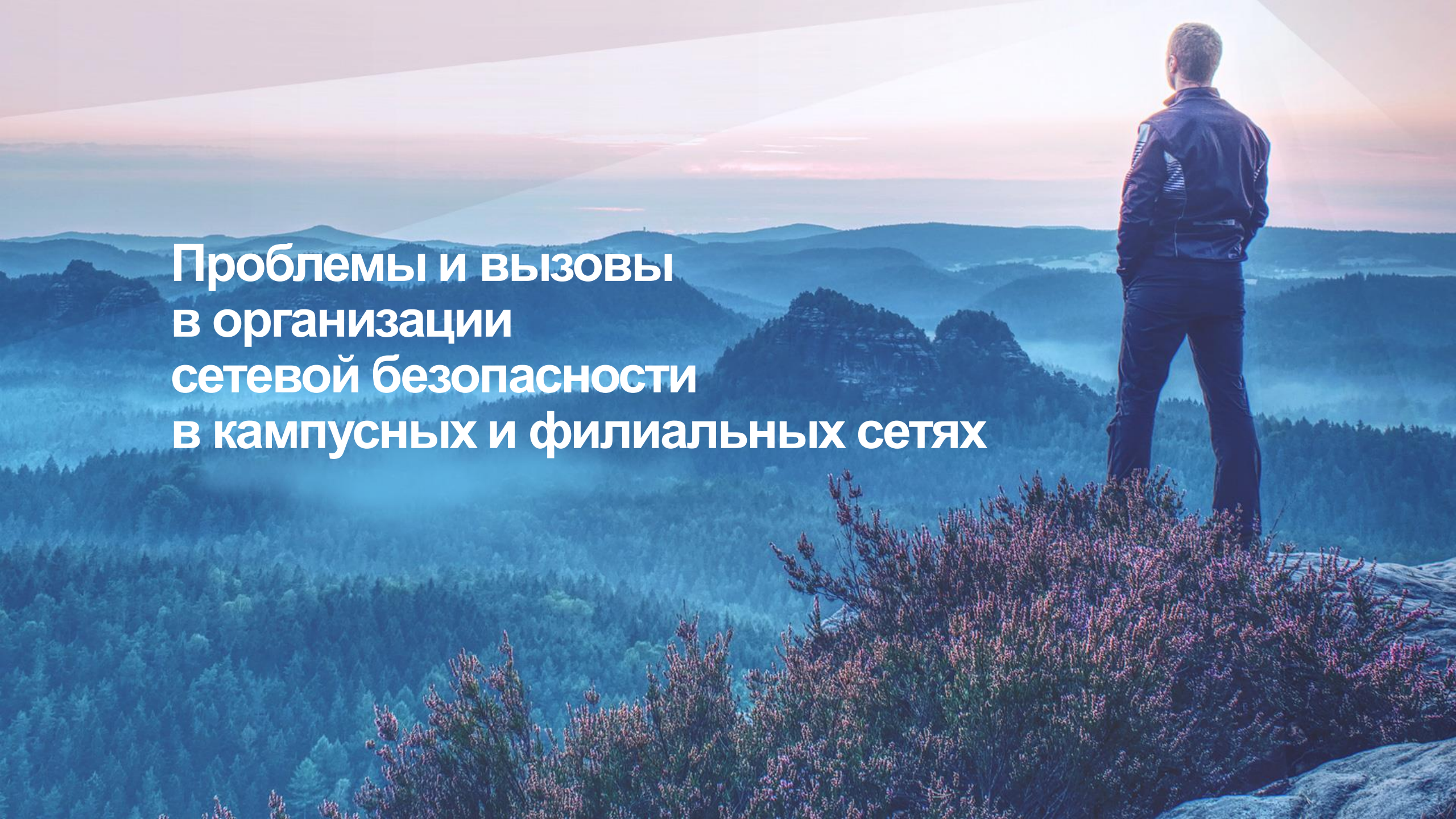
Организация сетевой безопасности в кампусных и филиальных сетях

Chingis Taltaev

SE

ctaltaev@fortinet.com

17.07.2020

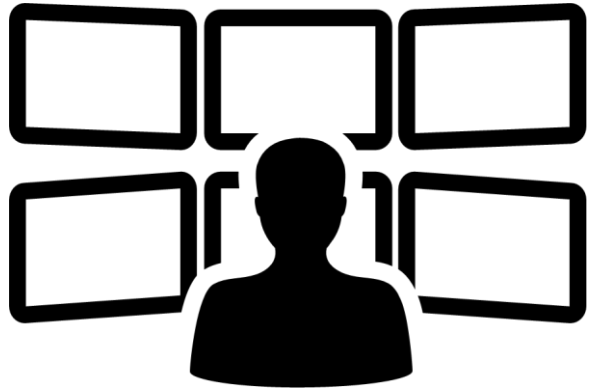


Проблемы и вызовы в организации сетевой безопасности в кампусных и филиальных сетях

Вызовы для уровня доступа

Рост количества пользовательских устройств

Обеспечение безопасности



Сложность управления

Вызовы для уровня доступа

Количество устройств

Снижается производительность

Безопасность

Сложность при интеграции с устройствами безопасности

Управление

Увеличивается время на решение инцидентов

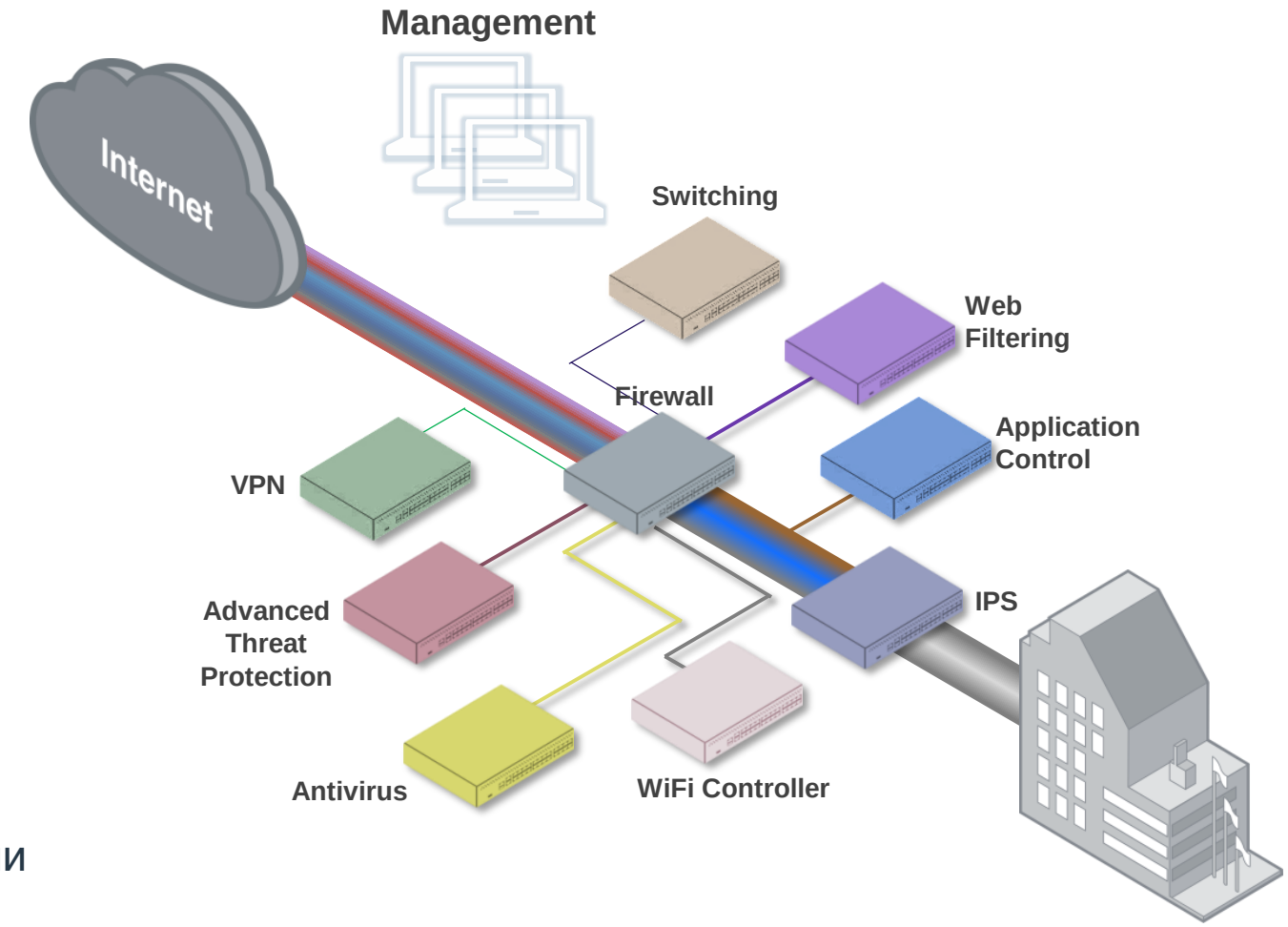
Безопасная проводная и беспроводная сеть в кампусе или филиале ?

Традиционный подход защиты на уровне доступа = Сложность

Сложность - это враг заказчика

- Множество точечных решений
- Множество платформ
- Множество консолей управления
- Отсутствие встроенной консистентности политик и сетевой части
- Различные циклы обновлений

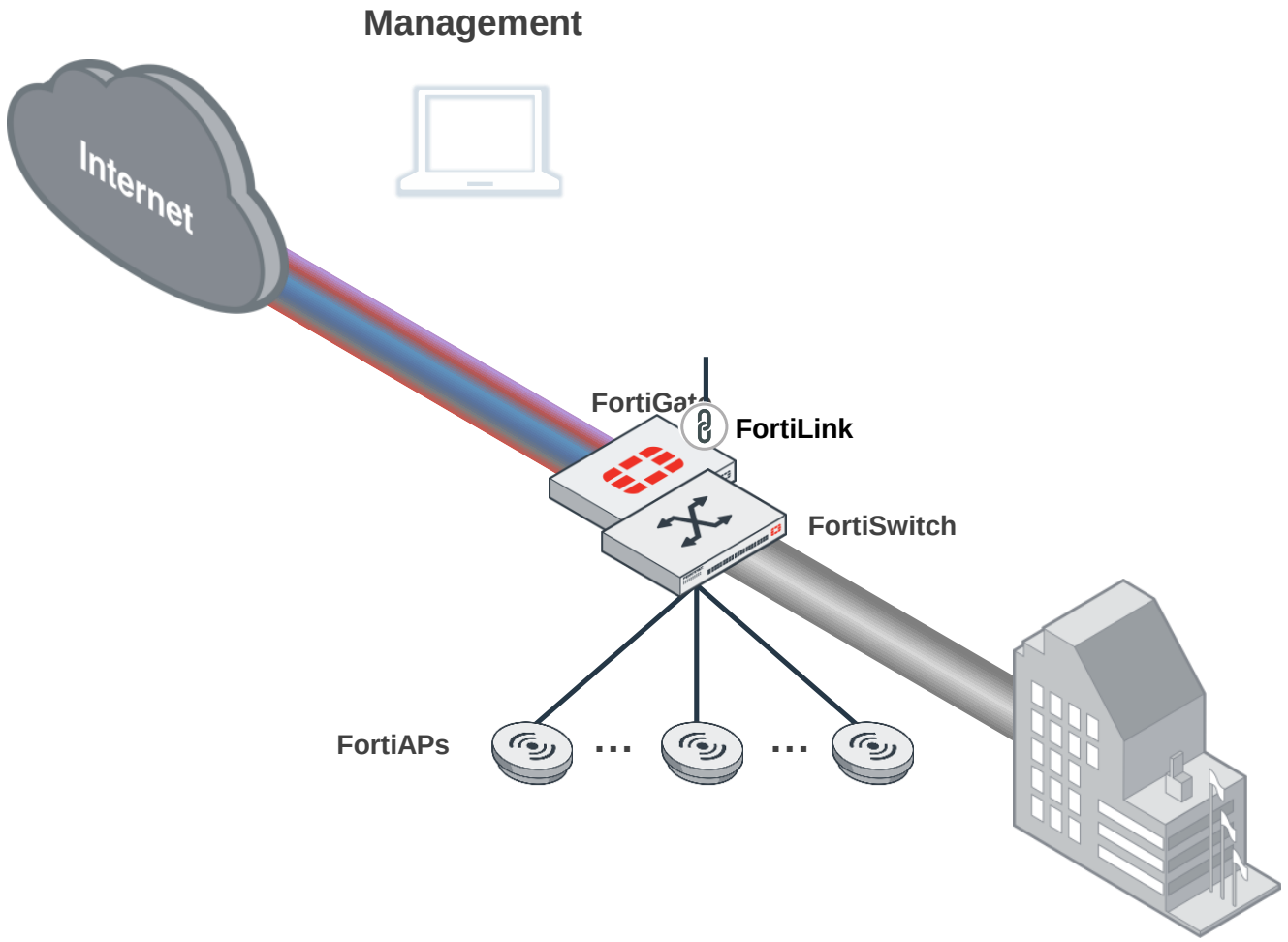
- Медленная и неоднозначная реакция на инциденты безопасности
- Постоянные сложности в поддержке
- Постоянные сложности в конфигурировании



Security driven подход к защите уровня доступа

FortiGate заменяет все апплайнсы и контролирует уровень доступа:

- FortiLink
  - Порты коммутаторов является расширением NGFW
- FortiLink wireless (CAPWAP)
  - SSIDs являются расширениями (логическими портами) NGFW
- Нет никаких лицензий на подключение точек доступа и коммутаторов !



Fortinet Security Fabric

Комплексная

Обеспечение полной видимости поверхности цифровой атаки для лучшего управления рисками ИБ

Интегрированная

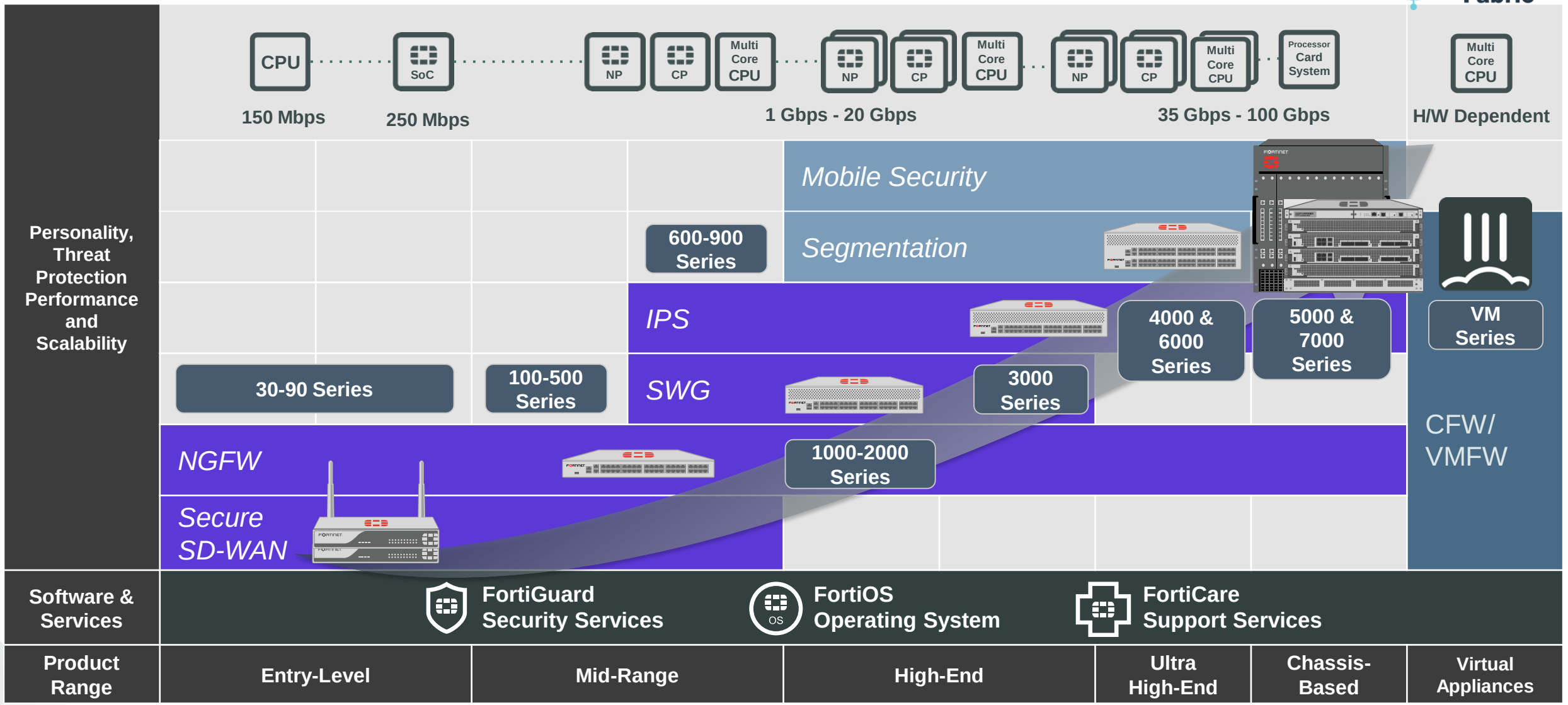
Уменьшение сложности сопровождения множества разнородных продуктов

Автоматизированная

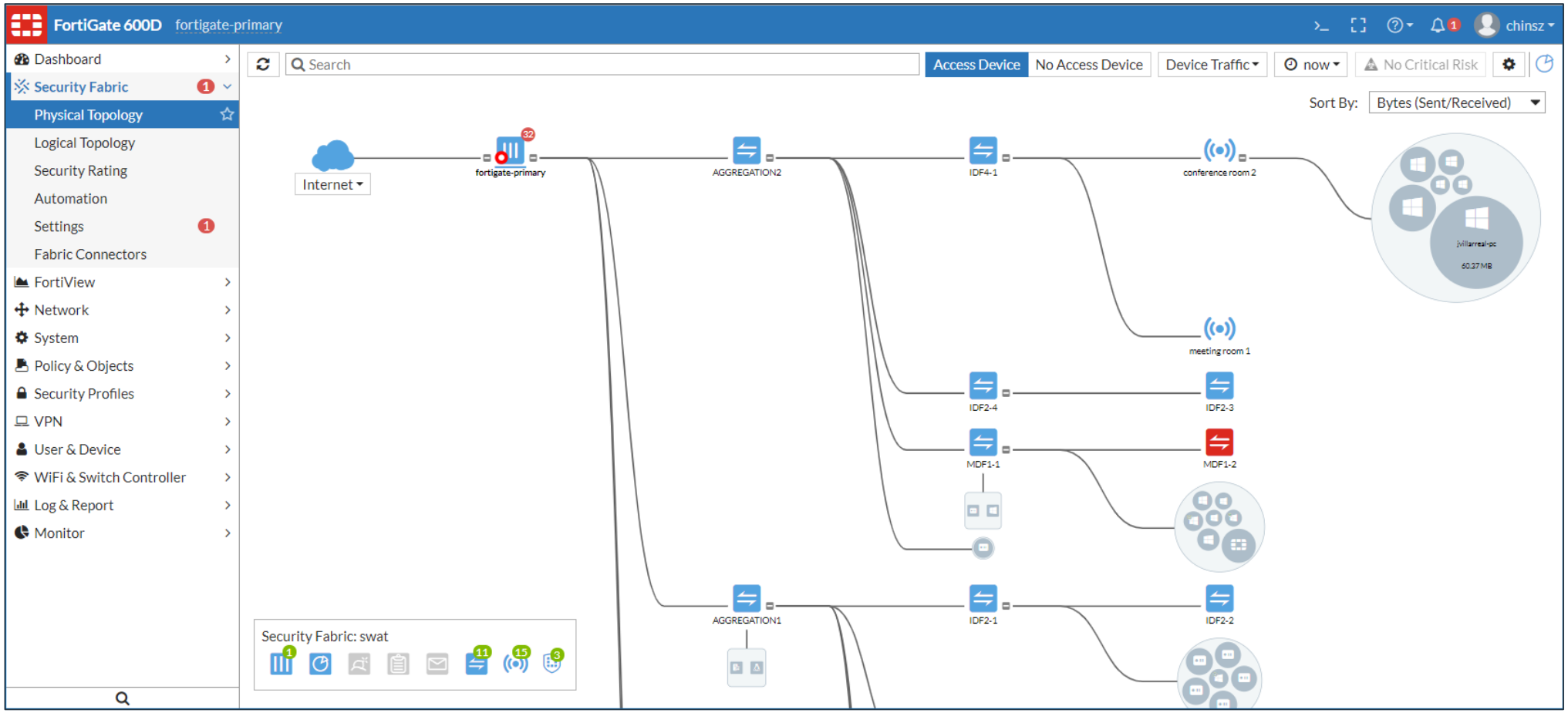
Увеличение скорости управления и отклика

