FortiOS 6.4 – ядро Fortinet Security Fabric

Chingis Taltaev

SE

ctaltaev@fortinet.com

Fortinet Security Fabric для Цифровых Инноваций

Платформа кибербезопасности для защиты каждого элемента инфраструктуры

Zero-trust Network Access

Идентификация и обеспечение безопасности пользователей и устройств внутри и вовне сети

Security-driven Networking

Обеспечение сетевой безопасности без ущерба производительности

Dynamic Cloud Security

Безопасность и контроль облачной инфраструктуры и приложений

AI-driven Security Operations

Автоматическое обнаружение, предотвращение, и реагирование на киберугрозы

Fortinet Security Fabric

Комплексная

Обеспечение полной видимости поверхности цифровой атаки для лучшего управления рисками ИБ

Интегрированная

Уменьшение сложности сопровождения множества разнородных продуктов

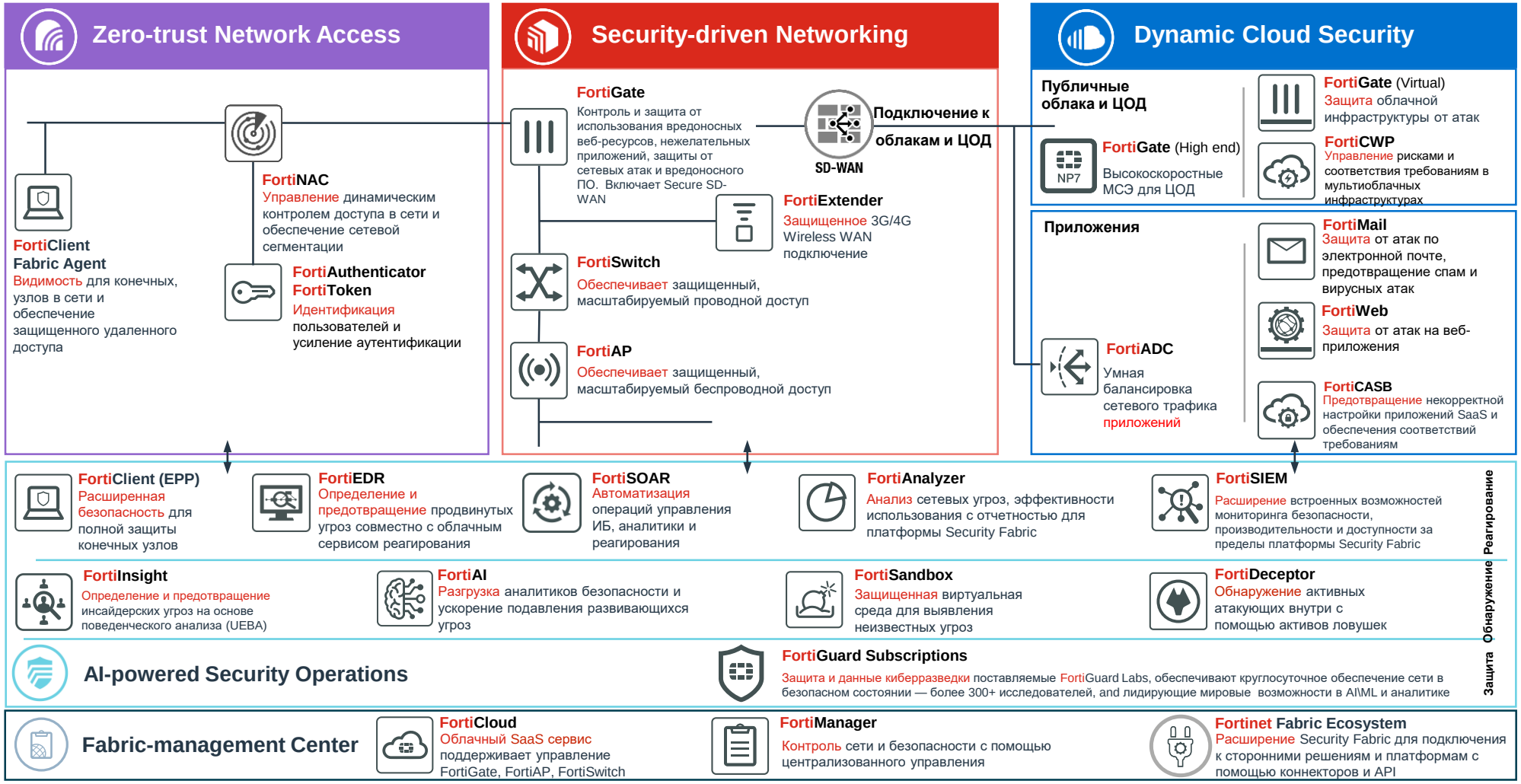
Автоматизированная

Увеличение скорости управления и отклика

Fortinet Security Fabric

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

Элементы платформы кибербезопасности



Операционная система FortiOS

Поддержка платформ

Поддержка аппаратных платформ FortiGate

FortiOS 6.4

FGR-30D/35D/60D/90D will not be supported on 6.4
Grey = EoO Products

	6.0.9	6.2.4	6.4
FG/FWF-30D Series	●		
FG/FWF-30E/50E Series	●	●	
FG/FWF-60E	●	●	●
FG/FWF-40F Series	?	6.2.5	6.4+
FG/FWF-60F Series	●	●	6.4+
FG/FWF-60D, FG-70D Series	●		
FG-80D	●	●	
FG-80E Series	●	●	●
FG/FWF-90D Series	●		
FG-90E Series	●	●	●
FG/FWF-92D Series	●	●	
FG-100D/140D Series	●	●	
FG-100/101E Series	●	●	●
FG-100F Series	●	●	6.4+
FG-200D Series	●		

