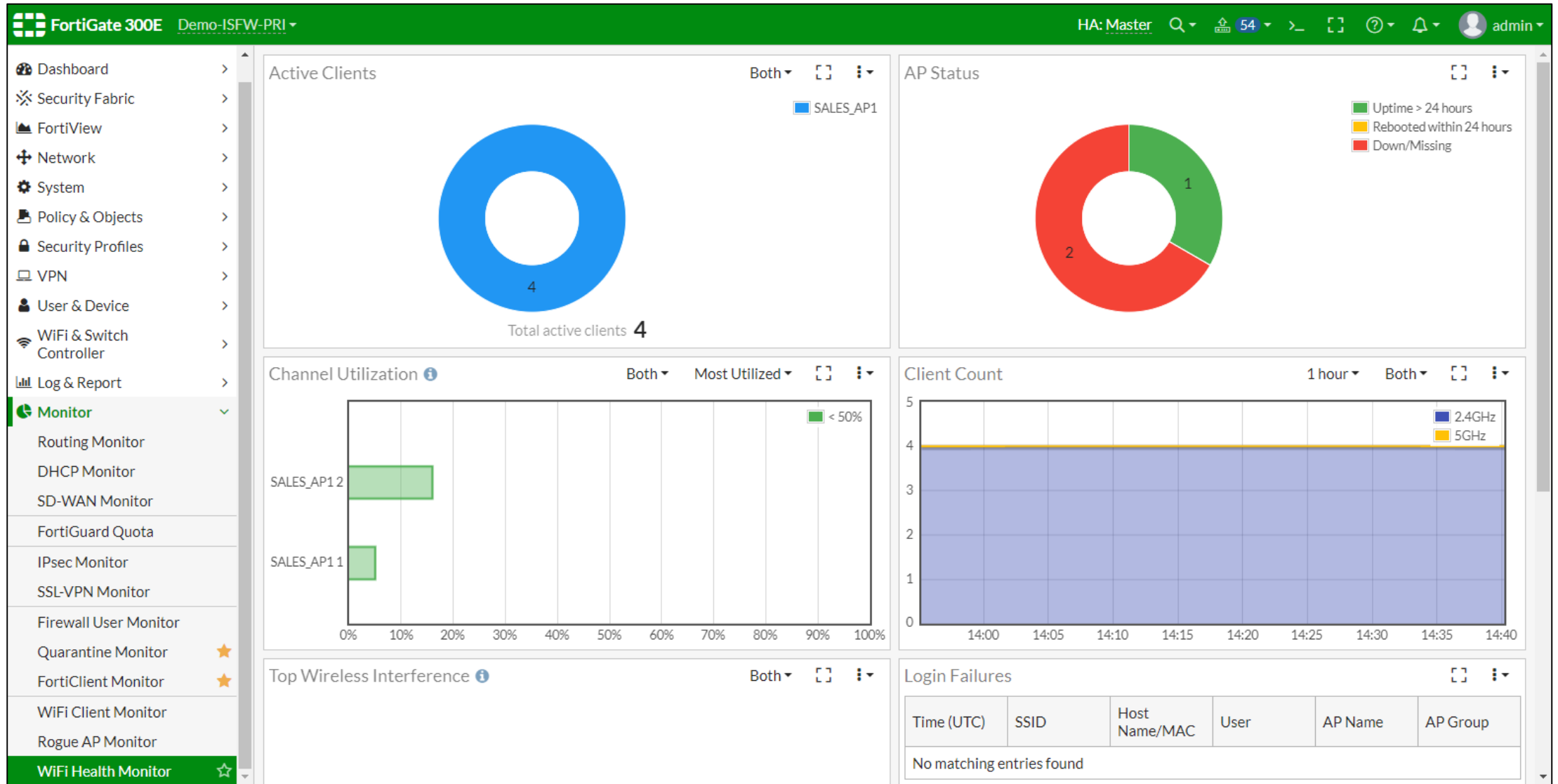
### Duty Cycle

### Duty Cycle Spectrogram

Close



# FortiWiFi monitoring: Health Monitor



# FortiWiFi monitoring: Maps

The screenshot displays the FortiGate 300E WiFi monitoring interface. The top header shows the device name 'FortiGate 300E', the demo environment 'Demo-ISFW-PRI', and the HA status 'HA: Master'. The user 'admin' is logged in. The interface includes a sidebar with navigation options and a main area showing a floor plan with three APs: SALES\_AP1 (blue), FIN\_AP1 (red), and ENG\_AP1 (red). SALES\_AP1 has a client count of 4. The interface also shows a search bar for '0 Unplaced AP(s)', a refresh button, and filters for 'Both Bands', 'Client Count', and 'LAB'. The sidebar lists various configuration options under 'WiFi & Switch Controller', including 'Managed FortiAPs', 'WiFi Maps', 'SSID', 'FortiAP Profiles', 'WIDS Profiles', 'FortiLink Interface', 'Managed FortiSwitch', 'FortiSwitch VLANs', 'FortiSwitch Ports', and 'FortiSwitch Security Policies'. The main area shows a floor plan with three APs: SALES\_AP1 (blue), FIN\_AP1 (red), and ENG\_AP1 (red). SALES\_AP1 has a client count of 4. The interface also shows a search bar for '0 Unplaced AP(s)', a refresh button, and filters for 'Both Bands', 'Client Count', and 'LAB'. The sidebar lists various configuration options under 'WiFi & Switch Controller', including 'Managed FortiAPs', 'WiFi Maps', 'SSID', 'FortiAP Profiles', 'WIDS Profiles', 'FortiLink Interface', 'Managed FortiSwitch', 'FortiSwitch VLANs', 'FortiSwitch Ports', and 'FortiSwitch Security Policies'.

# FortiWiFi monitoring: Security rating

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

Security Rating

Security Control Results

Severity of Failed Security Controls

Device Types

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.

**MARVEL**  
Дистрибуция

Hasta la vista!