Продуктовый ряд FortiGate

Fortinet Security Fabric



Расширение Security Fabric до уровня доступа = Простота управления и видимость



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

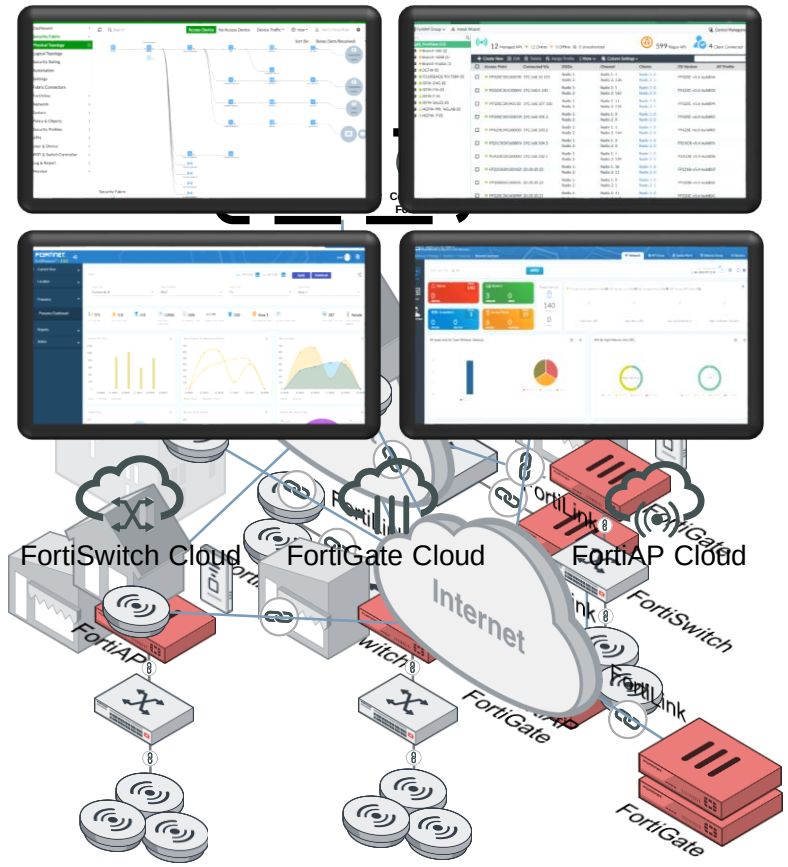
Management and Analytics

FortiGate

FortiManager

FortiPresence

FortiWLM



Campus

SD-Branch

Teleworker

Security-driven Networking

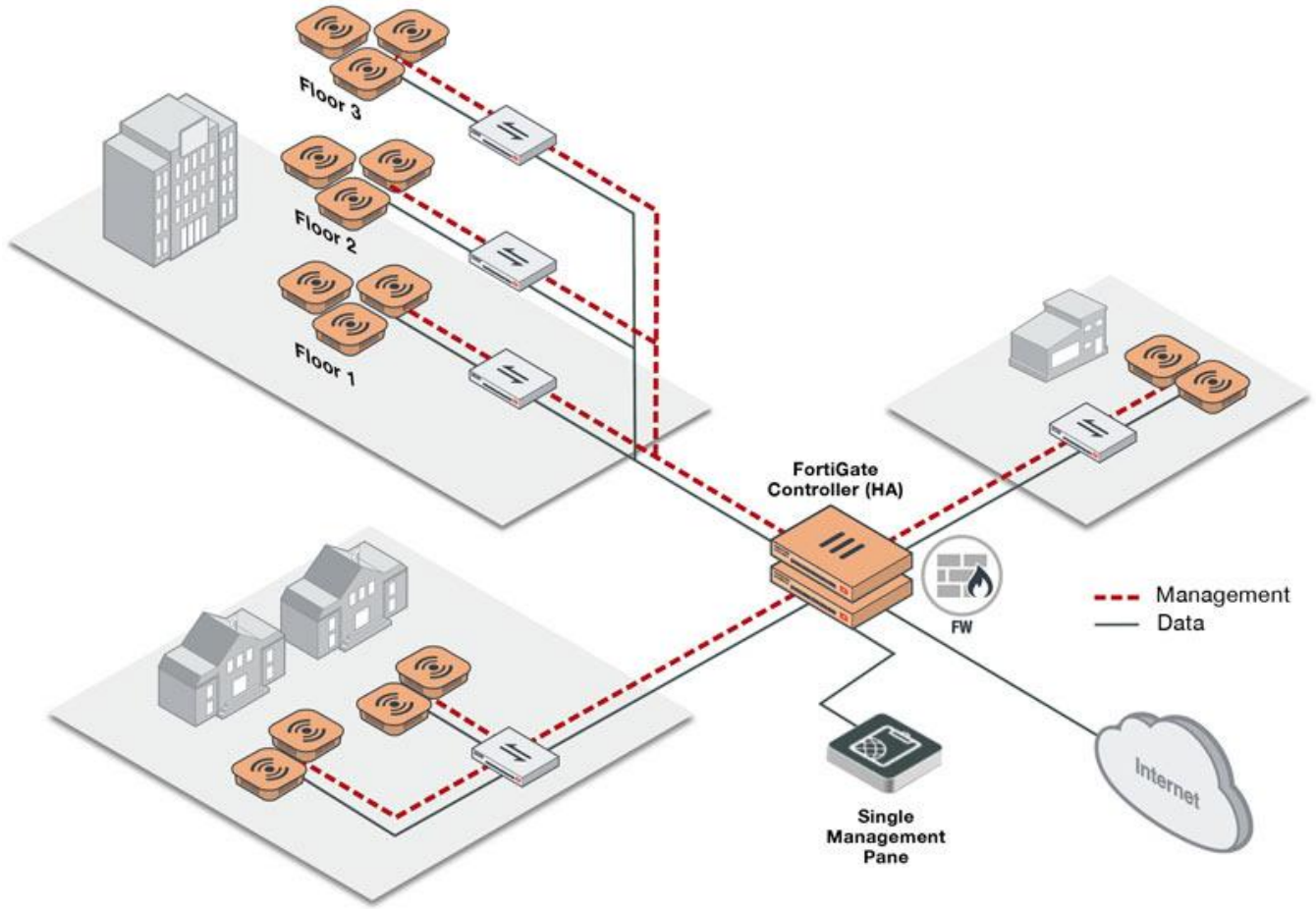
Обзор решения Integrated Wireless

Обзор решения Cloud Wireless

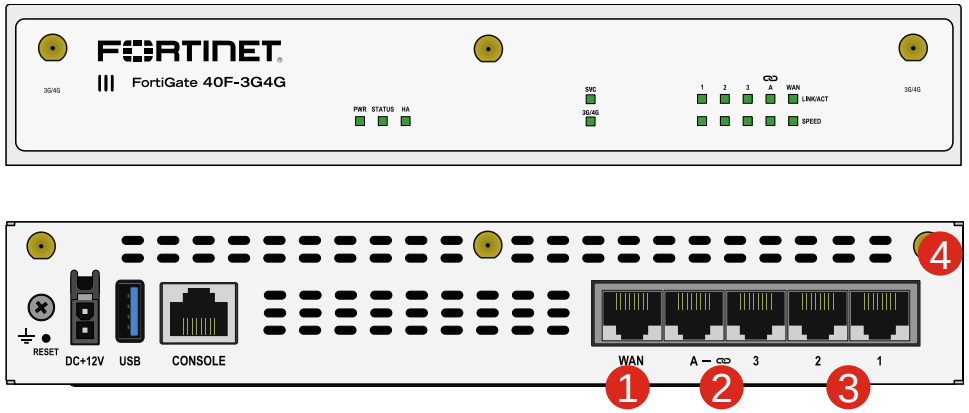
Security-driven Networking

Решение Integrated Wireless

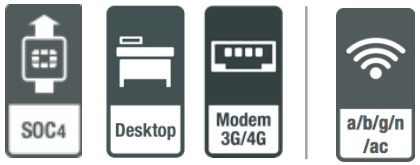
- FortiGate – это контроллер БЛВС !
- FortiAP – поддерживаемое семейство точек доступа
- Единое управление сетевой безопасностью и БЛВС
- Плотная интеграция с другими компонентами Fortinet Security Fabric
- Нет лицензий на подключение Wi-Fi точек доступа (базовый функционал FortiOS)
- Поддержка до 8192 Wi-Fi точек доступа FortiAP в зависимости от модели FortiGate



FortiGate/FortiWiFi 40F-3G4G



1. 1 x GE RJ45 WAN Port
2. 1 x GE RJ45 FortiLink Port
3. 3 x GE RJ45 Ports
4. WiFi Variant: 802.11a/b/g/n/ac W2



5 Gbps
Firewall throughput

35,000
New Sessions/Sec

700,000
Concurrent Sessions

310 Mbps
SSL Inspection Throughput

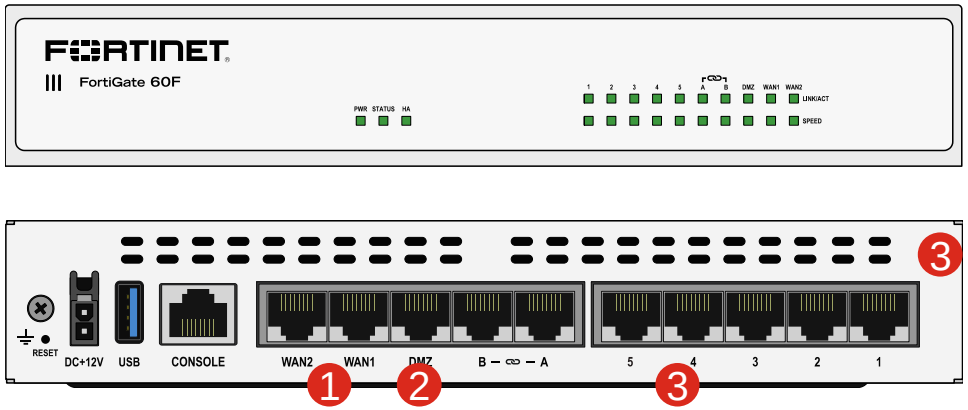
1 Gbps
IPS Throughput

800 Mbps
NGFW Throughput

600 Mbps
Threat Protection Throughput

Small Business / Remote Office
NGFW / Secure SD-WAN

FortiGate/FortiWiFi 60/61F



1. 2 x GE RJ45 WAN Ports
2. 1 x GE RJ45 DMZ Port
3. 7 x GE RJ45 Ports

10 Gbps
Firewall throughput

35,000
New Sessions/Sec

700,000
Concurrent Sessions

630 Mbps
SSL Inspection Throughput

1.4 Gbps
IPS Throughput

1. Gbps
NGFW Throughput

700 Mbps
Threat Protection Throughput

Small Business / Remote Office
NGFW / Secure SD-WAN

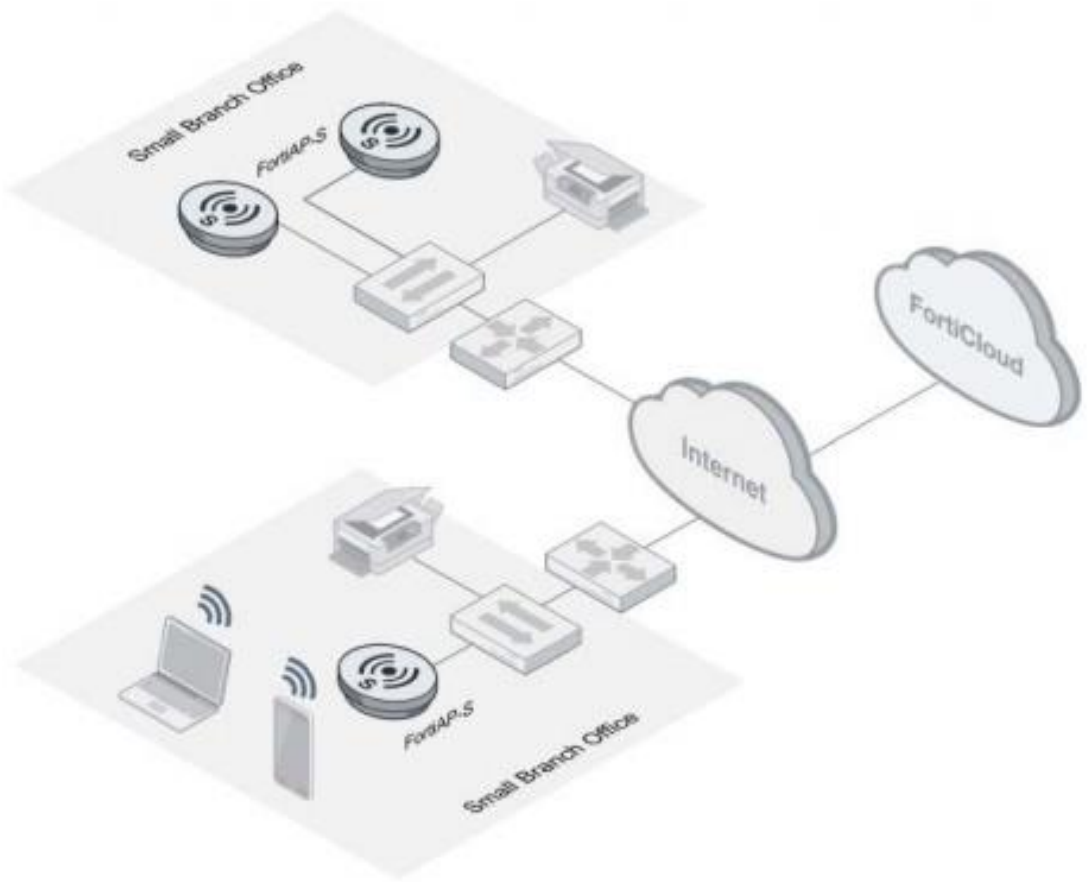
Security-driven Networking

Решение Cloud Wireless

- FortiAP Cloud – облачное управление FortiAP / FortiAP-S (без FortiGate)
- Лицензия на подключение к FortiAP Cloud уже включена в поставку FortiAP
- Отдельное семейство точек доступа FAP-S с поддержкой сервисов FortiGuard на борту (IPS, AV, AntiBot, AppControl, Web Filtering)

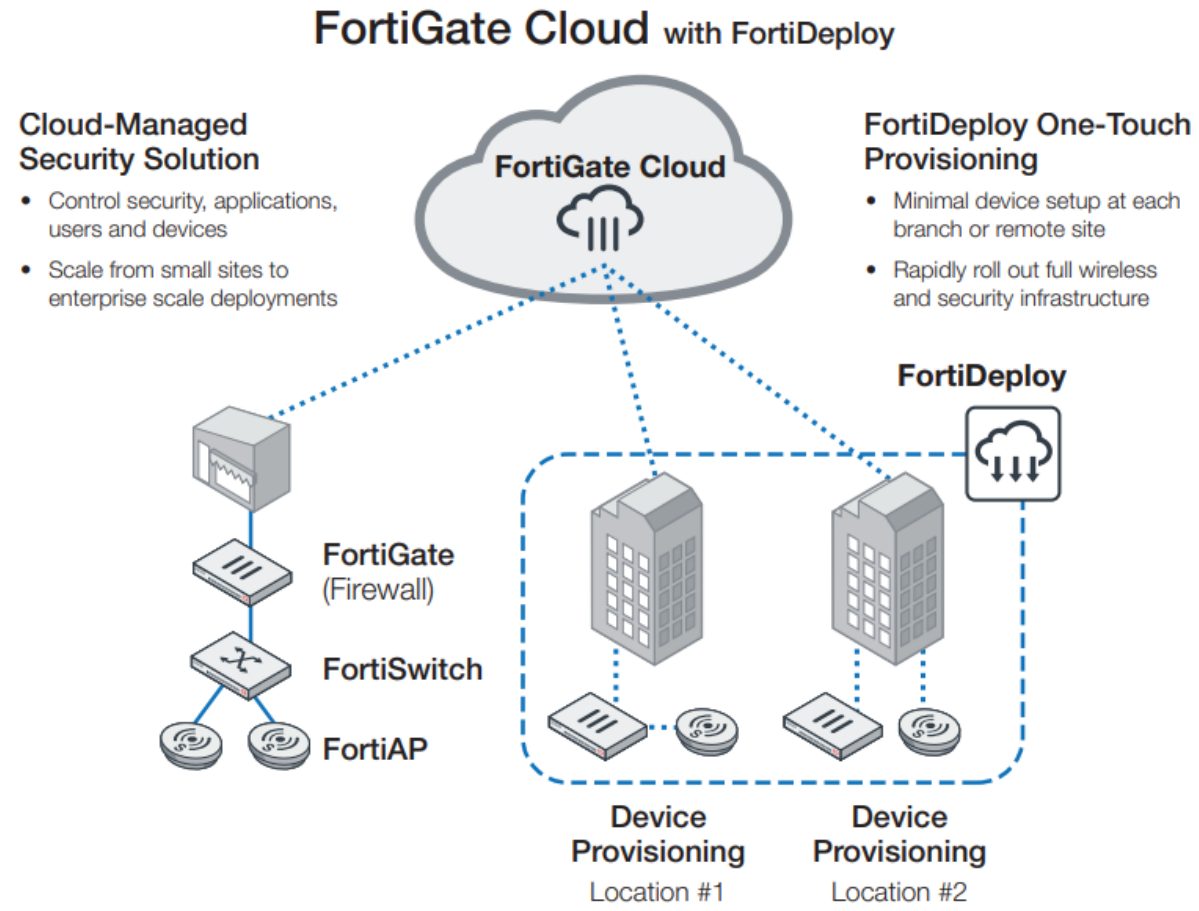
Fortinet Smart Remote Solution

Connection	1. Initial WiFi Connection
Credential Lookup	2. Lookup user
Authentication	3. Auth via Captive Portal, 802.1X, PSK
IPS, AV, Botnet	4. Scan with IPS, AV and botnet engine
URL Filter, App Control	5. Allow/block URLs and apps
Continue to Wire	6. Only clean traffic continues to wire