	6.0.9	6.2.4	6.4
FG-200/201E	●	●	●
FG-300D/400D/500D/600D	●	●	●
FG-300E/500E Series	●	●	●
FG-400E/600E Series	●	●	●
FG-800D/900D/1x00D Series	●	●	●
FG-1100E Series	●	●	●
FG-1800F Series	?	6.2.5	6.4+
FG-2200E, 3300E Series	●	●	6.4+
FG-2000E, 2500E	●	●	●
FG-3X00D Series	●	●	●
FG-3400E/3600E	●	●	●
FG-3960E/3980E	●	●	●
FG-5001D/5001E	●	●	●
FG-6000/7000 Series	●	6.2.3+	6.4+

Поддержка облачных платформ и платформ SDN

FortiOS 6.4

Гипервизоры и платформы публичных облаков	6.4
VMware ESXi / vSphere	●
Microsoft Hyper-V	●
KVM	●
Citrix XEN / Open Source XEN	●
Amazon Web Services (AWS)	● (BYOL / PAYG)
Microsoft Azure	● (BYOL / PAYG)
Google Cloud Platform (GCP)	● (BYOL / PAYG)
Alibaba AliCloud	● (BYOL / PAYG)
Oracle Cloud Infrastructure (OCI)	● (BYOL)
RackSpace	● (BYOL / PAYG)