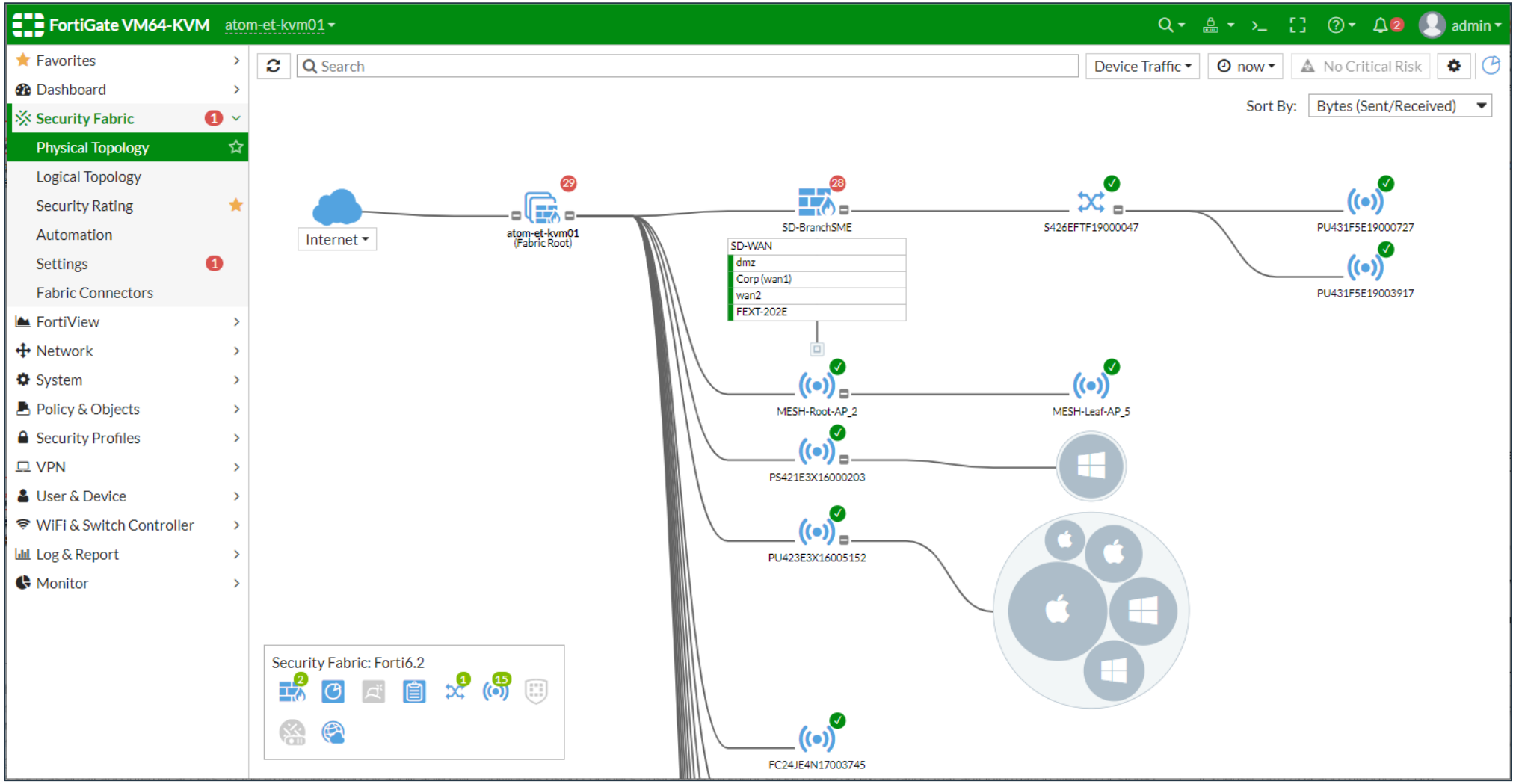
Security-driven Networking

FortiGate Cloud - облачное управление для FortiGate + FortiAP + FortiSwitch



Security-driven Networking

Визуализация логической и физической топологии ЛВС



Позиционирование семейств беспроводных точек доступа FortiAP

Fortinet Security Fabric

FAP-U
Universal

- Controller
- Integrated
- Cloud

FAP

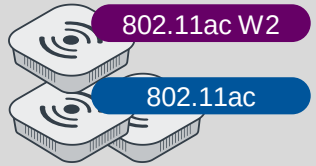
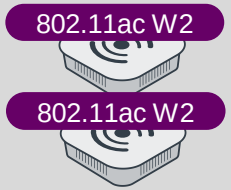
- Controller
- Integrated
- Cloud

FAP-S
Smart

- Controller
- Integrated
- Cloud

FortiAP Family

Fortinet Security Fabric

		Wall Plate	Outdoor	Indoor
4x4:4	Dual Radio			 802.11ac W2 **FAP-421/423E**
3x3:3	Dual Radio			 802.11ac W2 **FAP-321E** 802.11ac **FAP-320/321C**
2x2:2	Triple Radio			 802.11ac W2 **FAP-231E**
	Dual Radio	 802.11ac W2 **FAP-C24JE**	 802.11ac W2 **FAP-224E** 802.11ac W2 **FAP-222E**	 802.11ac W2 **FAP-221/223E**

FortiAP Family Overview

S-Series

		Wall Plate	Outdoor	Indoor
4x4:4	Dual Radio			
3x3:3				
2x2:2				 802.11ac W2 FAP-S221/223E

FortiAP Family Overview

U-Series

			Wall Plate	Outdoor	Indoor
4x4:4	Triple Radio	Resiliency			802.11ax FAP-U431/433F
	Dual Radio			802.11ac W2 FAP-U422EV	802.11ac W2 FAP-U421/423EV
3x3:3					802.11ac W2 FAP-U321/323EV
2x2:2			802.11ac FAP-U24JEV		802.11ac W2 FAP-U221/223EV

Security-driven Networking

Преимущества Secure Access Switching

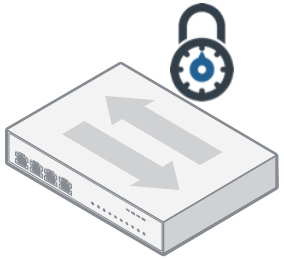
КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

Fortinet Security Fabric

ZERO-TOUCH PROVISIONING
АВТОМАТИЗАЦИЯ УСТАНОВКИ И НАСТРОЙКИ

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

БЕЗОПАСНОЕ И ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

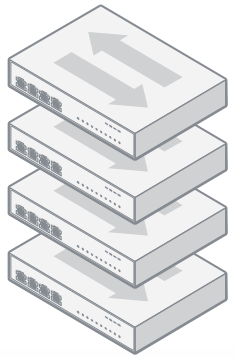


- FortiGate является единой точкой управления
- Централизованное управление VLAN и других функций провижининга

ИНТЕГРАЦИЯ КОММУТАТОРОВ С SECURITY FABRIC

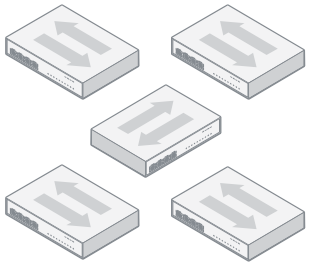
- Обнаружение подключаемых устройств
- Централизованная аутентификация
- Карантин на порту
- Динамическое назначение VLAN
- Логирование процессов

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

Портфолио коммутаторов FortiSwitch

Fortinet Security Fabric

	100 Series	200 Series	400 Series	500 Series	1000/3000 Series
48 ports		FSW-248E-FPOE	FSW-448D/E-FPOE	FSW-548D-FPOE	
		FSW-248D/E-POE	FSW-448D/E-POE		
		FSW-248D	FSW-448D/E	FSW-548D	FSW-1048E
32 ports					FSW-3032E FSW-3032D
24 ports	FSW-124E-FPOE	FSW-224D-FPOE	FSW-424D-FPOE	FSW-524D-FPOE	
	FSW-124E-POE	FSW-224E-POE	FSW-424D-POE		
	FSW-124E	FSW-224E	FSW-424D	FSW-524D	
8 ports	FSW-108E-FPOE				
	FSW-108E-POE				
	FSW-108E				
	+ 2x GE SFP uplink (except FS-124E/-POE/-FPOE)	+ 4x GE SFP uplink	+ 2x10 GE SFP+ uplink	+ 4x 10 GE SFP+ and 2x 40 GE stacking	Data Center Switches

Security-driven Networking

Управление ЛВС и БЛВС уже интегрировано в NGFW !

Простота управления

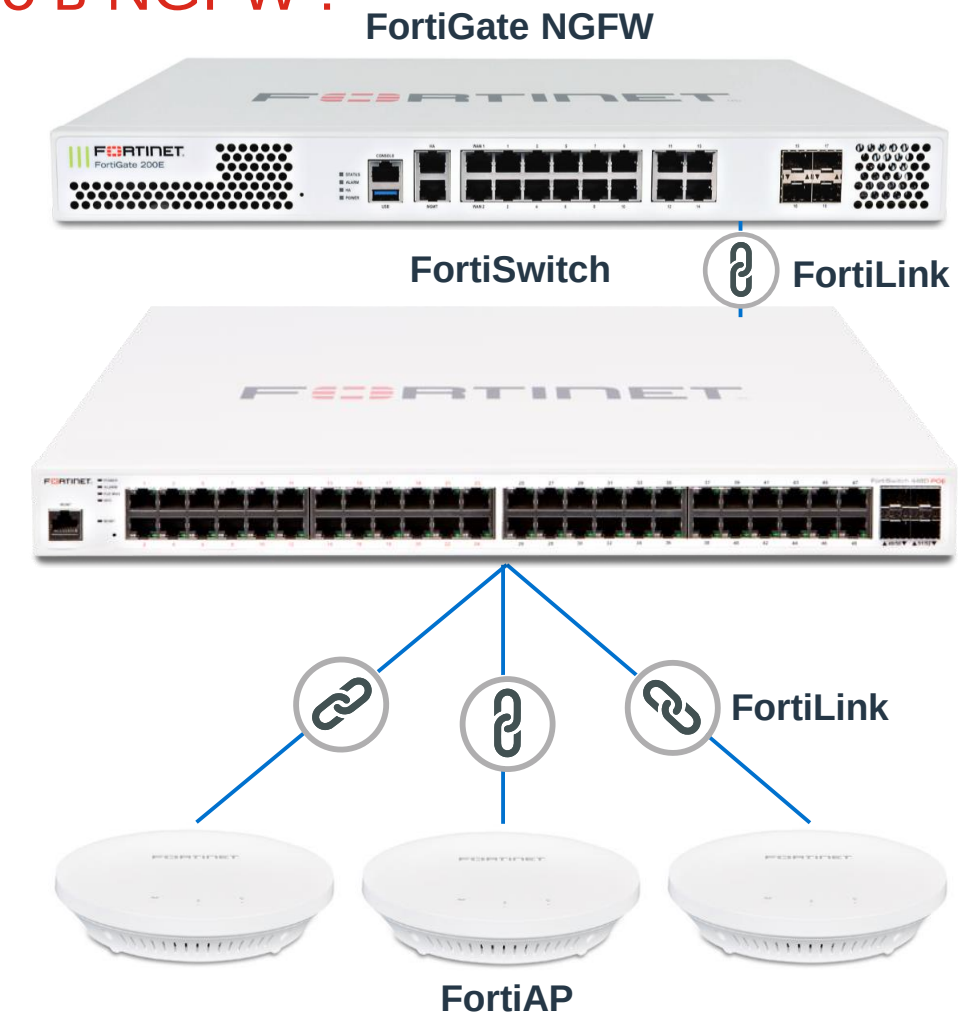
- Автоматическая настройка устройств доступа (FortiSwitch, FortiAP)
- Видимость, обеспечение безопасности и аналитика для проводного и беспроводного доступа
- Гибкая архитектура, может масштабироваться (до 256 коммутаторов FortiSwitch, до 8192 точек доступа FortiAP)

Безопасность

- Порты МСЭ и коммутатора равнозначны с точки зрения безопасности, SSIDs также привязаны к политикам МСЭ
- Глобальные политики безопасности до уровня порта и SSID

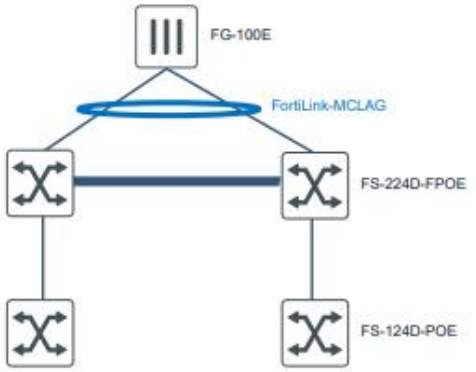
Уменьшение TCO

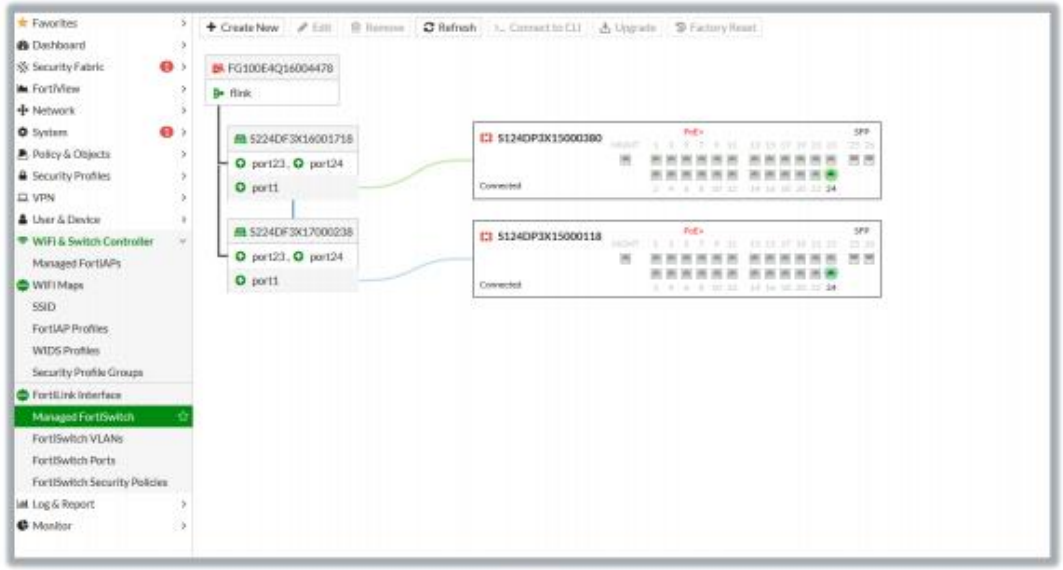
- NGFW FortiGate с поддержкой SD-WAN, Secure Access (FortiSwitch, FortiAP) под управлением FortiManager является основной частью решения SD-Branch



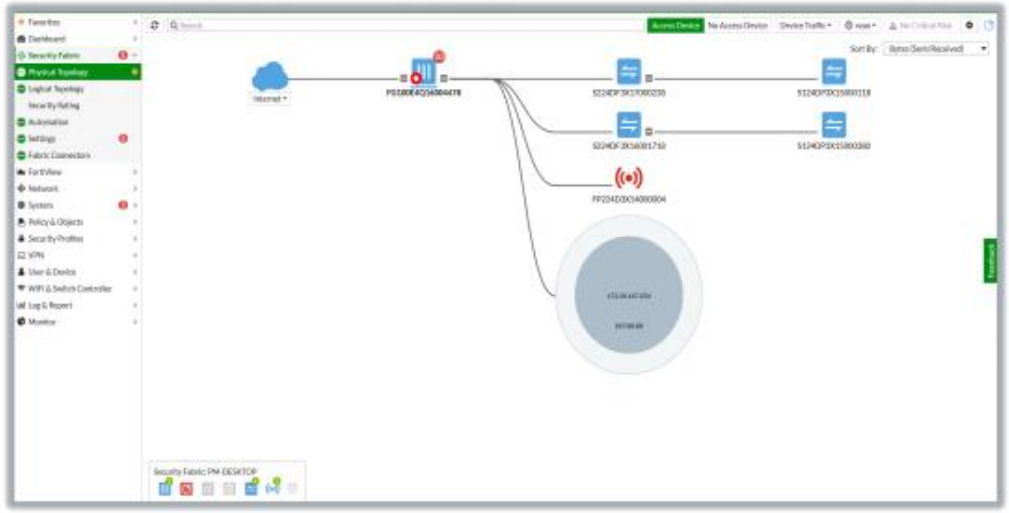
Security-driven Networking

FortiLink – Basic Topology Unit





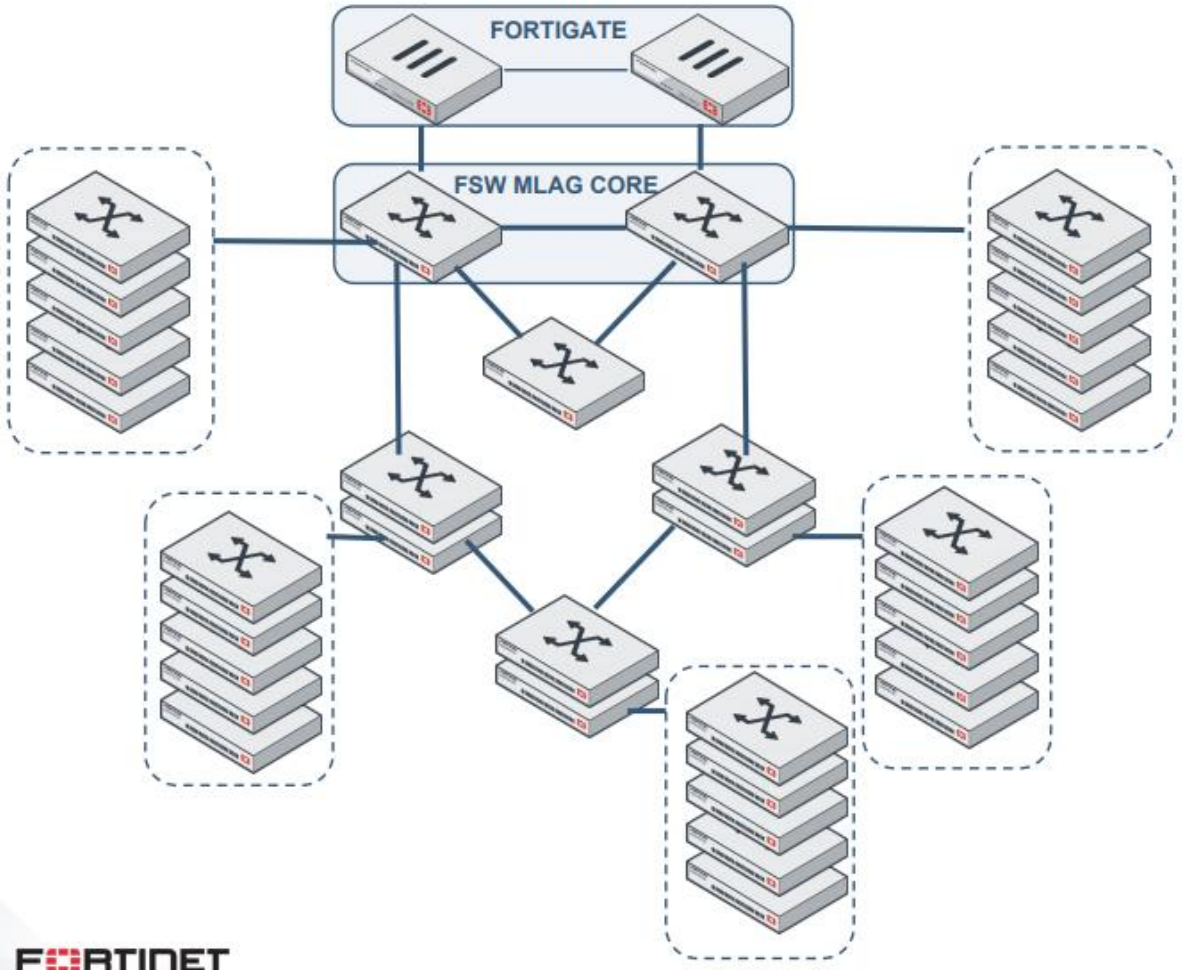
Switch-Controller View



Security Fabric View

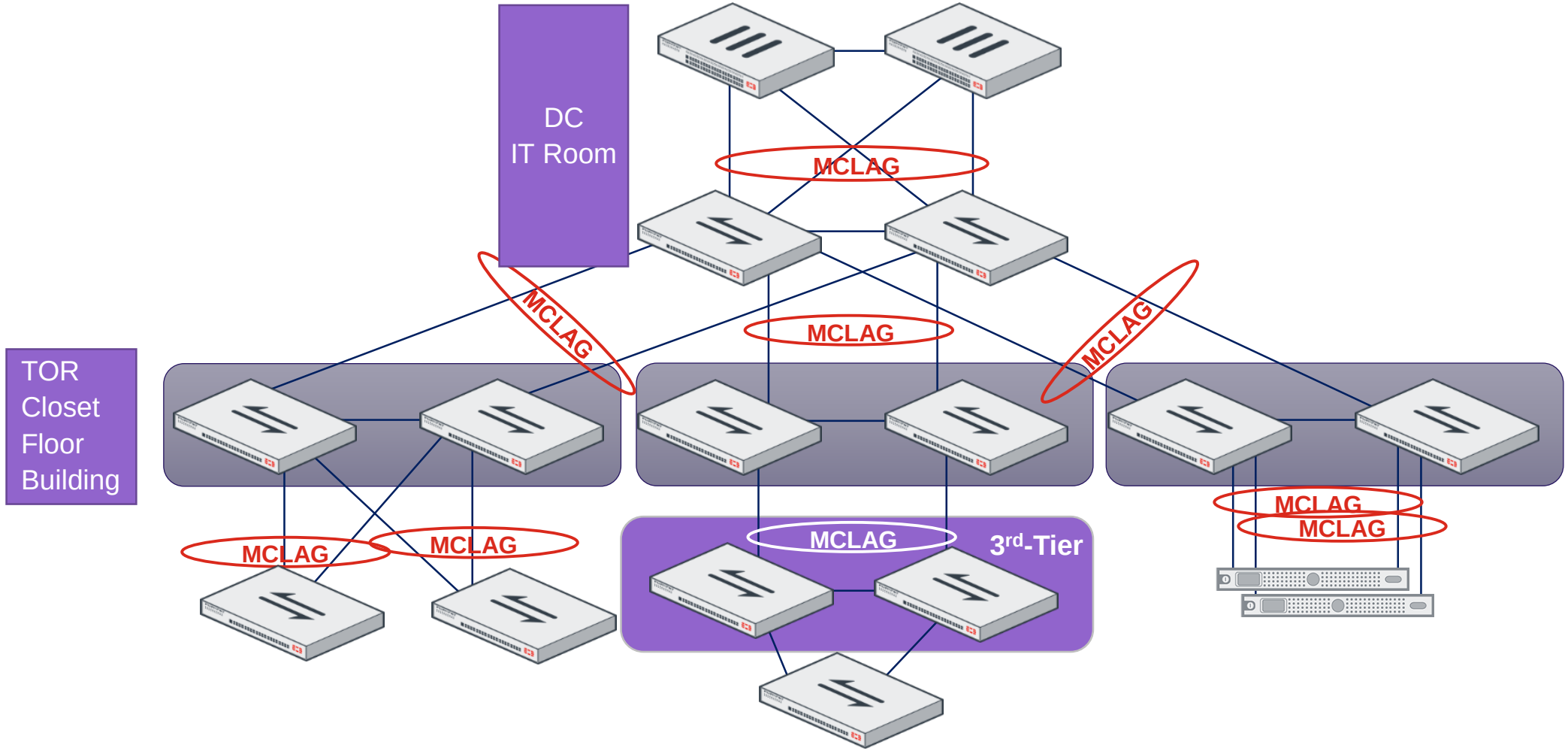
Security-driven Networking

Кампусная сеть FortiSwitch под управлением FortiGate (MCLAG + Stacking)