Платформы SDN	6.4
VMware NSX	●
Cisco ACI	●
OpenStack	●
Nuage VSP	●

Fabric Management Center

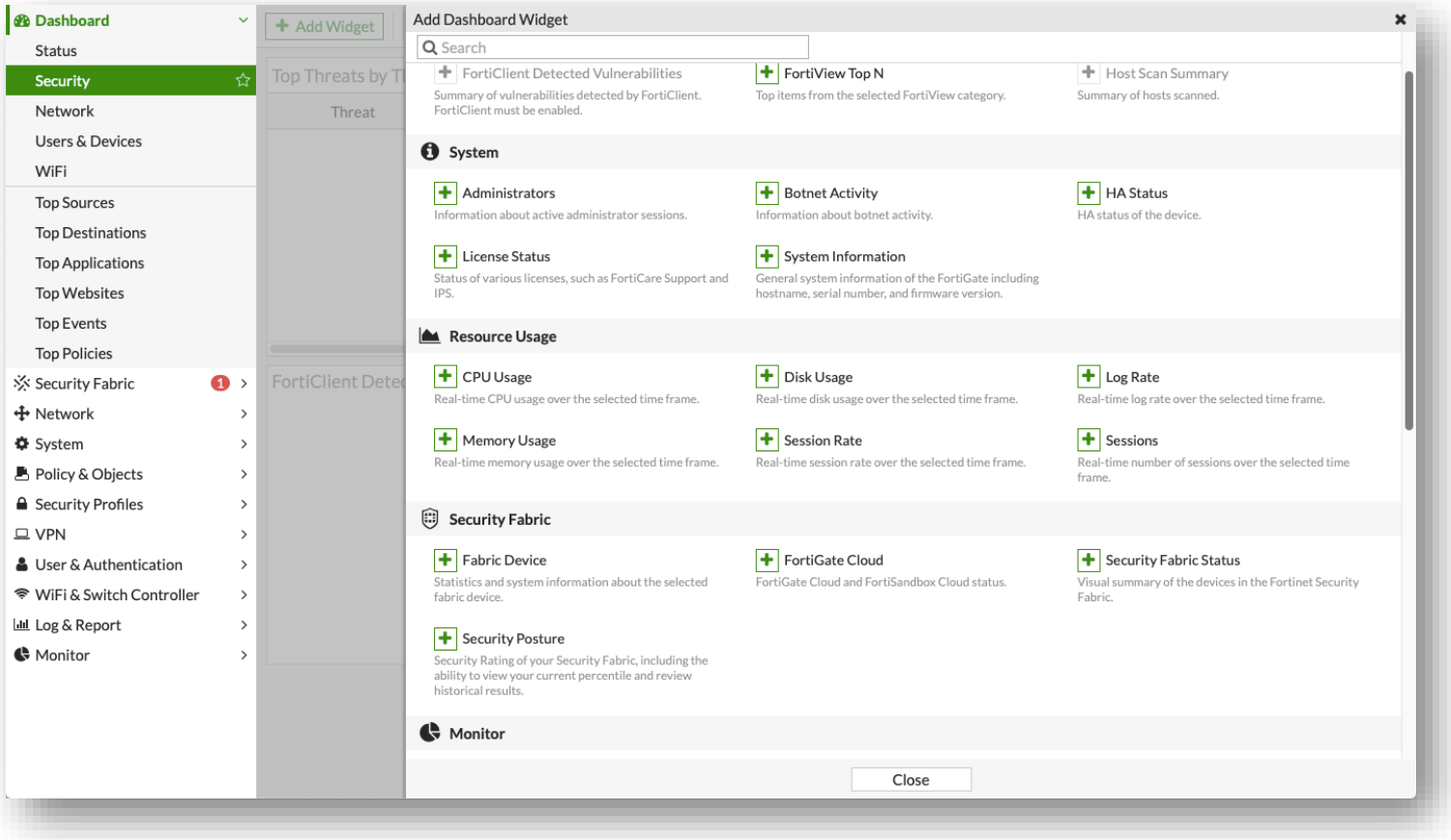
Управление Fortinet Security Fabric

Fabric Management Center

Объединение инструментов мониторинга Monitor и FortiView

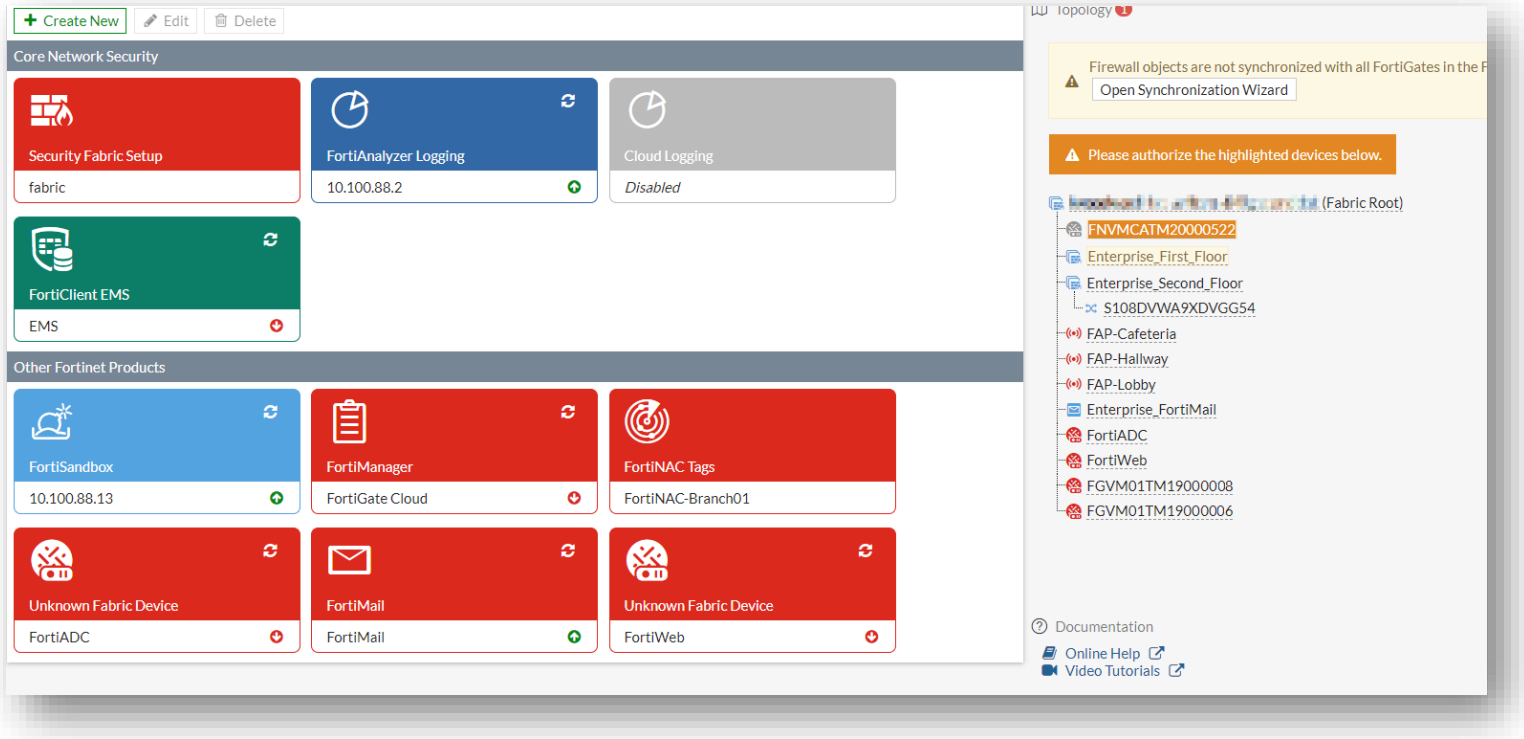
Страницы меню мониторинга FortiView и Monitor объединены в Dashboard.

- Установлено множество разделов FortiViews по умолчанию, дополнительные представления можно добавить в виде виджетов
- Предыдущие разделы меню Monitor такие как Routing, DHCP, IPsec и SSL-VPN Monitor объединены в Network Dashboard



Fabric Management Center

Улучшения в Fortinet Connectors



Редизайн Fabric Connector и страницы Fabric Setup для упрощения использования:

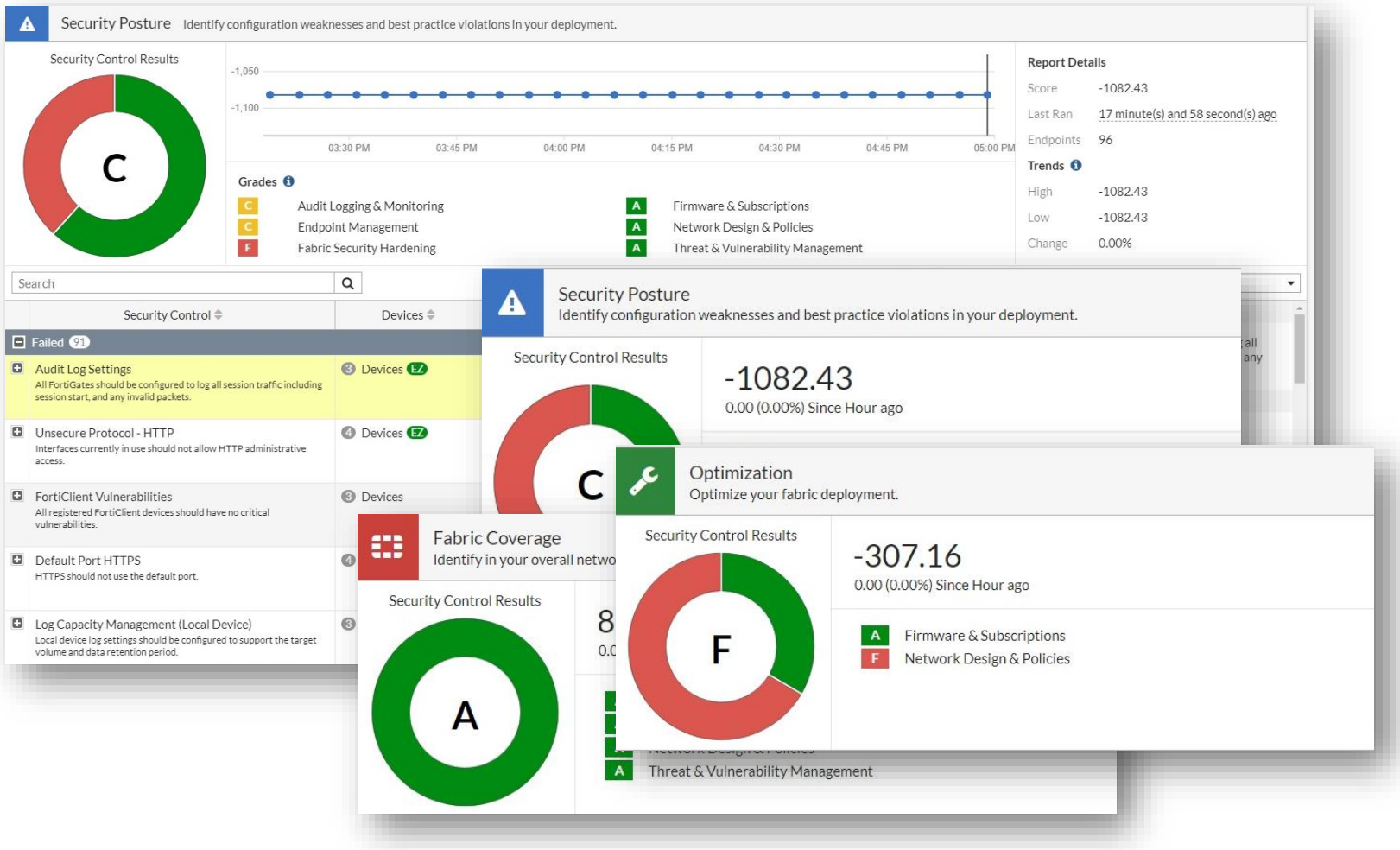
- Карточки по умолчанию доступны для различных продуктов и сервисов
- Также добавлено топологическое представление в боковой панели
- Коннекторы к сторонним системам настраиваются из раздела External Connectors.

Fabric Management Center

Улучшения в Security Rating / Fabric Score Card

Проведен редизайн - 3 основные панели карточек. Детальная информация доступна с помощью drilldown для каждой карточки с возможностью экспорта данных.

- Карточки - Security Posture, Fabric Coverage и Optimization.

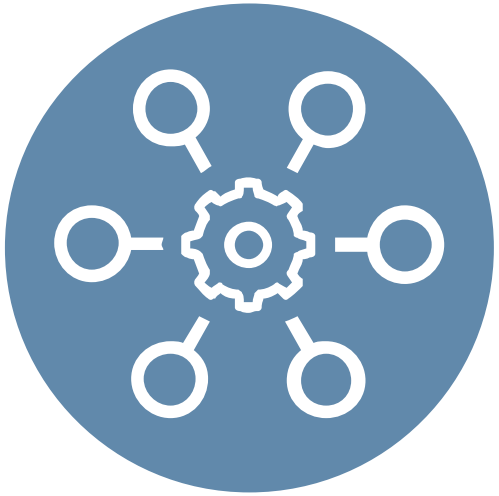


Fabric Management Center

Корневой FortiGate (Fabric root) использует диск для хранения исторической информации по пользователям и устройствам

Корневой FortiGate в Security Fabric хранит историческую информацию по пользователям и устройствам в базе данных на локальном диске. Это позволит администраторам визуализировать пользователей и устройства за период времени.