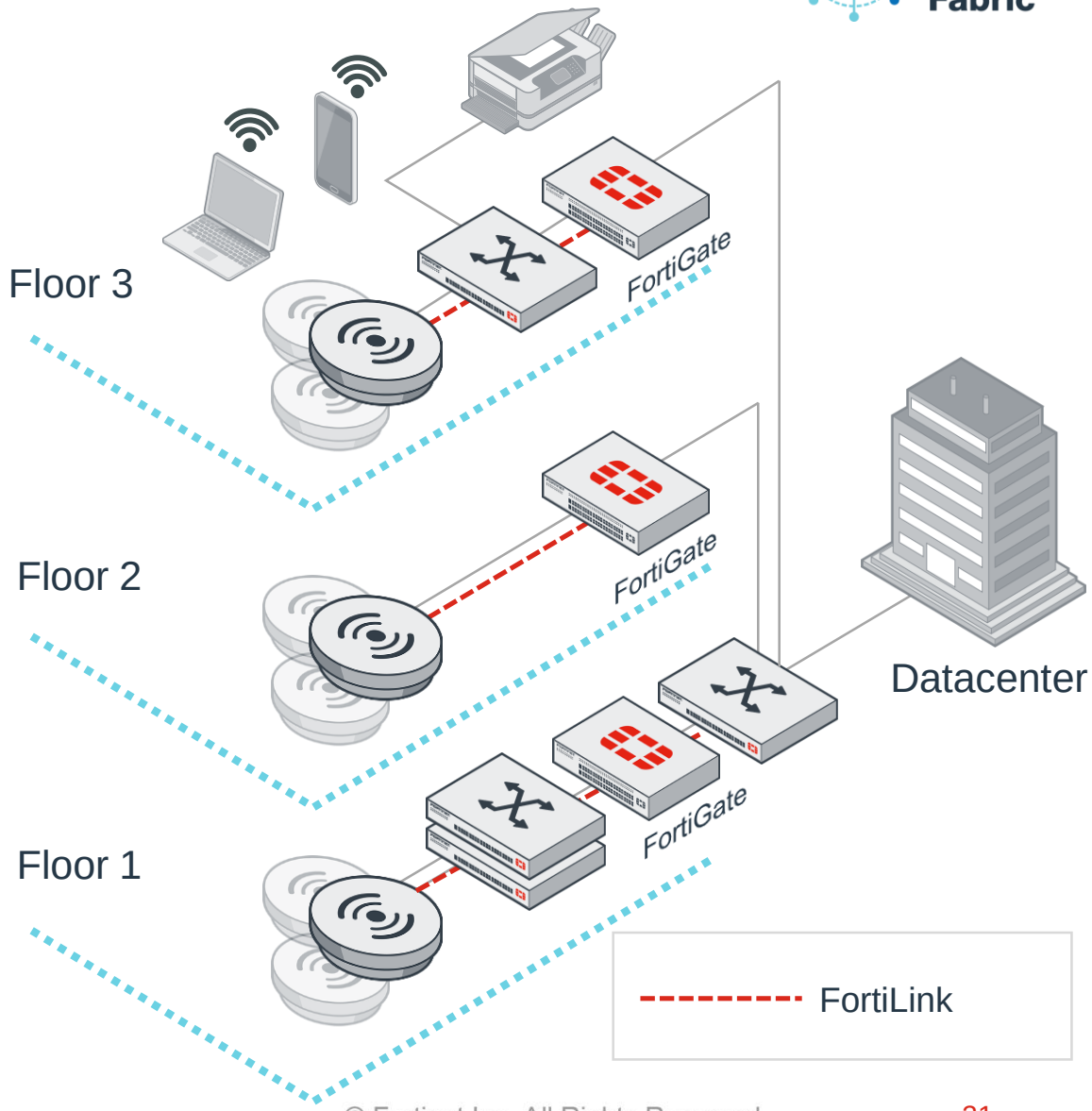
Security-driven Networking

Кампусная сеть FortiSwitch под управлением FortiGate (Multi Tier MCLAG)



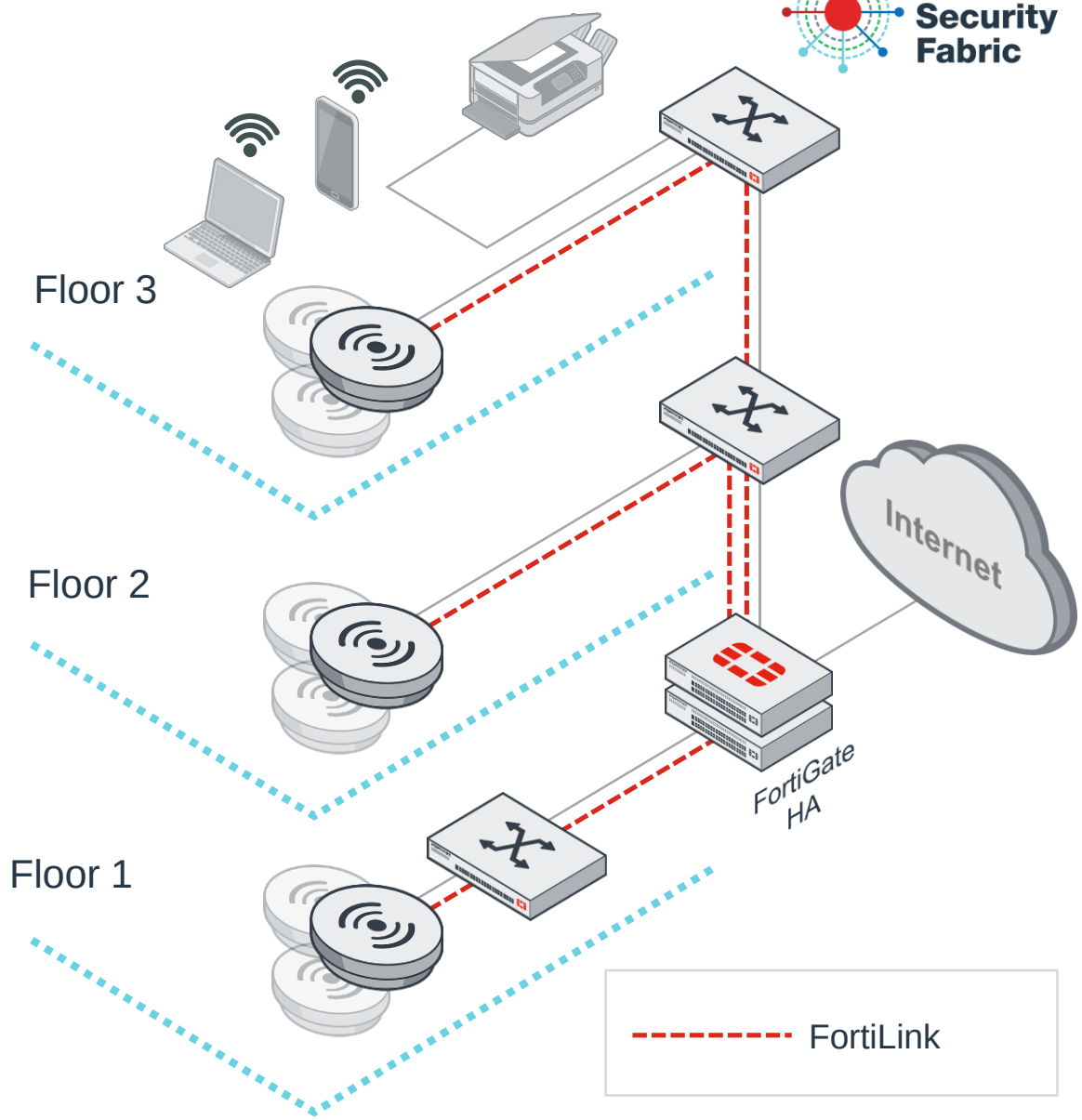
Кампусная сеть

- 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



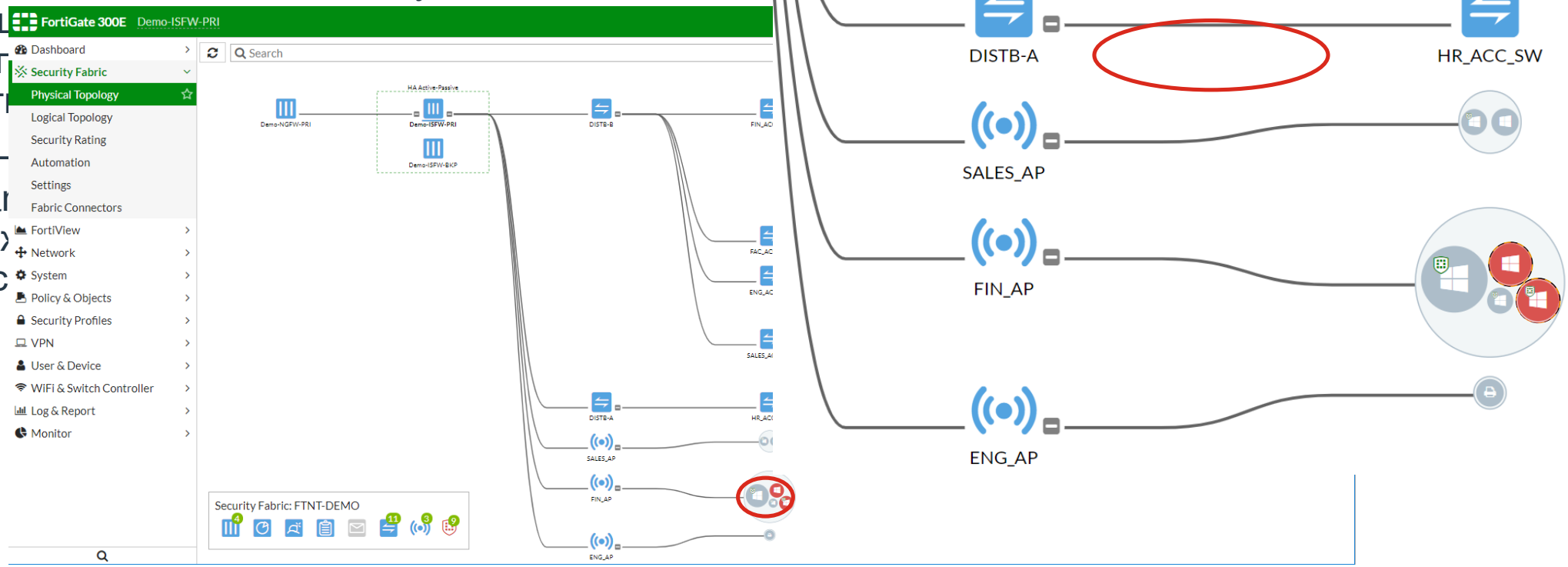
Кампусная сеть

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



Автоматический карантин при обнаружении скомпрометированного устройства

- Security driven networking в действии
  - Устройство определено как скомпрометированное с помощью элементов Security Fabric с помощью FortiGuard IOC
  - FortiAPs или FortiSwitches могут автоматически помещ
    доступ
    по сет
  - MAC H
    Quaran
    возмож
    для ус



Микросегментация в кампусной сети

Fortinet Security Fabric

Что это

- Микро или внутренняя сегментация контролирует коммуникации между устройствами в одном и том же L2 домене
- Межсетевой экран видит все устройства подключенные к нему напрямую и к портам коммутаторов доступа

Как работает

- Трафик направляется на вышестоящее оборудование, которое отвечает за контроль и инспекцию сетевого трафика
- Вышестоящее устройство – это FortiGate

Преимущества

- Улучшение видимости (Видим весь трафик между хостами)
- Улучшение контроля (Контролируем доступ для всего трафика между хостами)
- Улучшение сетевой безопасности (Проводим инспекцию трафика между хостами), контейнеризация скомпрометированного узла на уровне порта доступа

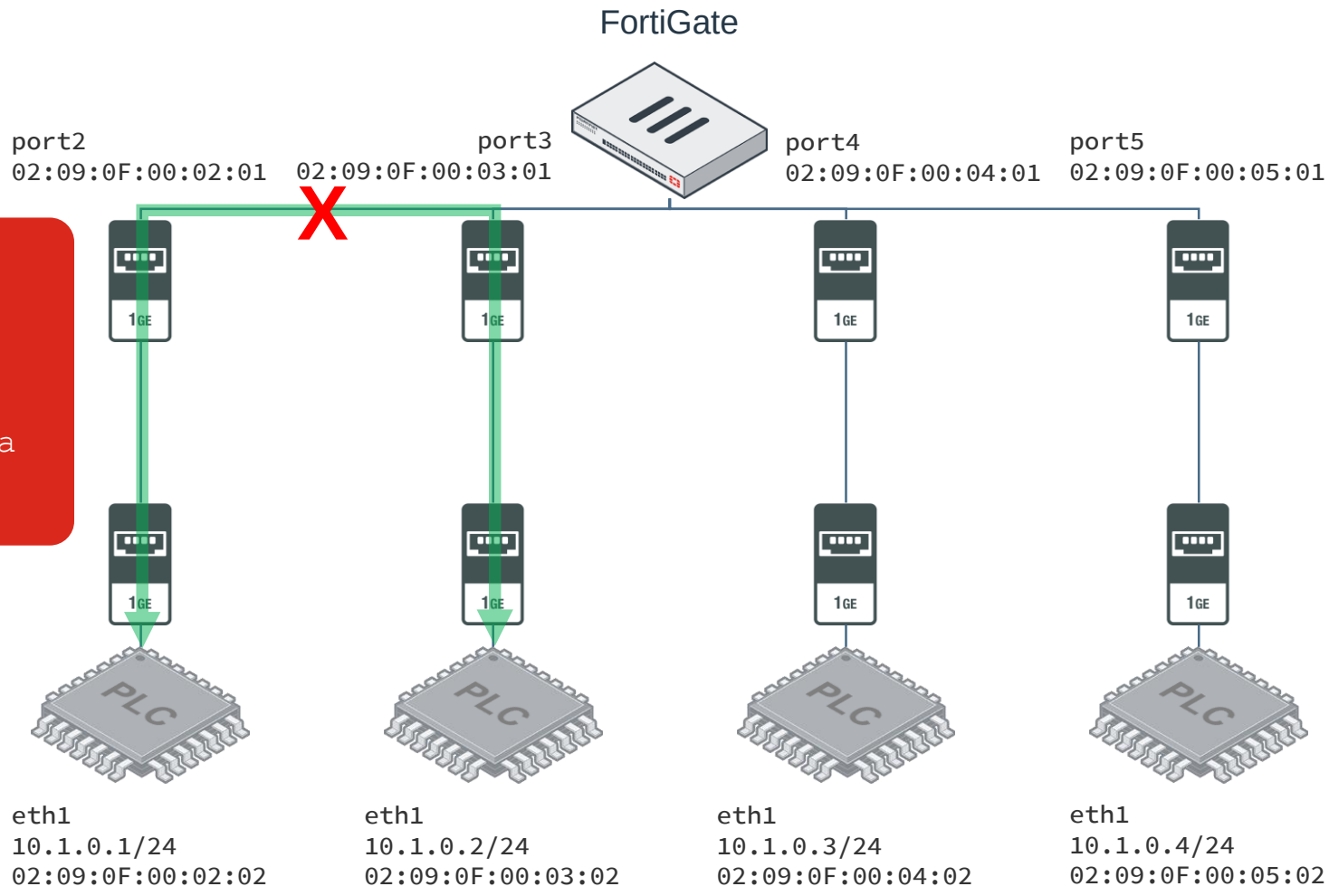
Варианты реализации микросегментации

Products	FortiGate Op. Mode	Micro-Segmentation Feature
Standalone FortiGate	NAT	Intra Switch Policy Virtual Wire Policy
	TP	*Enforced by default* Virtual Wire Policy
Managed FortiSwitch	NAT or TP	Access VLAN

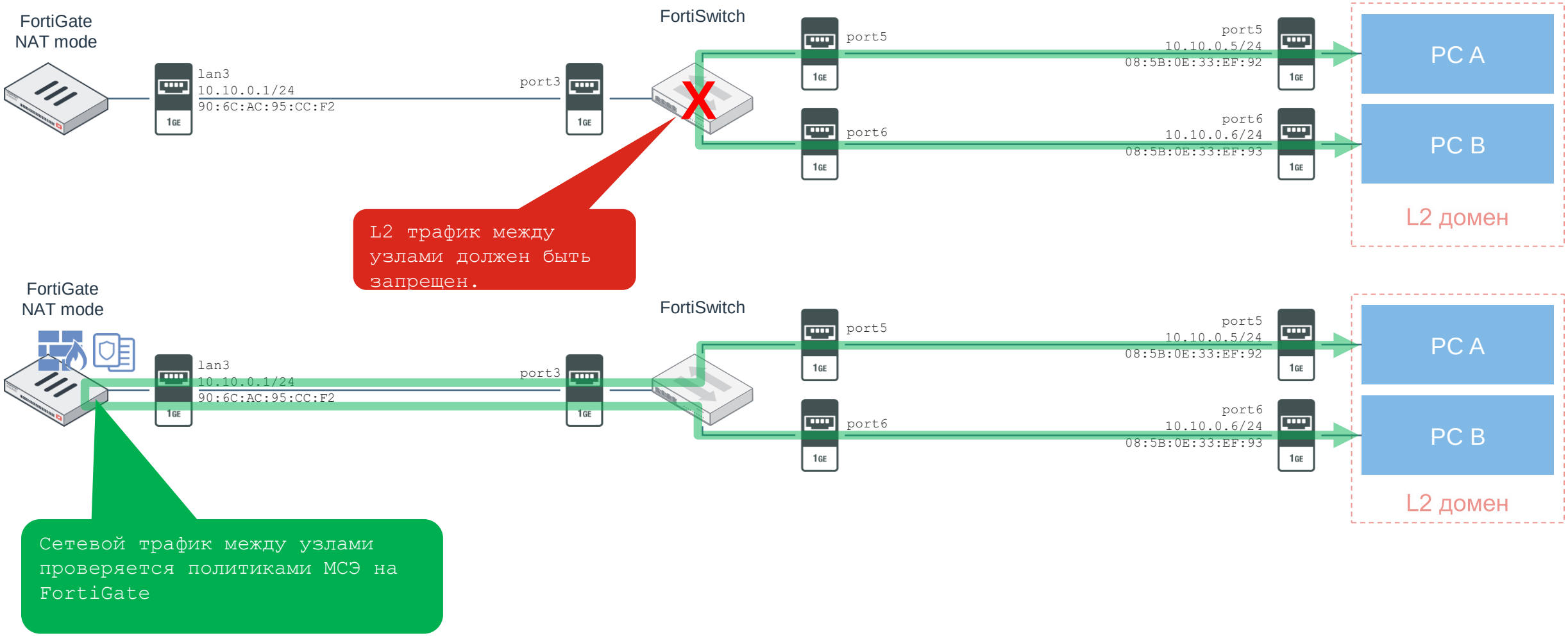
Микросегментация в Transparent Mode

Fortinet Security Fabric

Трафик в L2 домене контролируется явно политиками МСЭ, по умолчанию трафик дропается.
Микросегментация доступна в Transparent Mode by design.



Микросегментация в NAT / Route Mode (+ FortiSwitch)



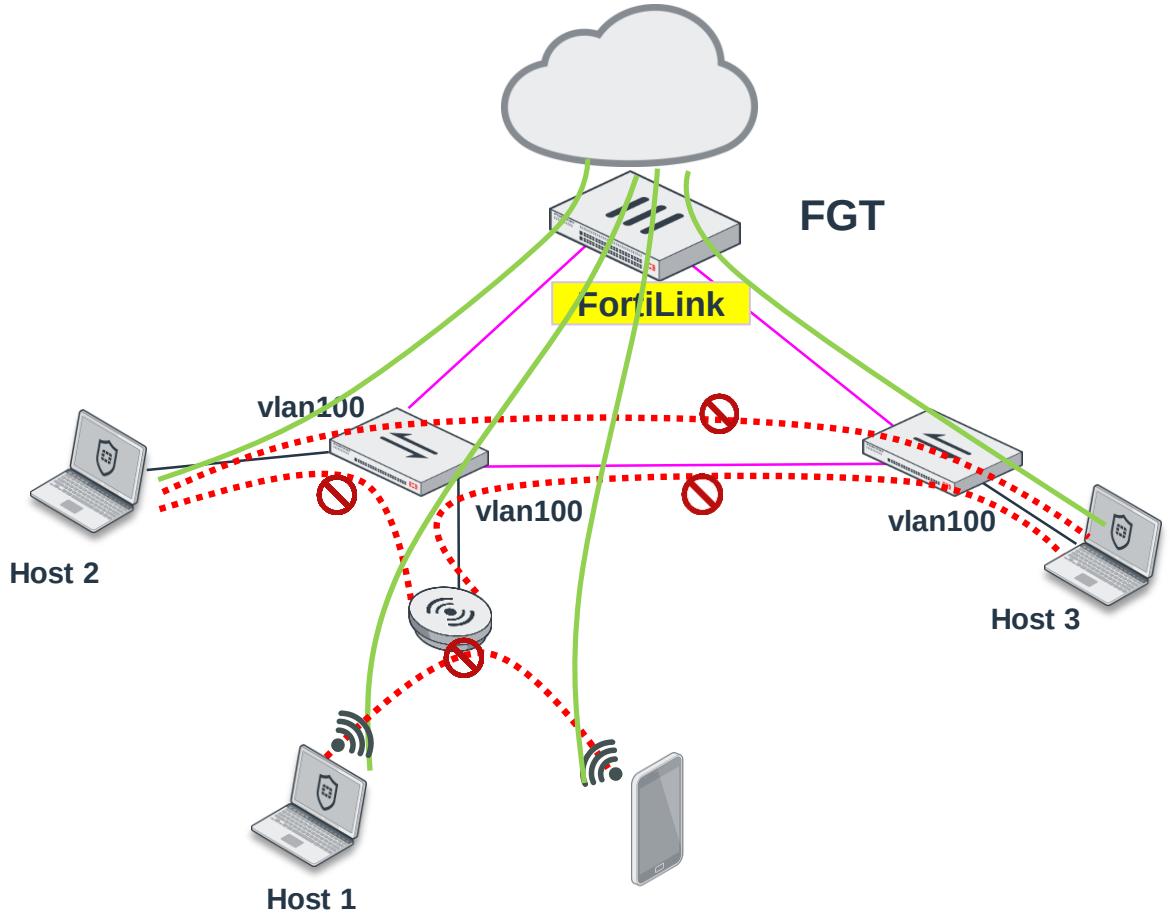
Преимущества микросегментации в пределах широковещательного домена

- Блокируются ***intra-host*** взаимодействия

в одном широковещательном домене

(Access VLAN, Block Intra-SSID)

- **Скомпрометированные хосты не быть использованы для инфицирования и атак на остальные хосты в сети**
- Дополнительная безопасность на уровне доступа:
  - Нет прямой коммуникации между хостами
  - Хосты имеют доступ только к FortiGate
  - FortiGate имеет возможность автоматически поместить в карантин скомпрометированный хост на уровне порта доступа коммутатора либо беспроводной точки доступа



Security-driven Networking

Увеличение количества поддерживаемых FortiSwitch и FortiAP (FOS 6.4)

Max. FortiSwitch	6.2	6.4
FG-200E Series	32	64
FG-300E, 400E, 500E Series	48	72
FG-600E Series	64	96
FortiGate 1100E, 1800F, 2000E, 2200E, 2500E Series	128	196

Max. FortiAP	6.2	6.4
FG-40F Series	10	16
FG-60F Series	30	64
FG-200E Series	128	256
FG-3960E, 3980E	4,096	8,192

Security-driven Networking

Обзор Internal Segmentation Firewall (ISFW)

Security-driven Networking

Вызовы в обеспечении безопасности ЛВС

Факт №1

Растет:

- Количество угроз
- Сложность угроз
- Связанный ущерб

Факт №2

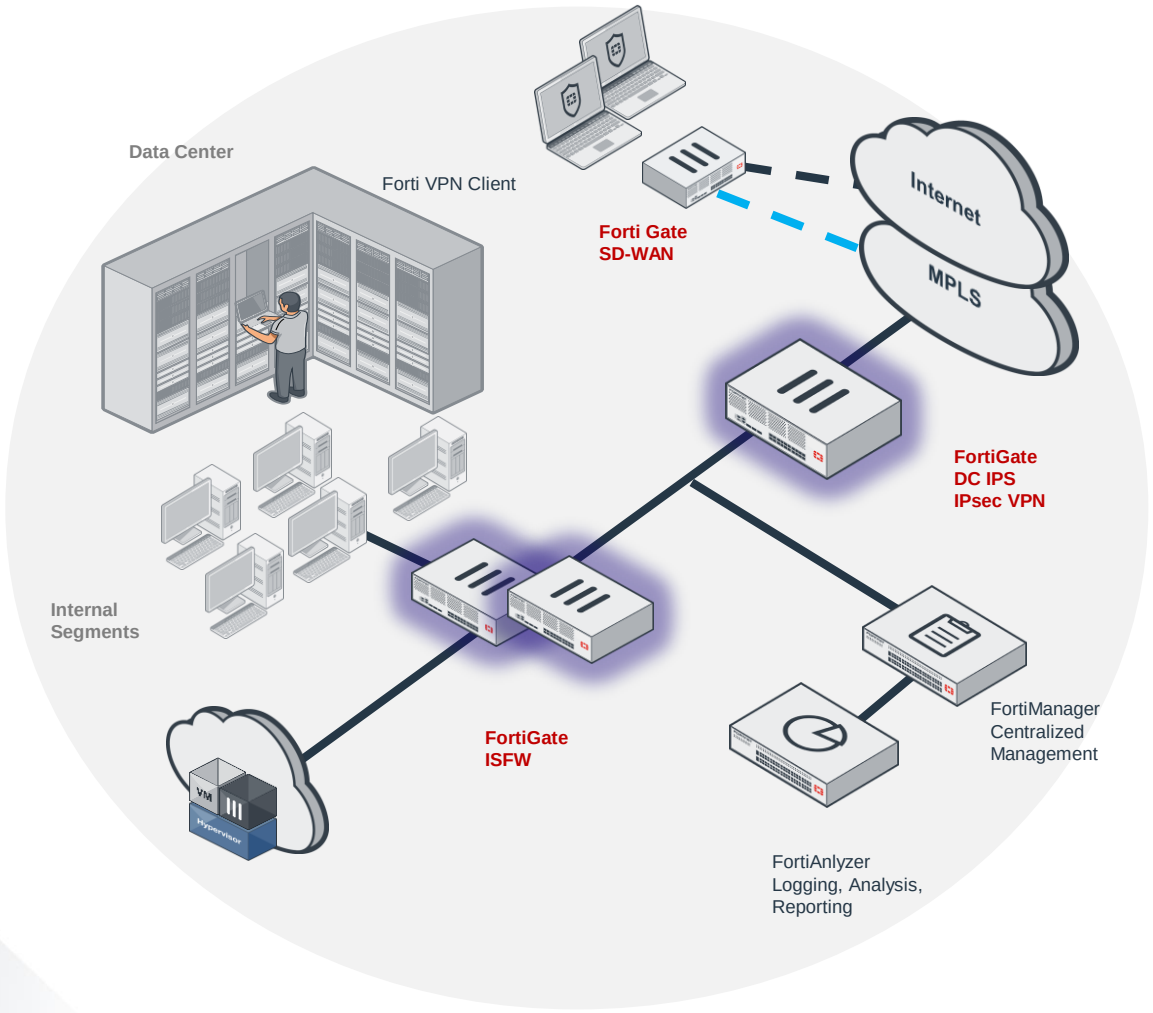
- Плоский дизайн ЛВС и базовые меры защиты (VLAN, ACL L3/L4) ведут к легкости распространения атаки внутри сети
- Отсутствие видимости на уровне приложений, подозрительной активности, угроз и потоков трафика внутри сети

Факт №3

- Сегментации на уровне VLAN недостаточно для защиты от сложных атак
- Сложные атаки успешно преодолевают L3 устройства (маршрутизаторы / коммутаторы), соединяющие VLAN
- Модель сегментации на уровне VLAN имеет ограничения в масштабируемости (до 4K VLAN)

Security-driven Networking

Что это такое и зачем нужен Internal Segmentation Firewall (ISFW) ?

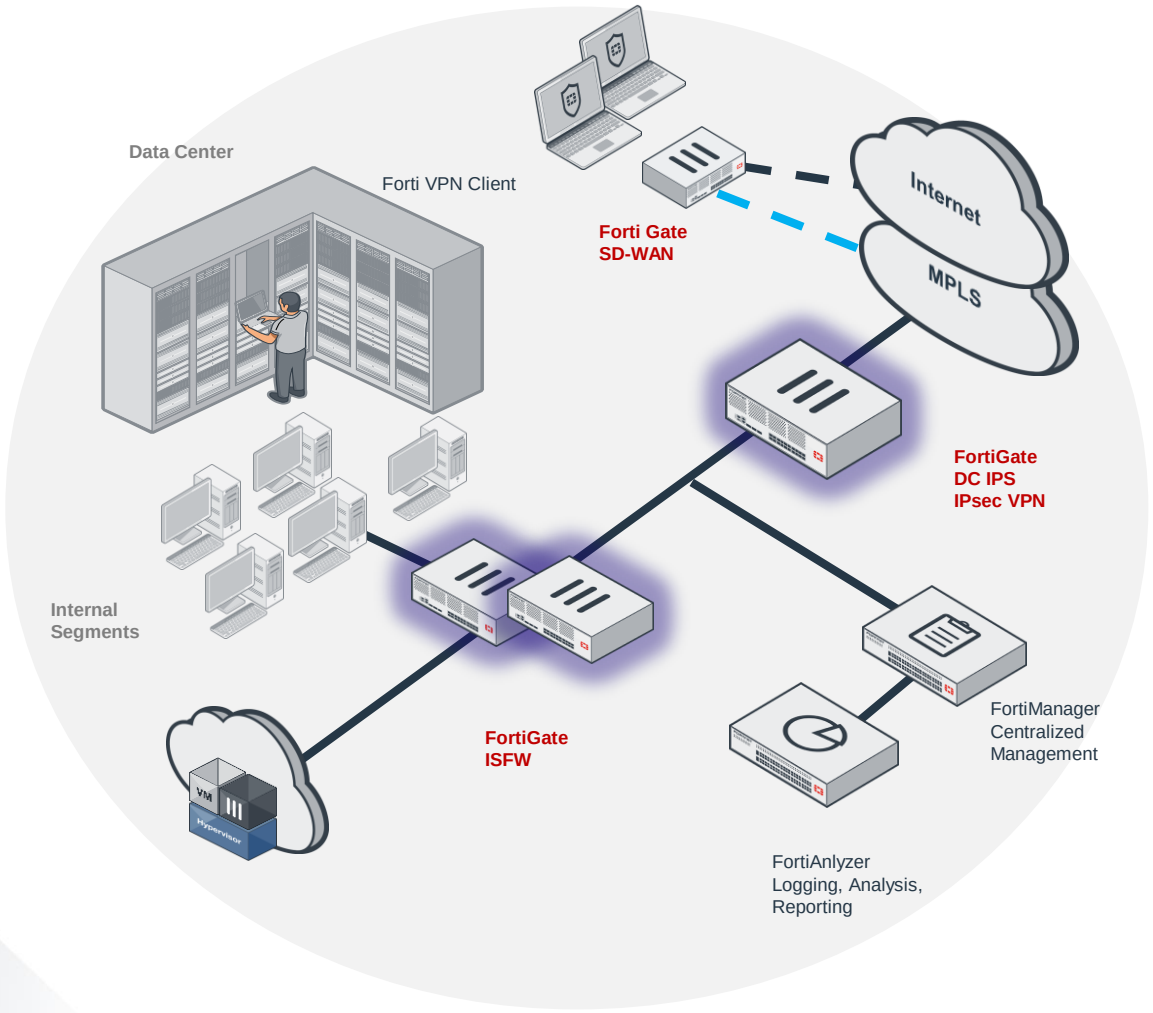


Задачи заказчика

- Внутреннюю ЛВС необходимо защитить от продвинутых угроз
  - Слабый контроль за потоками трафика в ЛВС
  - Горизонтальное перемещение зловредного ПО и сетевых атак
- МСЭ внешнего периметра не работают с ЛВС (скорости в LAN в 10X выше чем в WAN)
  - Дорого
  - Сложно во внедрении
  - Малая портовая емкость

Security-driven Networking

Задачи для Internal Segmentation Firewall (ISFW)



- Контроль доступа к критическим ресурсам как можно ближе к пользователю
  - Идентификация пользователя, устройства и приложения
  - Интеграция с Directory Services (AD, LDAP…)
  - Динамический маппинг пользователя к политике МСЭ

- Барьер для распространения угроз внутри сети
- Ограничение потенциального ущерба внутри сети
- Улучшение видимости угроз, обнаружение и ликвидация брешей в безопасности

Сравнение режимов развертывания NGFW (ISFW с NGFW, DCFW, DEFW, CCFW)

Режим развертывания	ISFW	NGFW	DCFW	DEFW	CCFW
Назначение	Видимость и защита для внутренних сегментов ЛВС	Видимость и защита от внешних угроз	Высокая производительность, низкая задержка МСЭ	Видимость и защита от внешних угроз и активности пользователей	Сетевая безопасность для поставщиков услуг (Service Providers)
Расположение	Уровень доступа	Внешний периметр	Уровень ядра / Шлюз ЦОД	Внешний периметр	Варьируется
Режим работы	Прозрачный режим	NAT/Маршрутизатор	NAT/Маршрутизатор	NAT/Маршрутизатор	NAT/Маршрутизатор
Требования Hardware	Высокая плотность портов; Встроенная коммутация	GE and 10GE порты	GE/10 GE/40GE/100GE - высокая плотность портов, аппаратная акселерация	Высокая плотность GE портов, встроенные возможности беспроводного доступа и PoE	GE/10 GE/40GE/100GE - высокая плотность портов, аппаратная акселерация
Компоненты безопасности	(User-based) МСЭ, IPS, AV / ATP, Application Control	(User-based) МСЭ, VPN, IPS, AV / ATP, Application Control, Web Filtering, SSL Inspection и т.д.	МСЭ, IPS, DDoS protection	(User-based) МСЭ, VPN, IPS, AV / ATP, Application Control, Web Filtering. SSL Inspection и т.д.	S/Gi МСЭ, CGN, LTE & mobile security
Другие характеристики	Быстрое развертывание, минимум действий для конфигурации	Интеграция с Advanced Threat Protection (Sandbox)	Высокая доступность	Широкие возможности подключения к WAN (например 3G/4G LTE)	Высокая доступность

Security-driven Networking

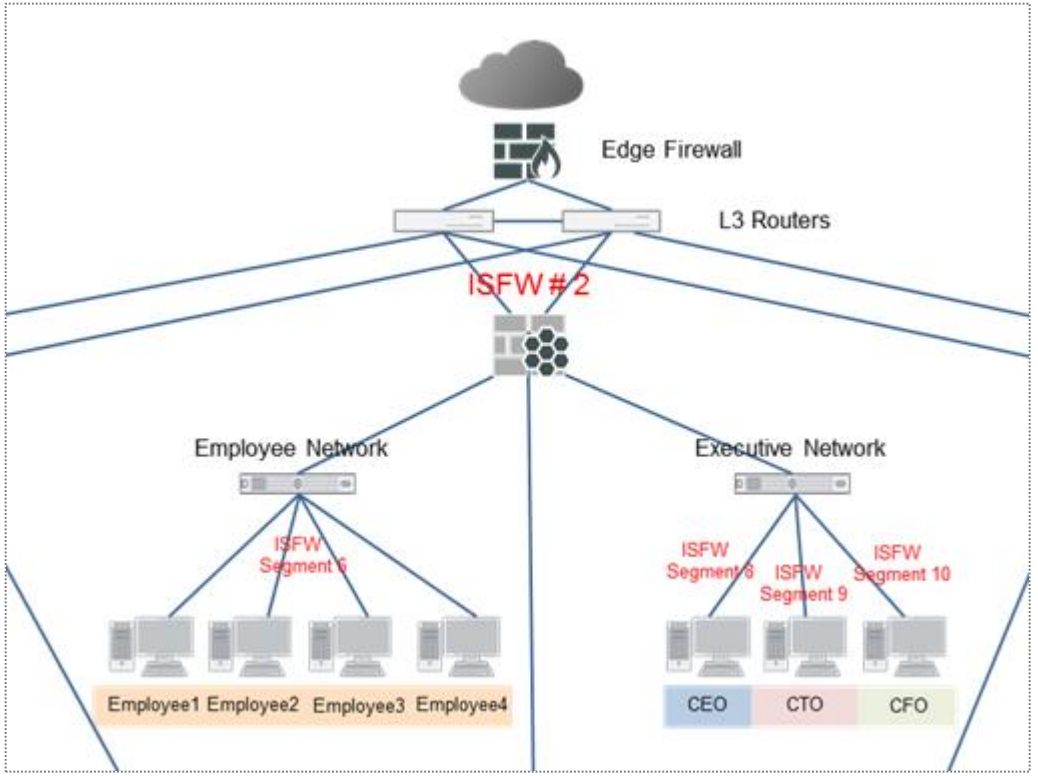
Преимущества ISFW FortiGate

- **Сетевая сегментация End to end**
- **Гранулярные возможности контроля и видимости**
  - Интеграция с Security Fabric для защиты в реальном времени и восстановления внутри сети
- **Многослойная защита**
  - Лидирующие возможности защиты на множественных уровнях:

    NGFW, IPS, ATP (sandboxing), anti-malware
  - North-South and East-West protection
- **Fortinet Security Processors**
  - Сердце NGFW с поддержкой аппаратной акселерации обработки сетевого трафика и инспекции
  - Работа в прозрачном режиме с ультранизким уровнем задержки межсетевого экранирования

ISFW

Предназначение ISFW в разделении и защите внутренних сегментов ЛВС в кампусе, ЦОД, HQ