- Захват информации по пользователям и устройствам и хранение ее на диске
- Задел на будущее – для реализации в GUI отображения информации по пользователям и устройствам

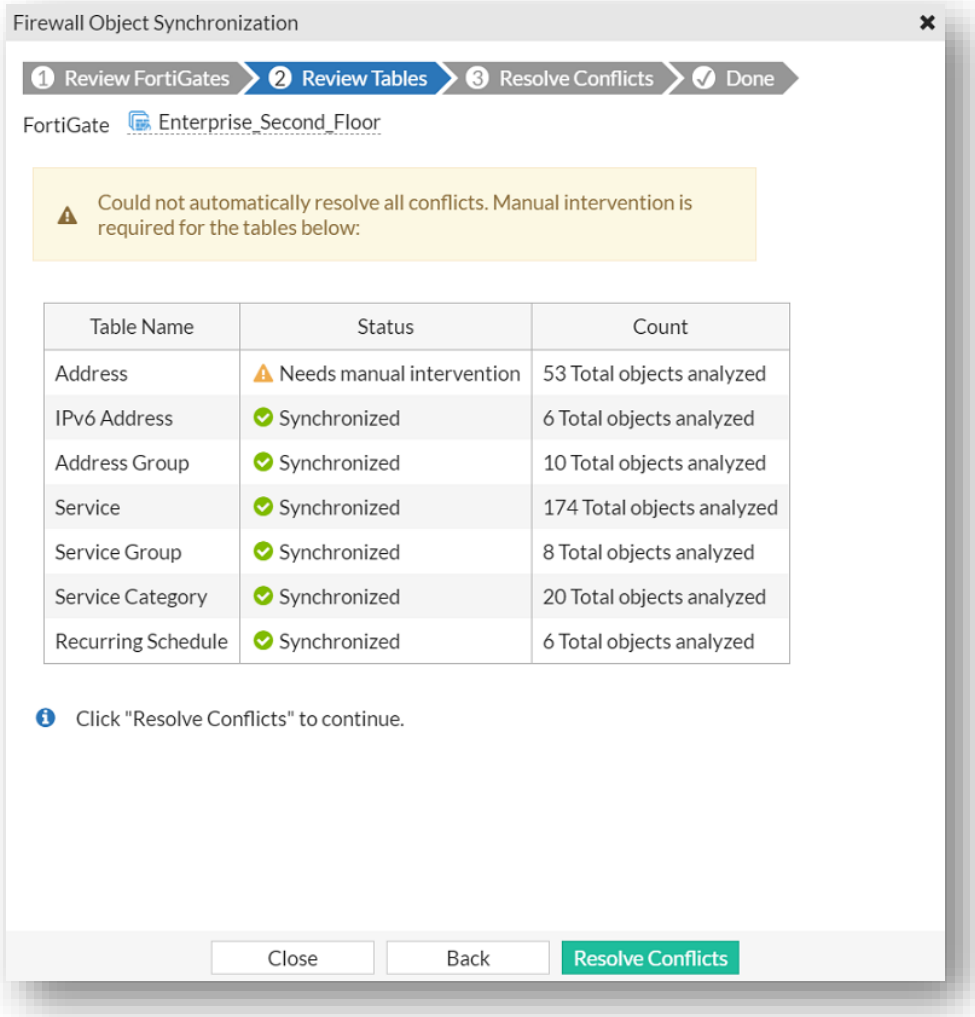


Fabric Management Center

Синхронизация объектов в Security Fabric

Возможность синхронизировать объекты между всеми FortiGate входящими в Security Fabric с использованием помощника.

- Помощник вызывается из меню Fabric Connectors
- Синхронизируемые объекты включают:
  - Address and Address Group
  - Service, Service Group and Service Category
  - Schedule and Schedule Group
- Конфликты синхронизации (по именам объектов) могут быть разрешены в автоматически или ручном режиме