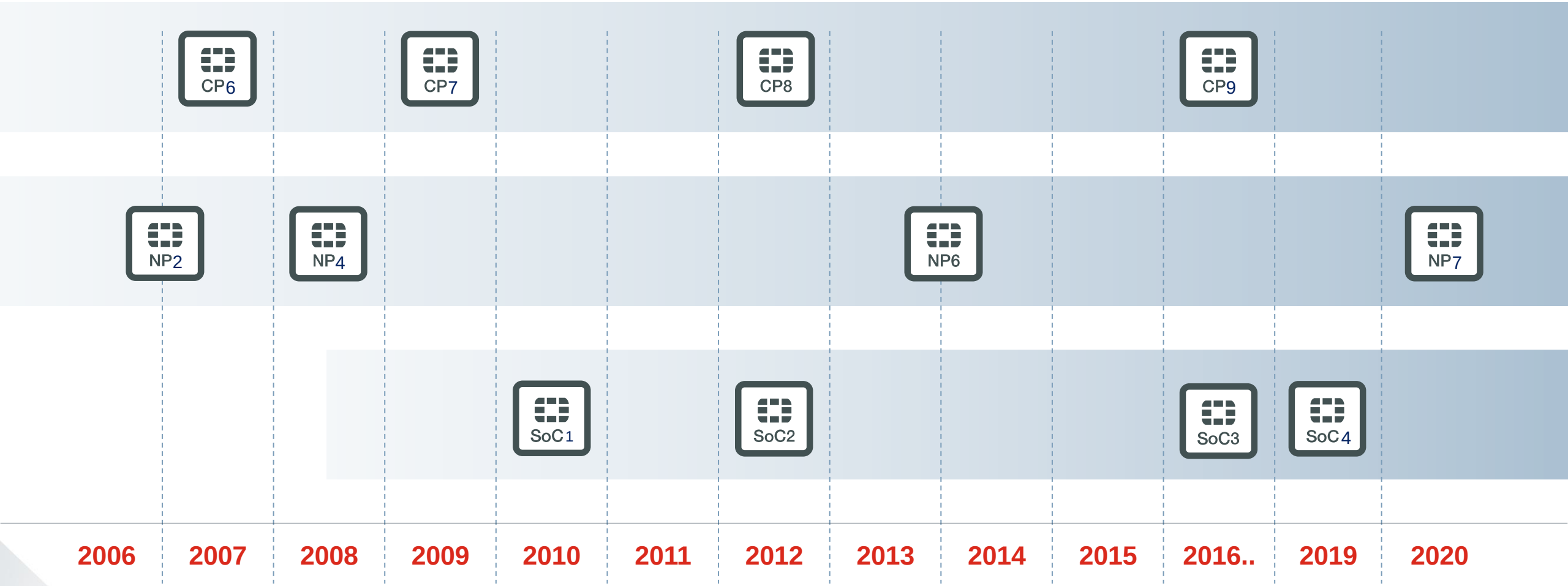


Security-driven Networking

Возможности FortiGate в роли ISFW для кампусных сетей

- User / Device / Application Aware политики межсетевого экранирования
- Интеграция с RADIUS / LDAP / AD для аутентификации и управления
- Полный комплект сервисов безопасности для ISFW – AV, IPS, Application Control
- Аппаратная акселерация обработки сетевого трафика и инспекции для обеспечения высокой производительности и низких задержек важных для ISFW
- Высокая плотность портов 10GE / 25GE / 40GE /100 GE для подключения множества коммутаторов доступа
- Широкий выбор устройств для сетей любого размера
- Масштабируемые возможности управления с помощью FortiManager / FortiAnalyzer, FortiAuthenticator. Простая интеграция в Fortinet Security Fabric

Эволюция процессоров
Fortinet Security Processing Units (SPU)

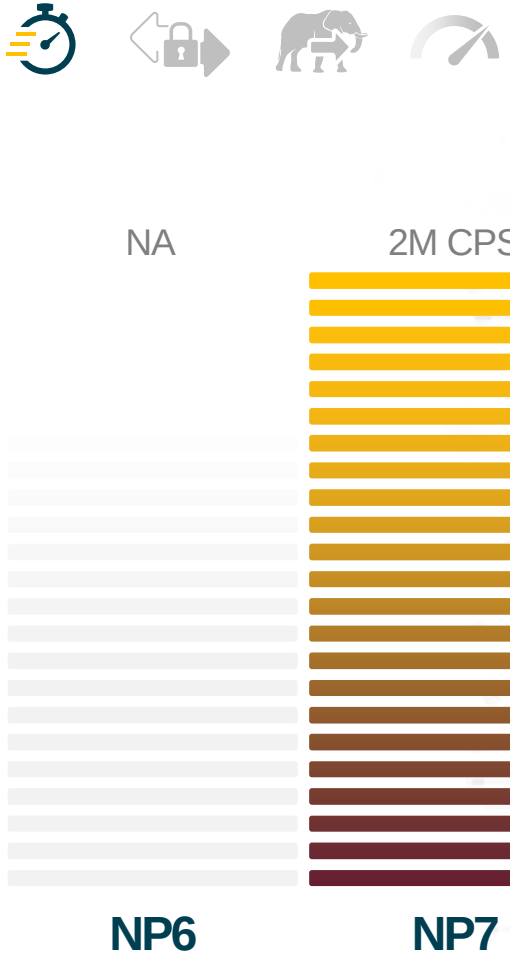


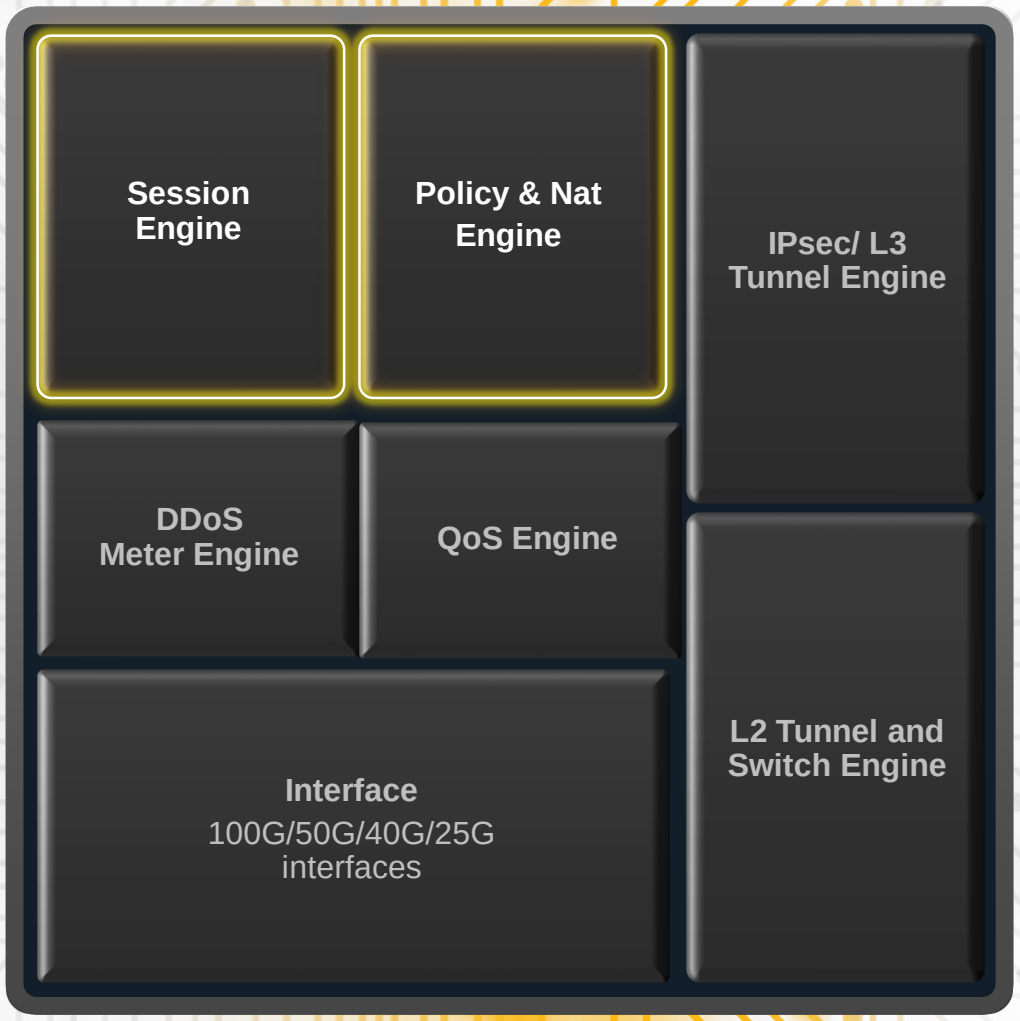
NP7

Security
Processing
Unit

NP7 - Security Processing Unit

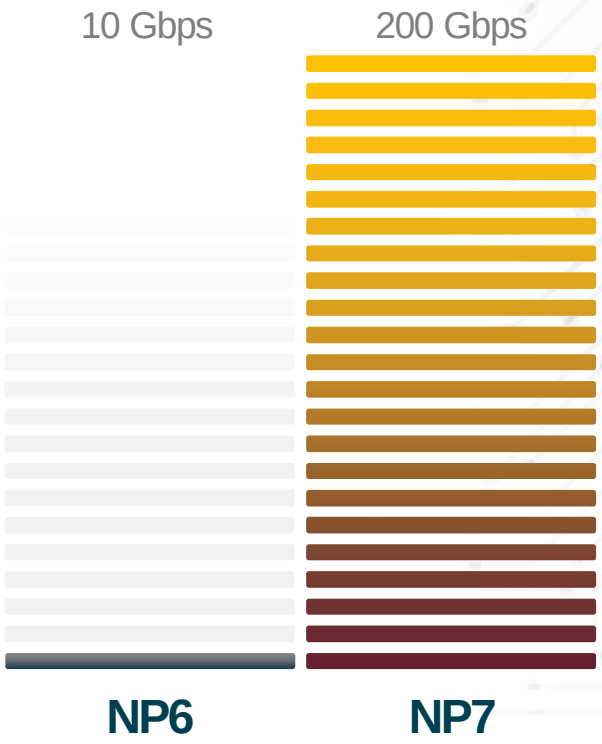
Accelerated Session Setup and Logging

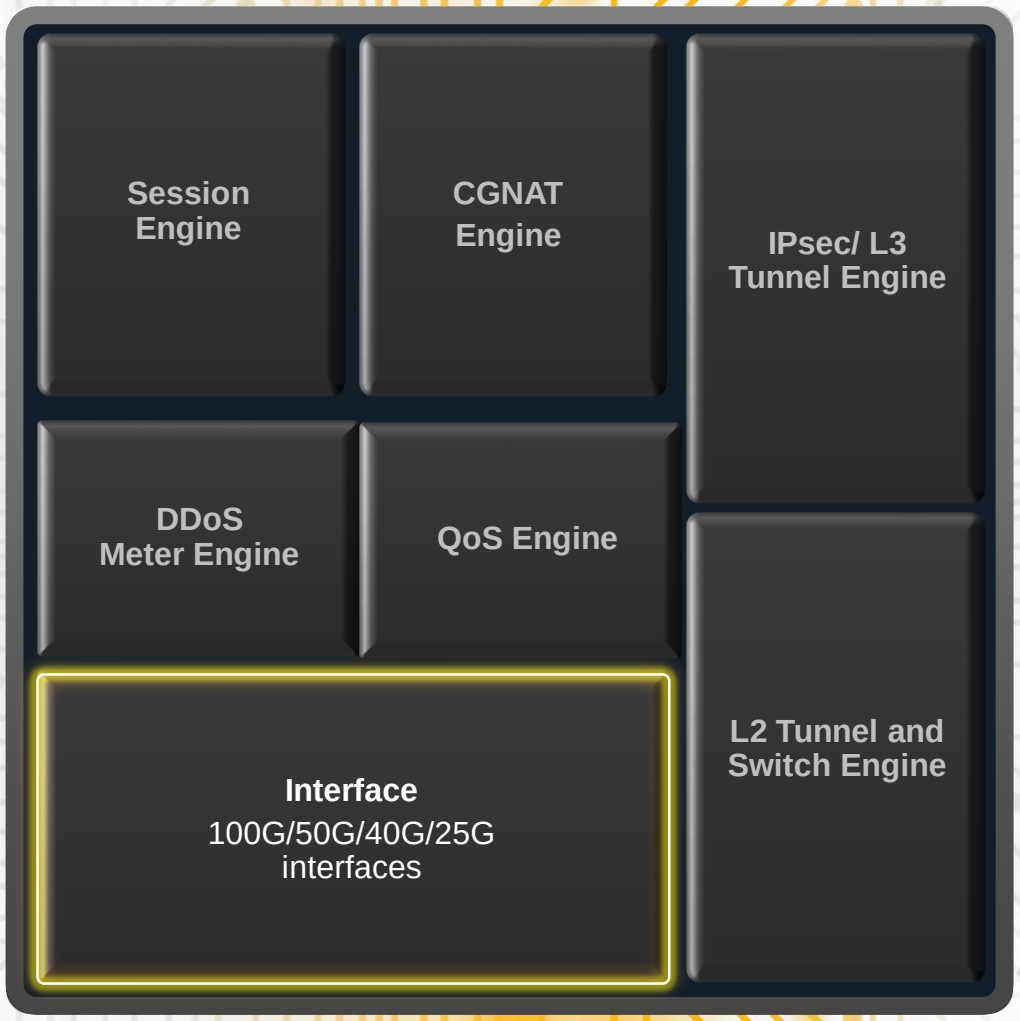




NP7 - Security Processing Unit

Elephant Flow Acceleration

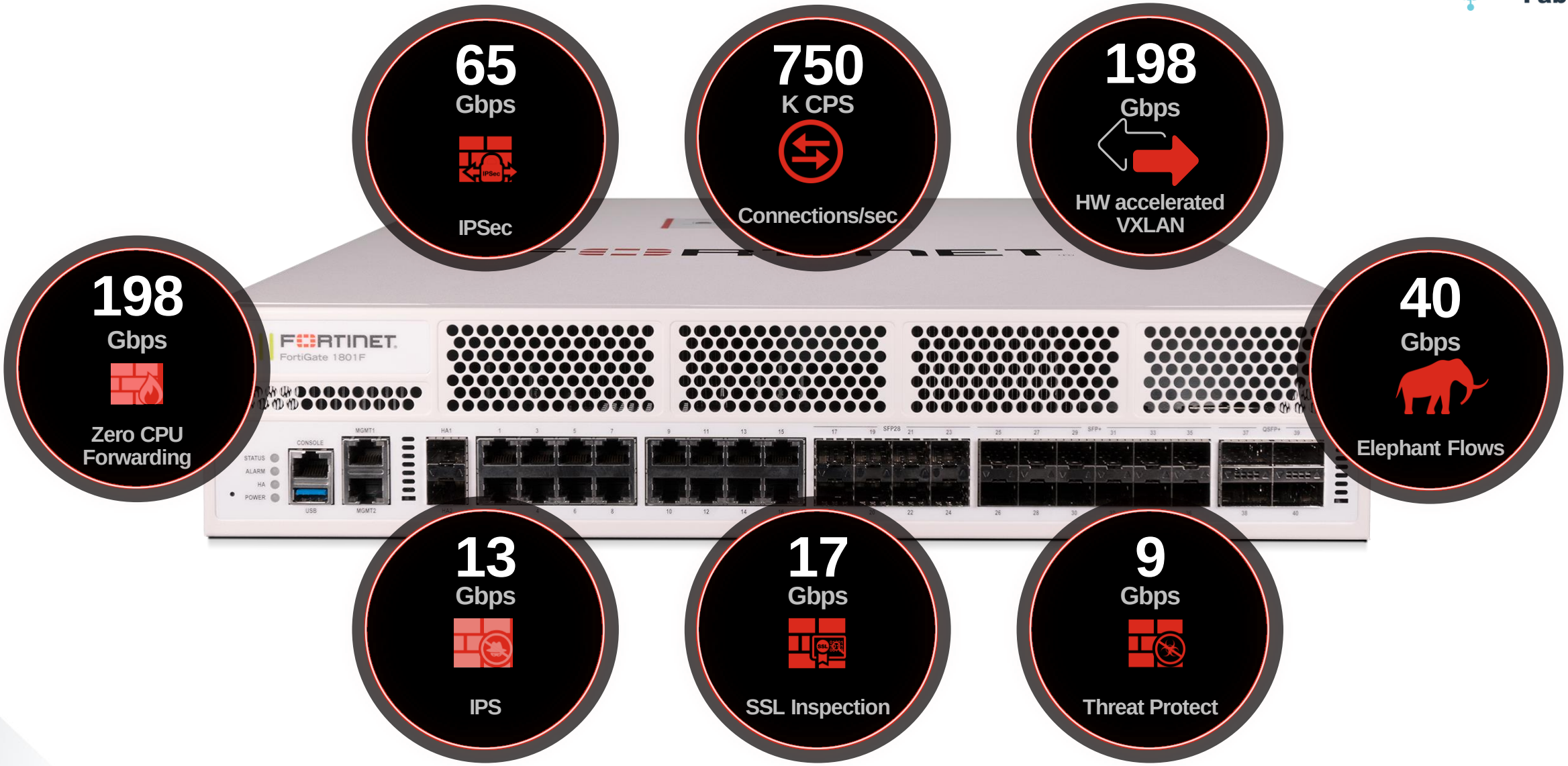




FortiGate 1800F

Пример NGFW / ISFW на SPU FortiASIC-NP7 !

Fortinet Security Fabric



Zero-Trust
Network Access

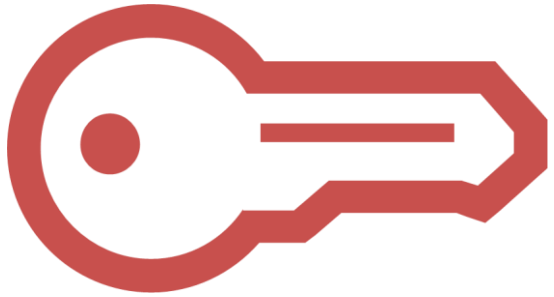
Масштабируемая идентификация и аутентификация пользователей и устройств в ЛВС. Обеспечение контроля доступа в ЛВС.

Zero-Trust Network Access

Централизованное управление аутентификацией и доступом

FortiAuthenticator

Identity and Access Management



Централизованная аутентификация

- Единая точка Identity management для FortiGates, Switches, Wireless, and Cloud улучшает управление безопасностью и сокращает время для решения задач аутентификации.

Упрощение процедуры входа (SSO)

- Функциональность Single Sign-on для локальных и облачных сервисов упрощает жизнь пользователям, в то же время улучшает безопасность

Централизация двухфакторной аутентификации (2FA)

- Управление токенами для множества FortiGate или других сетевых устройств доступа

Управление гостевым доступом для пользователей и устройств

Zero-Trust Network Access

Двухфакторная аутентификация для кампусных сетей и сетей филиалов

Fortinet Security Fabric

FortiToken

Identity and Access Management

Множество вариантов использования токенов для разных сценариев использования

- Приложение FortiToken Mobile app и программный токен упрощает использование 2FA для пользователя до уровня “click to accept”
- Аппаратные токены для любых случаев использования
- Простые варианты развертывания
- Постоянное лицензирование, отсутствие будущих затрат на локально управляемые FortiToken.