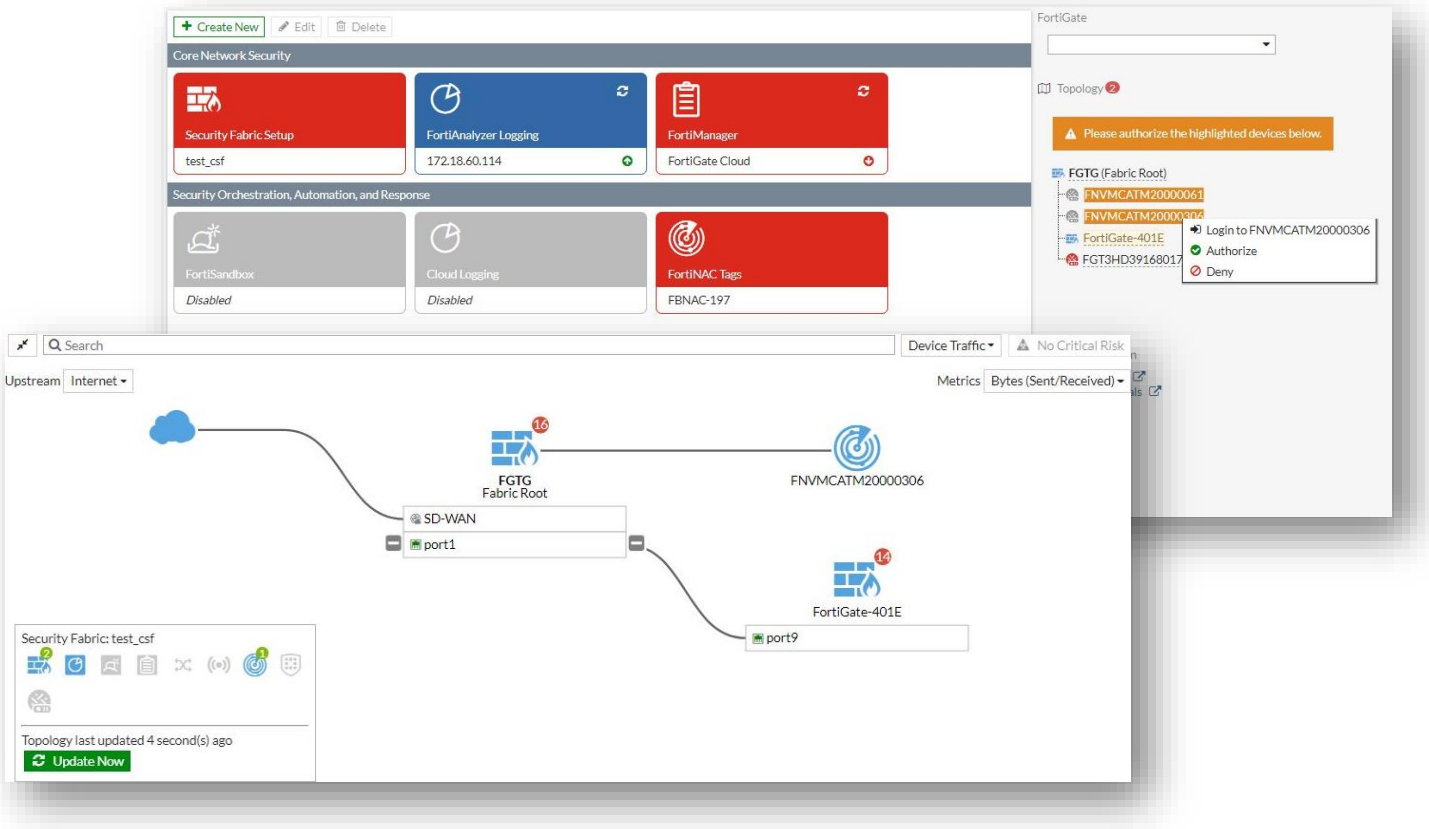


Fabric Management Center

Поддержка присоединения FortiNAC в FortiGate Fabric

FortiNAC можно авторизовать на корневом FortiGate (Fabric Root)

- Отображается в Physical и Logical Topology View
- Поддержка прямого логина на FortiNAC



Security-driven Networking

Сетевая безопасность без ущерба производительности

Security-driven Networking

Новая функциональность в FortiOS 6.4

NGFW

- Queue up logs in Local Storage if External Storage is temporarily unavailable
- Support UTM Inspection on asymmetric traffic in FGSP
- Consolidate IPv4 and IPv6 policy configuration
- Route leaking between VRFs
- Remove option to use normal AV database
- Command to force HA fail over

SD-WAN

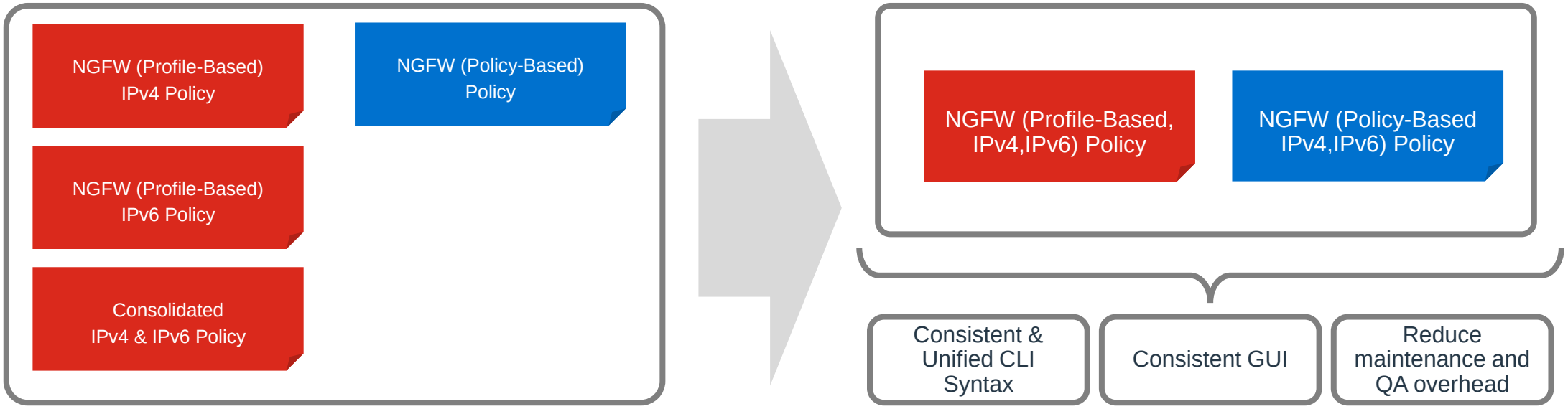
- Support IBGP / EBGP in VRF
- Connect Bandwidth Monitor Results to Interface Bandwidth
- SD-WAN factory default SLA further improvements
- SD-WAN: allow monitor to work on ADVPN short-cut
- Improved SD-WAN GUI and monitoring capabilities
- SD-WAN logs Improvements
- ADVPN Hole Punching
- SD-WAN support on OCVPN
- Allow FortiClient to join OCVPN
- Apply DSCP tag to SLA/Health Check probes