Zero-Trust Network Access

Облачный сервис управления токенами

FortiToken Cloud

Identity and Access Management

Two-Factor that's Easy to Manage and Easy to Use

Все что нужно для 2FA в окружении FortiGate

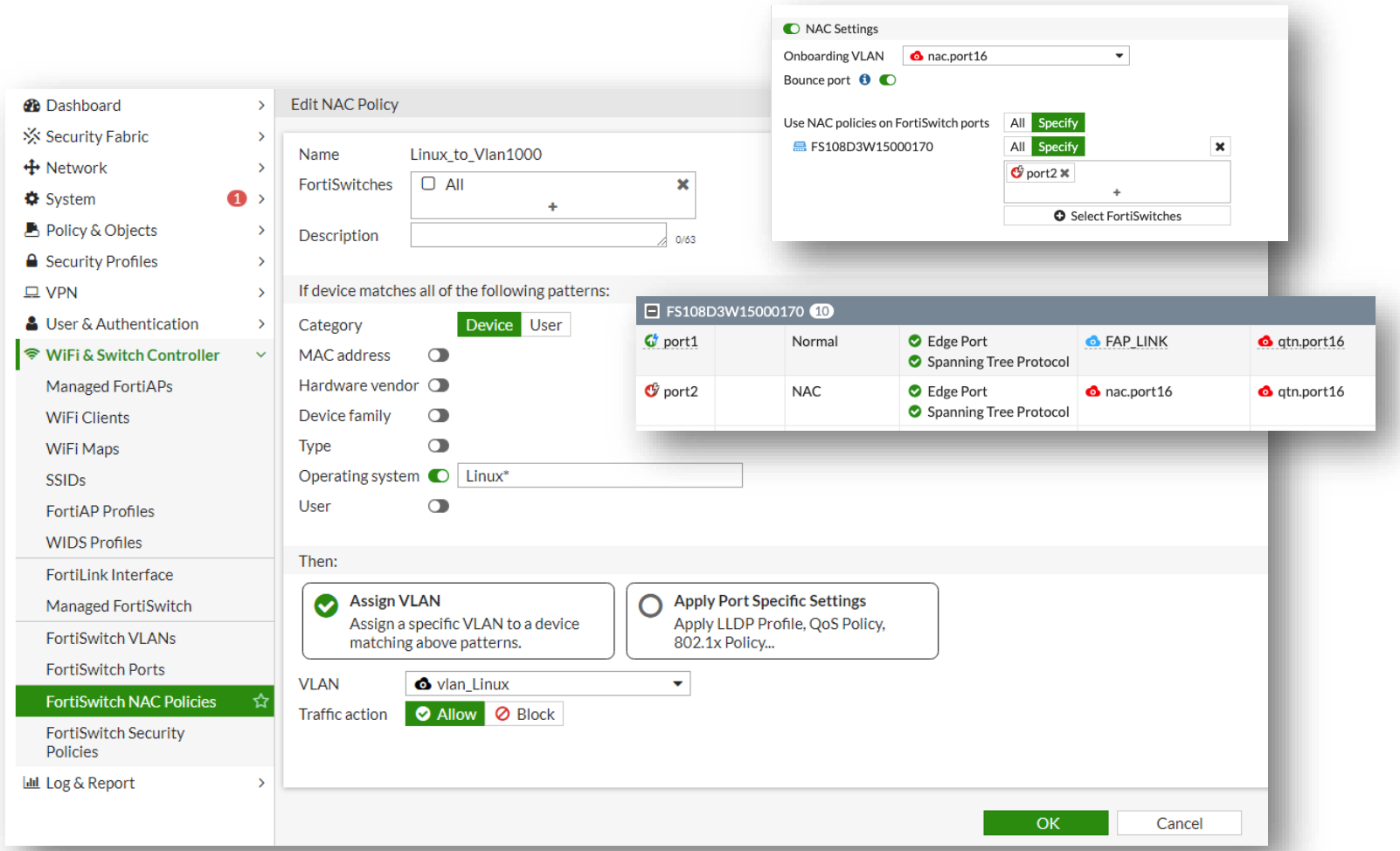
Ключевые возможности:

- Управление 2FA из облака (провиженинг и отзыв токенов)
- Приложение FortiToken Mobile app и программный токен упрощает использование 2FA для пользователя до уровня "click to accept"
- Не требуется дополнительное оборудования и ПО в ЛВС
- Легко масштабируется по мере роста.

Zero-Trust Network Access

FortiSwitch NAC – встроенный NAC в FortiGate

- Базовые средства контроля доступа в ЛВС (NAC) на FortiSwitch уже встроены в FortiGate (FortiSwitch NAC, **FortiOS 6.4**).
- Функциональность не лицензируется
- Доступ в ЛВС осуществляется согласно политикам NAC (NAC policy) в FortiOS
- Политики NAC для групп пользователей или устройств
- Настройки FortiSwitch NAC должны быть проведены до настройки политик NAC:
  - Ручной вариант конфигурации
  - С помощью помощника (NAC Wizard)



Zero-Trust Network Access

Решение **FortiNAC** для кампусных и филиальных сетей

Fortinet Security Fabric

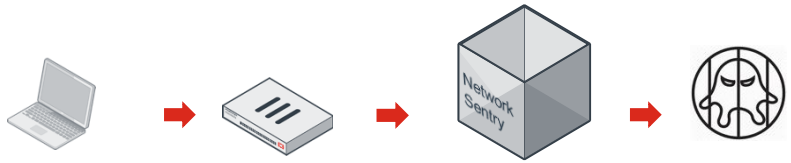
Обеспечивает видимость пользователей и устройств в сети и автоматизирует ответную реакцию на возникающие угрозы

- Идентификация и профайлинг устройств
- Упрощение гостевого доступа с помощью портала самостоятельной регистрации в сети
- Постоянное управление рисками
- Микросегментация конечных узлов
- Автоматическое реагирование на определенные риски
- Оркестрация для устройств сторонних производителей

Профилирование для всех устройств

1. Printer connected to network
2. MAC notification trap triggers FortiNAC
3. FortiNAC Profiles device as printer
4. FortiNAC Informs Fabric to allow Printer-type access to network

Изоляция угроз в сети на уровне доступа / устройства



1. User brings infected laptop to work
2. FGT sends event to FortiNAC
3. FortiNAC quarantines the laptop at access layer
4. Virus contained at switch node

FORTINET

Fabric Management Center

Централизованное управление, аналитика и отчетность

Fabric Management Center

Компоненты Fabric Management Center

FortiManager

Упрощение развертывания

Централизация управления

FortiAnalyzer

Аналитика Security Fabric

Отчетность для соответствия требованиям

Сетевая автоматизация

FortiManager & FortiAnalyzer

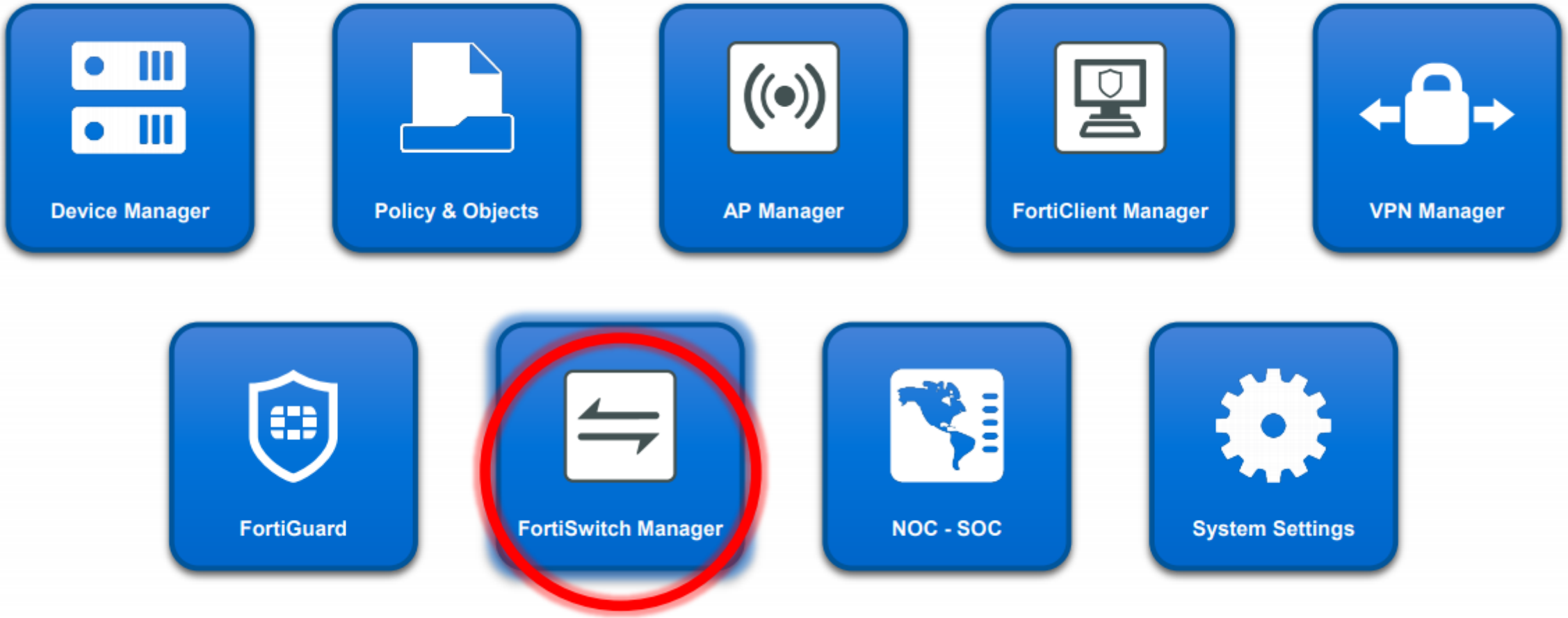
25K+ Customers

Gartner® Firewall & SD-WAN Magic Quadrants

Appliance | Virtual Machine | Cloud | Security-as-a-Service

Fabric Management Center

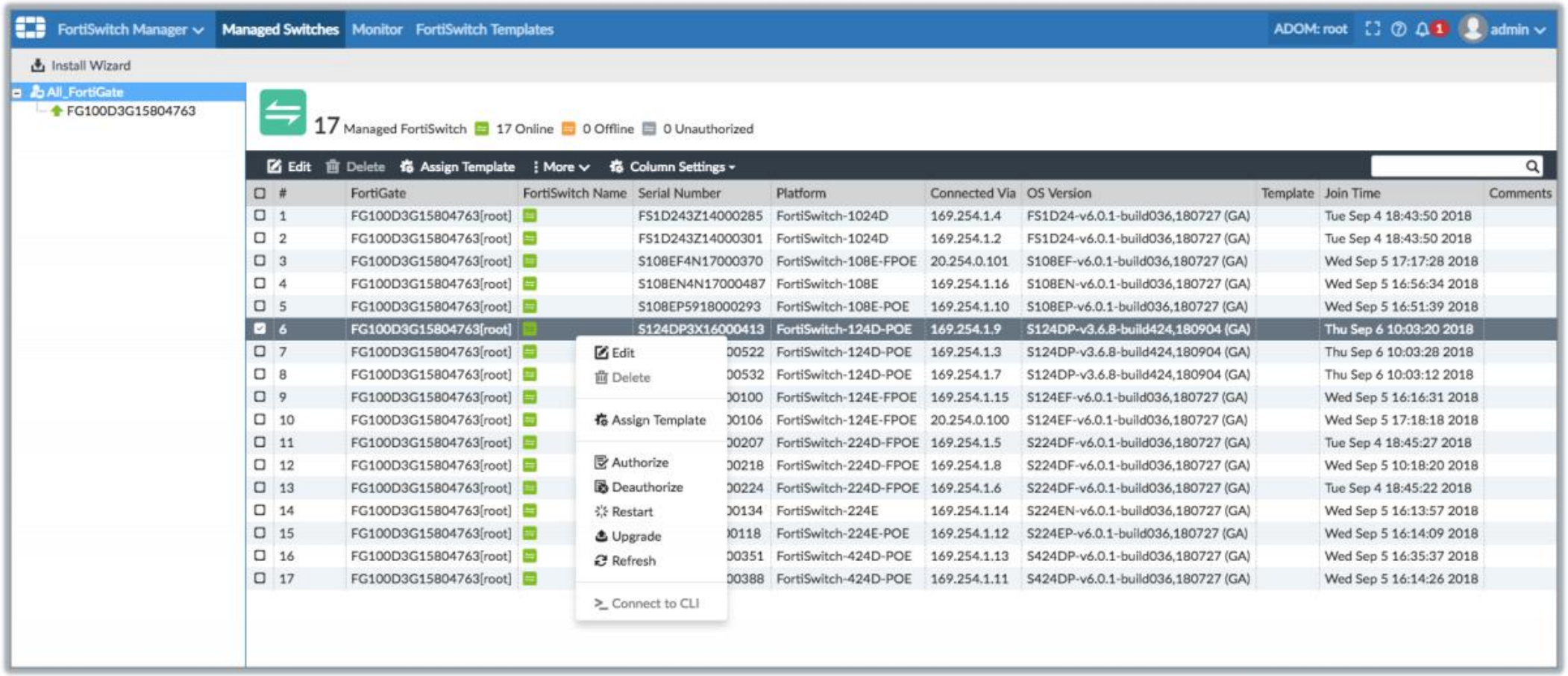
FortiManager – централизованное управление FortiSwitch (Managed Mode)



Fabric Management Center

FortiManager – централизованное управление FortiSwitch (Managed Mode)

Авторизация коммутаторов, перезагрузка и обновление ПО, шаблоны конфигураций коммутаторов

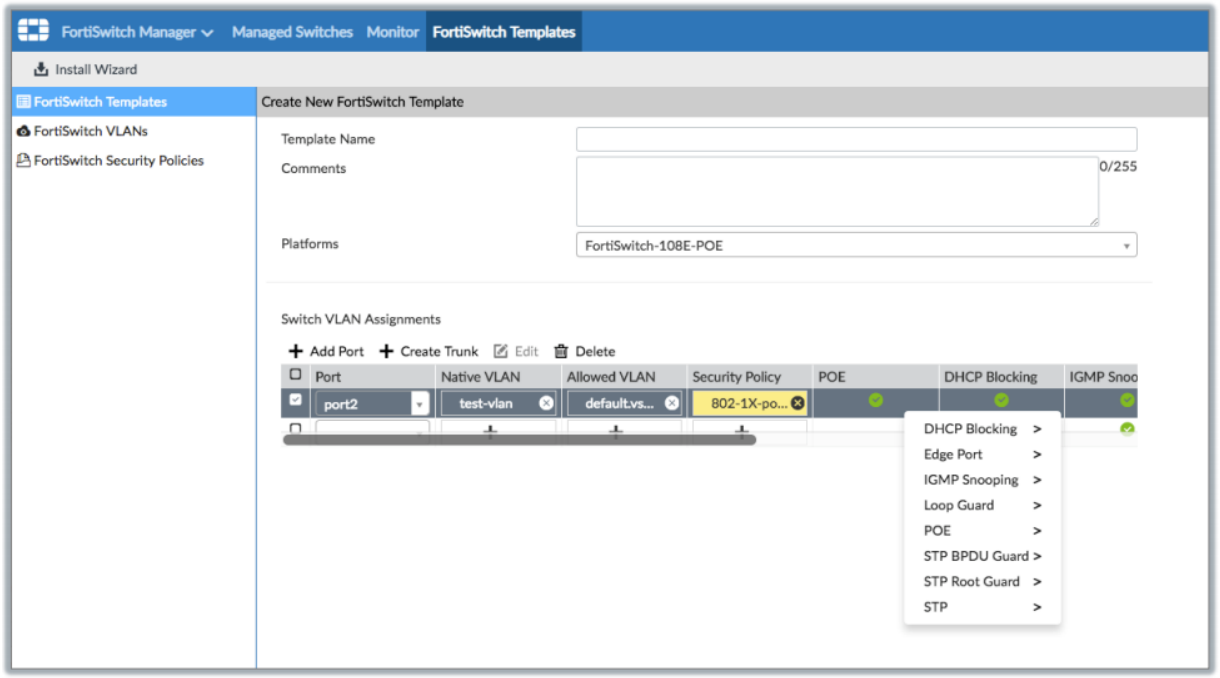


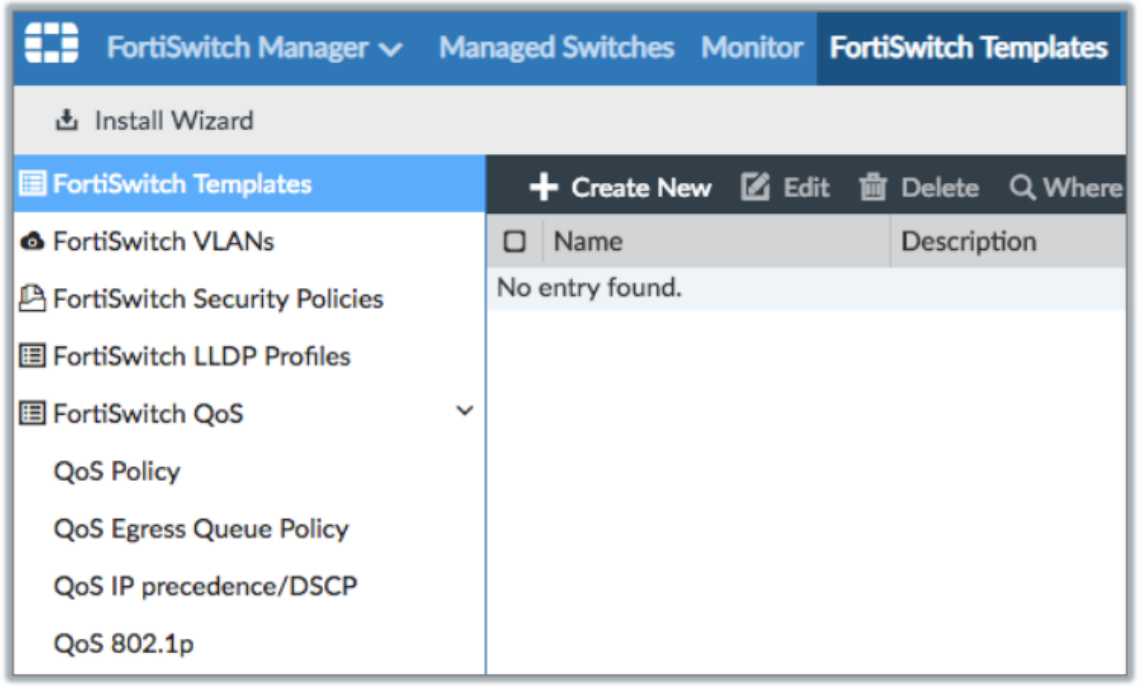
#	FortiGate	FortiSwitch Name	Serial Number	Platform	Connected Via	OS Version	Template	Join Time	Comments
1	FG100D3G15804763[root]		FS1D243Z14000285	FortiSwitch-1024D	169.254.1.4	FS1D24-v6.0.1-build036,180727 (GA)		Tue Sep 4 18:43:50 2018	
2	FG100D3G15804763[root]		FS1D243Z14000301	FortiSwitch-1024D	169.254.1.2	FS1D24-v6.0.1-build036,180727 (GA)		Tue Sep 4 18:43:50 2018	
3	FG100D3G15804763[root]		S108EF4N17000370	FortiSwitch-108E-FPOE	20.254.0.101	S108EF-v6.0.1-build036,180727 (GA)		Wed Sep 5 17:17:28 2018	
4	FG100D3G15804763[root]		S108EN4N17000487	FortiSwitch-108E	169.254.1.16	S108EN-v6.0.1-build036,180727 (GA)		Wed Sep 5 16:56:34 2018	
5	FG100D3G15804763[root]		S108EP5918000293	FortiSwitch-108E-POE	169.254.1.10	S108EP-v6.0.1-build036,180727 (GA)		Wed Sep 5 16:51:39 2018	
6	FG100D3G15804763[root]		S124DP3X16000413	FortiSwitch-124D-POE	169.254.1.9	S124DP-v3.6.8-build424,180904 (GA)		Thu Sep 6 10:03:20 2018	
7	FG100D3G15804763[root]		00522	FortiSwitch-124D-POE	169.254.1.3	S124DP-v3.6.8-build424,180904 (GA)		Thu Sep 6 10:03:28 2018	
8	FG100D3G15804763[root]		00532	FortiSwitch-124D-POE	169.254.1.7	S124DP-v3.6.8-build424,180904 (GA)		Thu Sep 6 10:03:12 2018	
9	FG100D3G15804763[root]		00100	FortiSwitch-124E-FPOE	169.254.1.15	S124EF-v6.0.1-build036,180727 (GA)		Wed Sep 5 16:16:31 2018	
10	FG100D3G15804763[root]		00106	FortiSwitch-124E-FPOE	20.254.0.100	S124EF-v6.0.1-build036,180727 (GA)		Wed Sep 5 17:18:18 2018	
11	FG100D3G15804763[root]		00207	FortiSwitch-224D-FPOE	169.254.1.5	S224DF-v6.0.1-build036,180727 (GA)		Tue Sep 4 18:45:27 2018	
12	FG100D3G15804763[root]		00218	FortiSwitch-224D-FPOE	169.254.1.8	S224DF-v6.0.1-build036,180727 (GA)		Wed Sep 5 10:18:20 2018	
13	FG100D3G15804763[root]		00224	FortiSwitch-224D-FPOE	169.254.1.6	S224DF-v6.0.1-build036,180727 (GA)		Tue Sep 4 18:45:22 2018	
14	FG100D3G15804763[root]		00134	FortiSwitch-224E	169.254.1.14	S224EN-v6.0.1-build036,180727 (GA)		Wed Sep 5 16:13:57 2018	
15	FG100D3G15804763[root]		00118	FortiSwitch-224E-POE	169.254.1.12	S224EP-v6.0.1-build036,180727 (GA)		Wed Sep 5 16:14:09 2018	
16	FG100D3G15804763[root]		00351	FortiSwitch-424D-POE	169.254.1.13	S424DP-v6.0.1-build036,180727 (GA)		Wed Sep 5 16:35:37 2018	
17	FG100D3G15804763[root]		00388	FortiSwitch-424D-POE	169.254.1.11	S424DP-v6.0.1-build036,180727 (GA)		Wed Sep 5 16:14:26 2018	