Secure Access

- FortiGate spectrum analysis GUI Support
- Wireless IPv6 support
- Wireless L3 firewall
- Switch Controller LLDP-MED Voice detection

Security-driven Networking

Консолидация конфигурации политик МСЭ IPv4 и IPv6



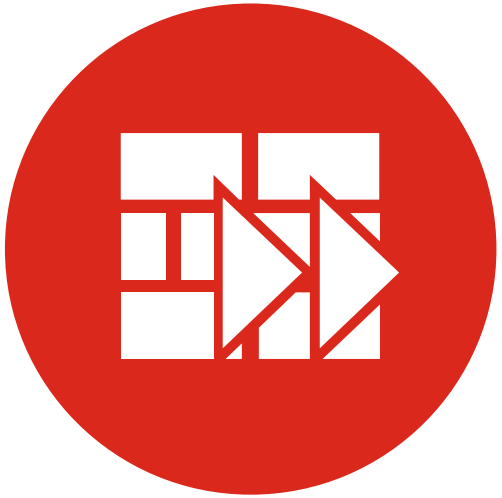
- В NGFW profile-based mode, консолидированные политики IPv4 и IPv6 объединены в единую политику МСЭ
- В NGFW policy-based mode, консолидированная политика теперь объединена с политикой МСЭ с поддержкой IPv6

Security-driven Networking

Изменения в базе сигнатур AV по умолчанию

Изменения в базе сигнатур AV:

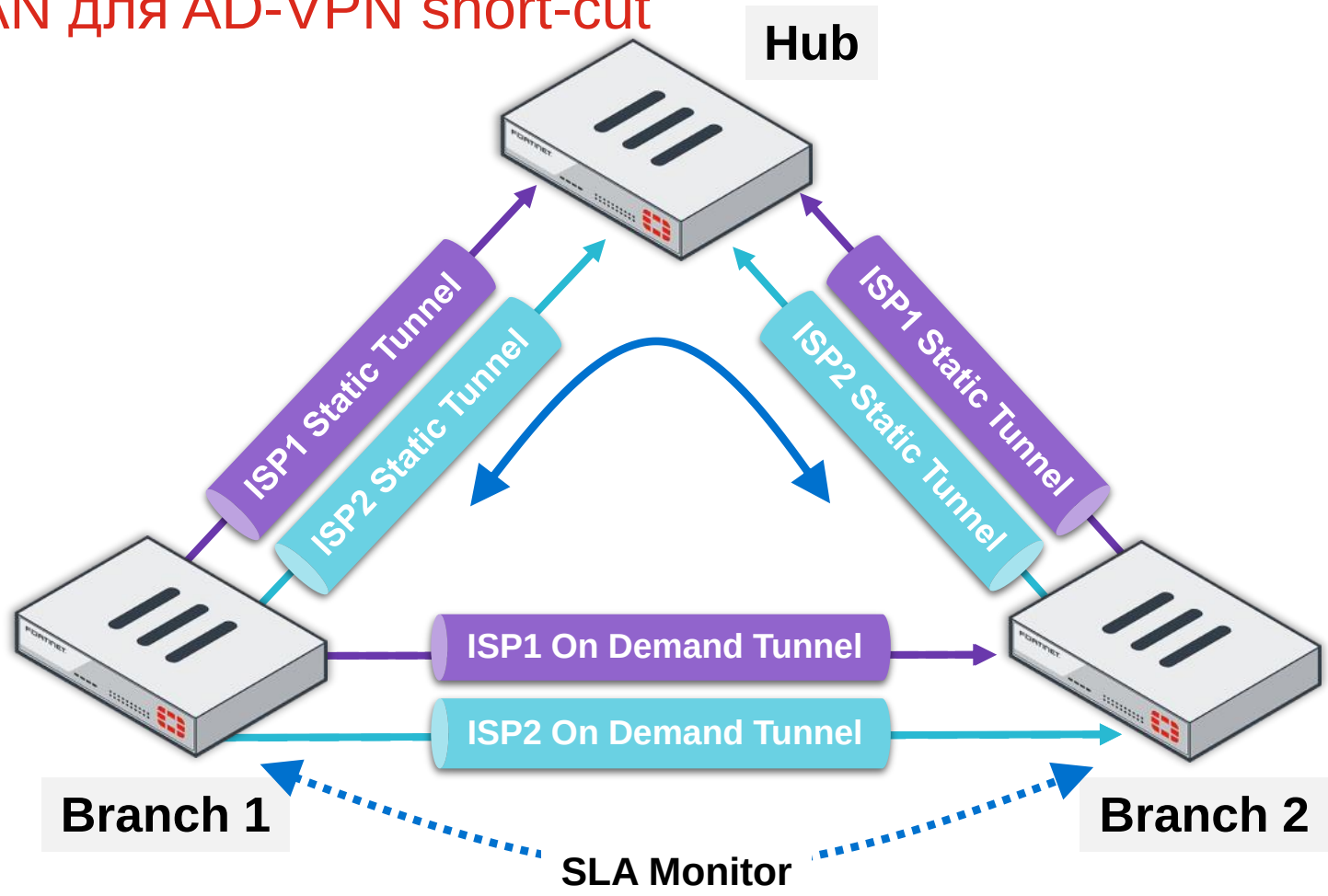
- По умолчанию установлена расширенная база AV сигнатур = Extended DB
- На high end моделях FortiGate, дополнительно доступна база AV сигнатур Extreme-DB
- База сигнатур Regular DB не используется и не доступна на FortiGate.