Fabric Management Center

FortiManager – централизованное управление FortiSwitch (Managed Mode)

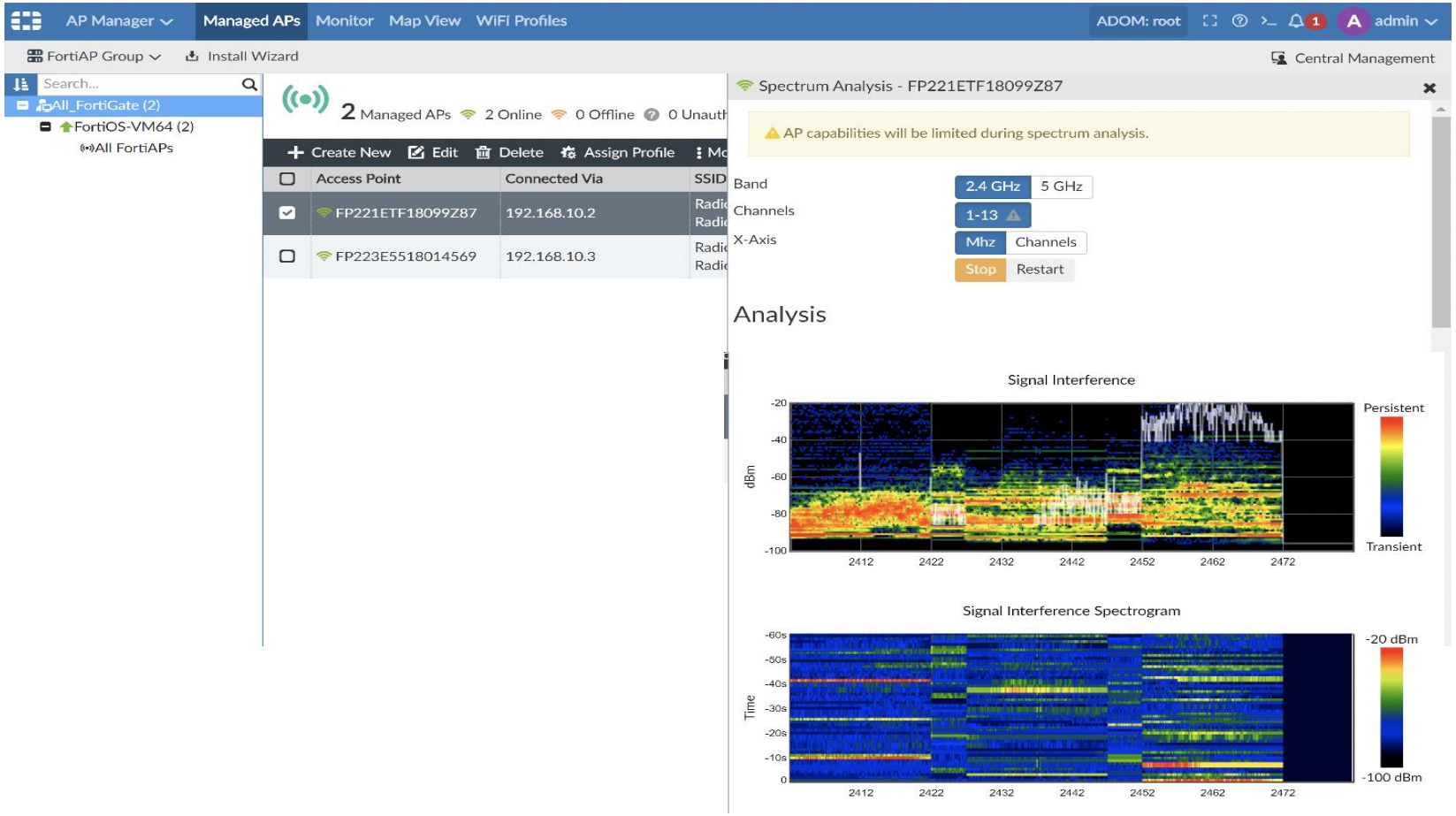
- Шаблоны конфигурации для настройки FortiSwitch из FortiManager (VLAN / Port, STP, 802.1x, LoopGuard, DHCP и IGMP Snooping, LLDP и QoS Profile, PoE)
- Zero Touch Provisioning (ZTP) для FortiSwitch, импорт конфигурации FortiSwitch с FortiGate





Fabric Management Center

FortiManager - управление и мониторинг беспроводной сети в Real Time



Использование FortiManager Monitor for Real-time Visibility (< last day):

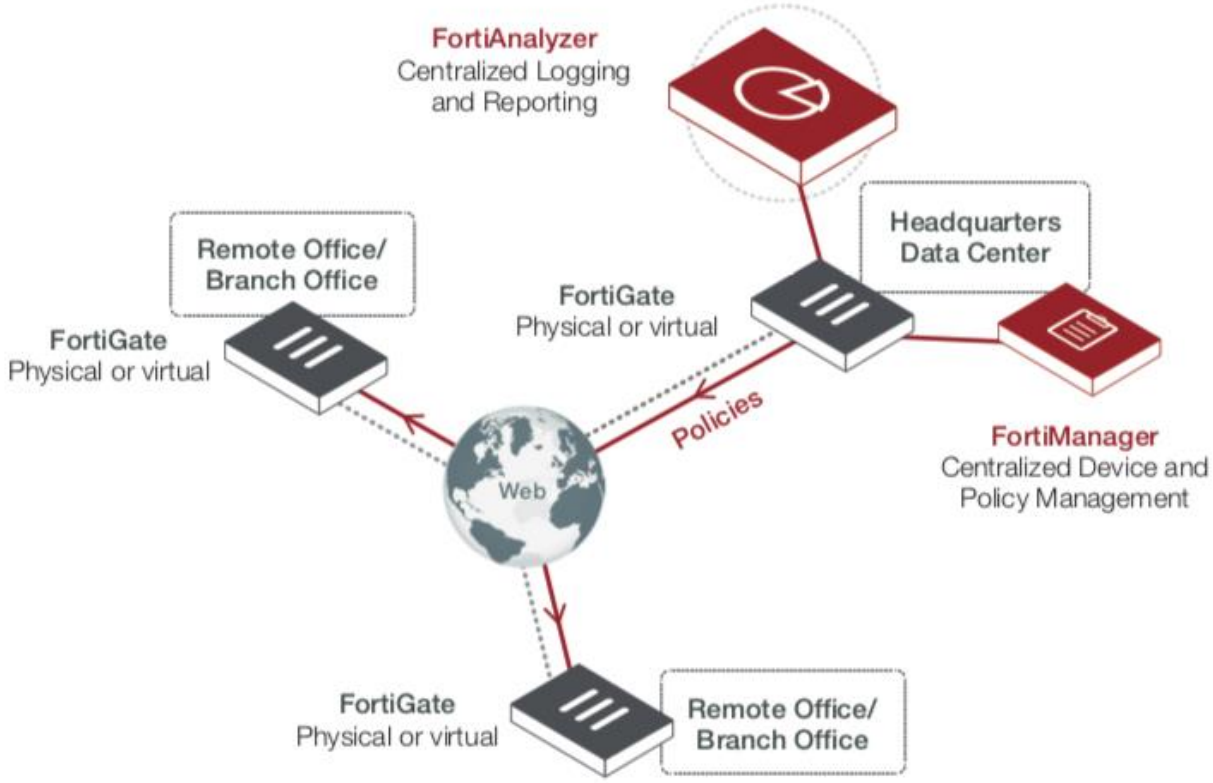
- Понимание RT Bandwidth Usage
- Понимание Real-time SLA Insights
- Мониторинг точек доступа и коммутаторов

Fabric Management Center

FortiAnalyzer – обязательный компонент Security Fabric

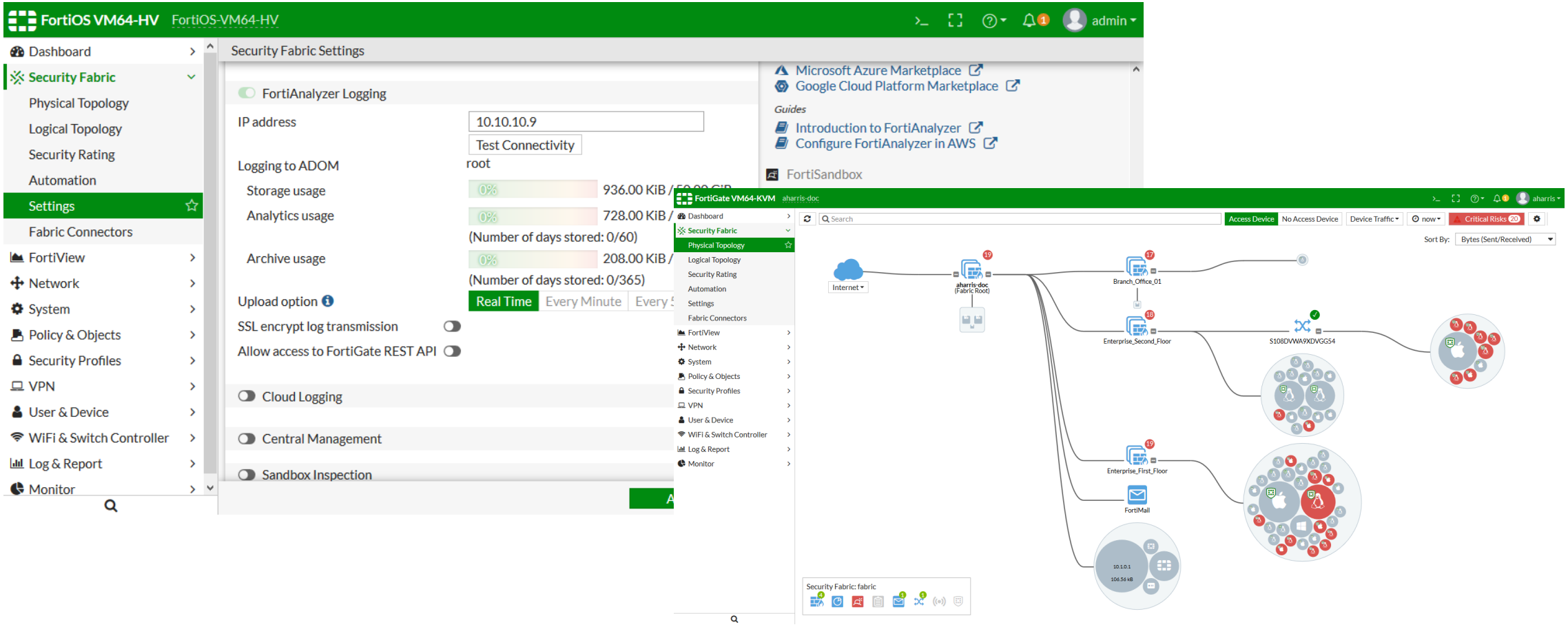
Журналирование, отчетность и аналитика с множества устройств Fortinet

- Централизованный поиск и отчетность
- Мониторинг в реальном времени или исторический мониторинг сетевой активности
- Сканирование журналов безопасности с использованием данных FortiGuard IOC Intelligence для противостояния комплексным угрозам
- Легковесное управление событиями
- Бесшовная интеграция с Fortinet Security Fabric



Fabric Management Center

FortiAnalyzer – обязательный компонент Security Fabric



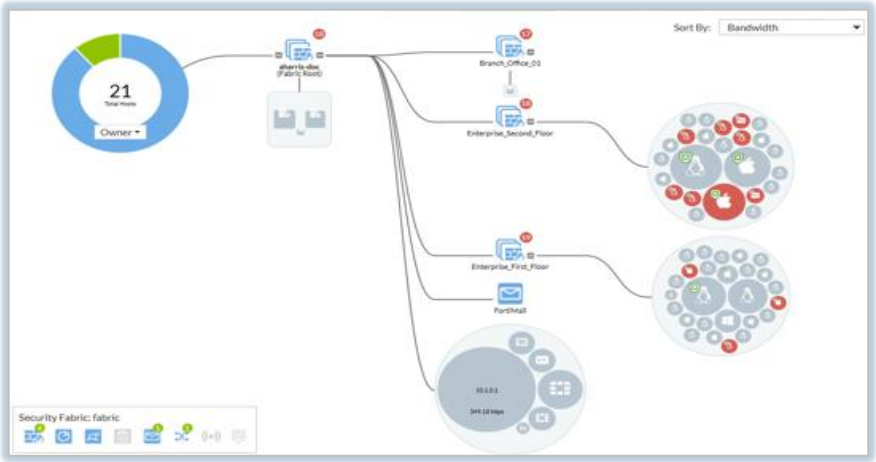
- FortiAnalyzer активирует Topology View в FortiGate

Fabric Management Center

FortiAnalyzer идентифицирует сетевые риски и риски безопасности в реальном времени

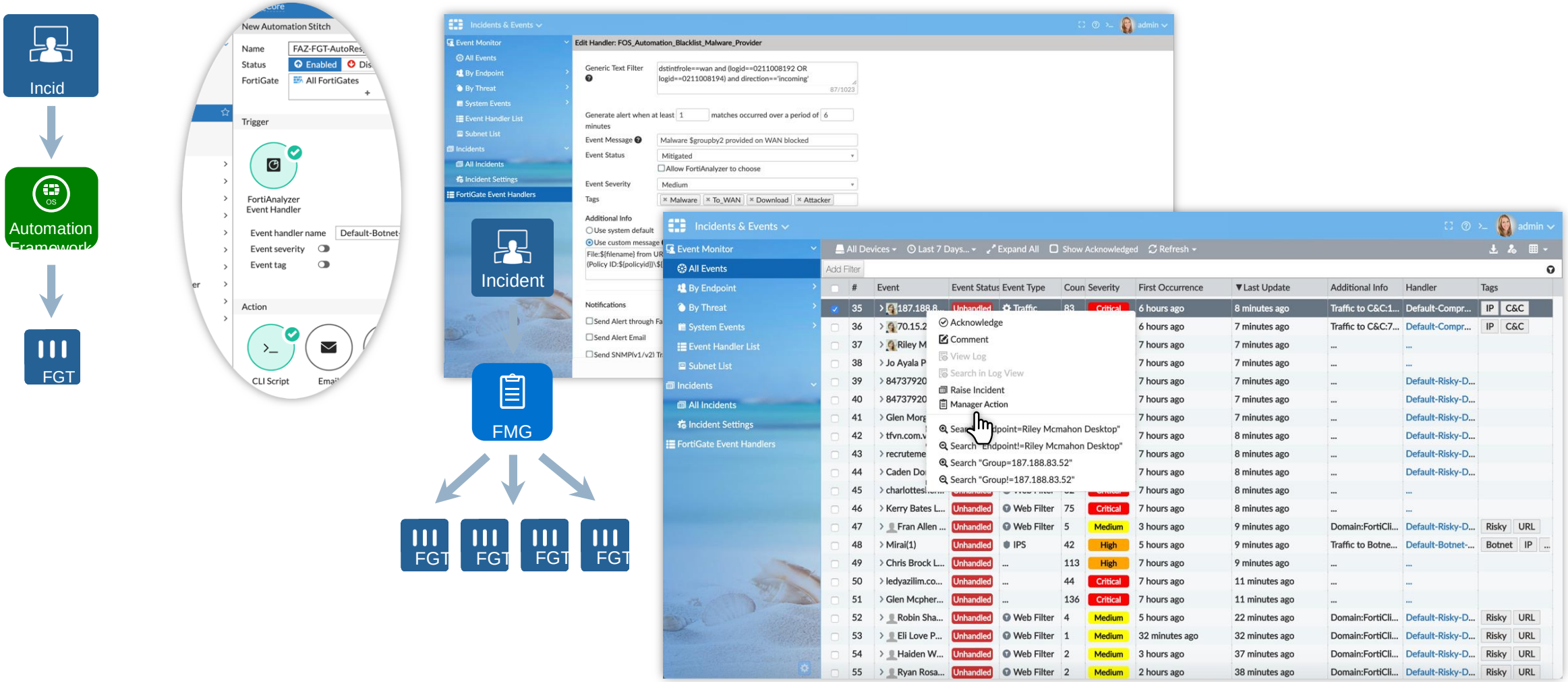
Ключевые возможности

- Network Health Visibility
- Realtime SLA Reporting
- Historic SLA Reporting
- Application Usage Reports & Dashboards
- Adaptive Response Handlers

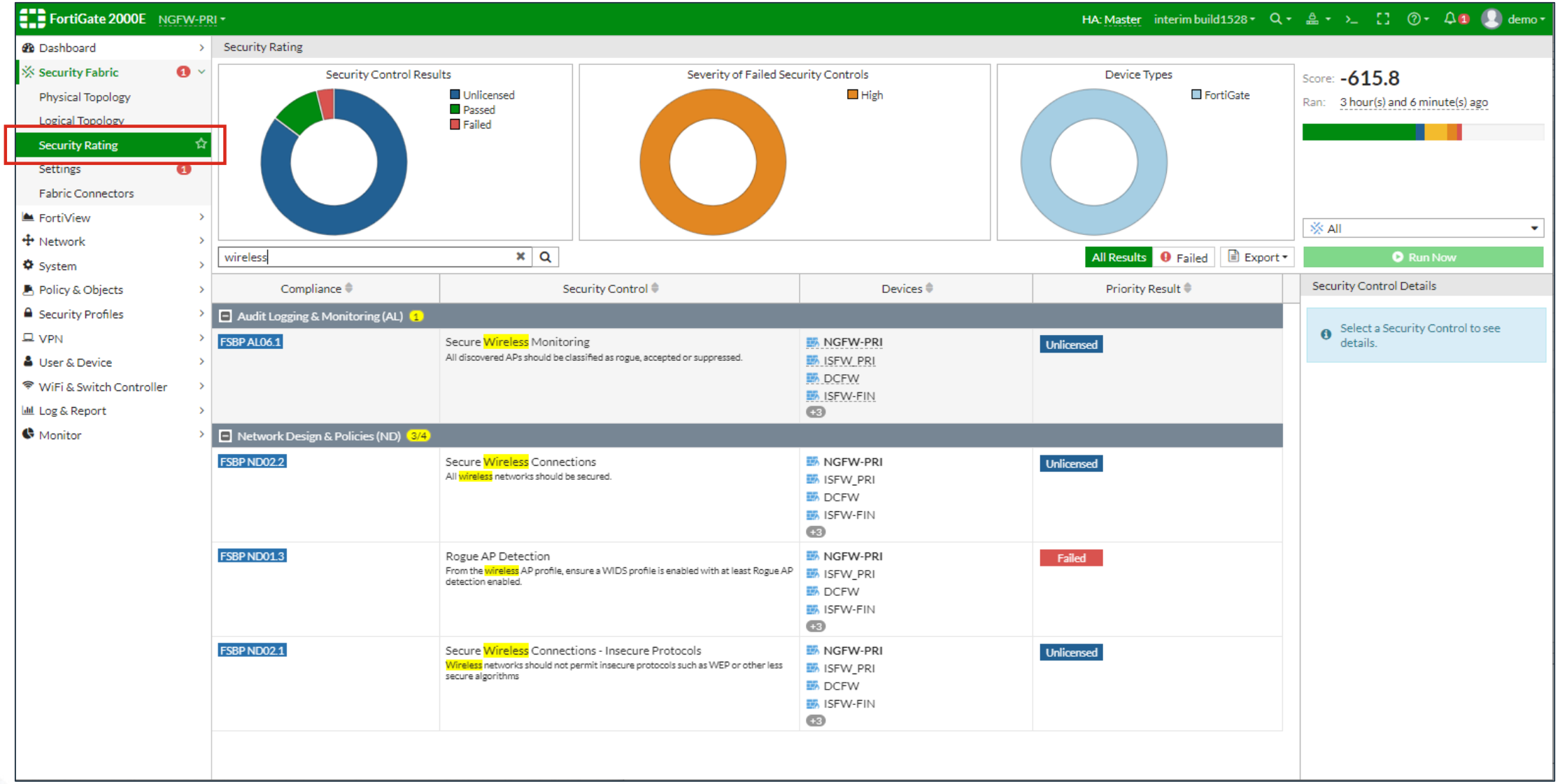


Fabric Management Center

Автоматизация реагирования на инциденты безопасности



Security Rating



Появились вопросы ?
Пишите нам:
cis@fortinet.com
cis_se@fortinet.com