Security-driven Networking

Поддержка мониторинга SD-WAN для AD-VPN short-cut

- Ранее возможность мониторинга оверлейных линков была доступна только для развертывания Hub-and-Spoke (без short-cut, прямые динамические оверлейные линки между филиалами)
- Расширяет мониторинг SLA в SD-WAN для AD-VPN short-cut (прямые динамические оверлейные линки между филиалами)

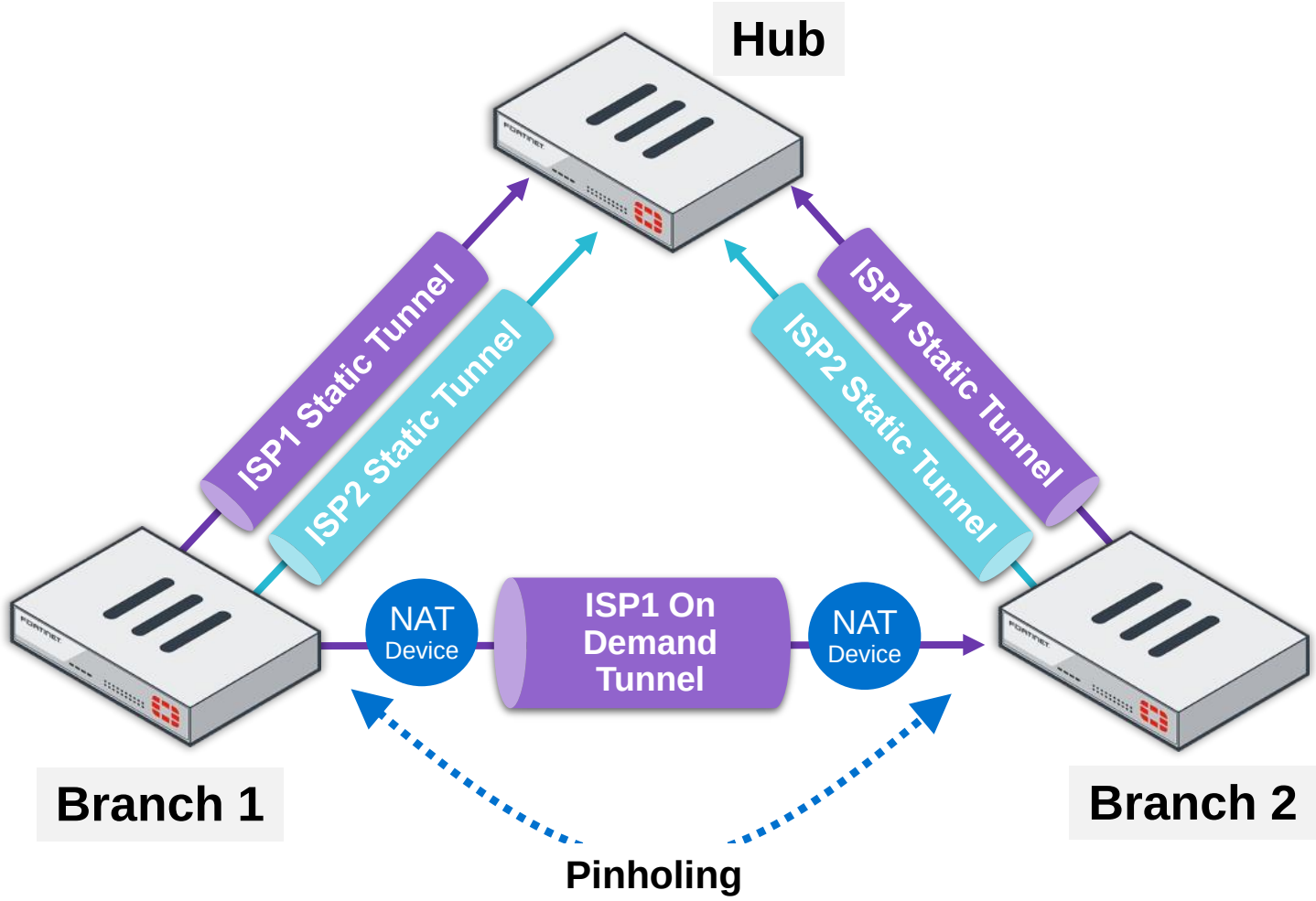


Security-driven Networking

Поддержка AD-VPN между филиалами за NAT (AD-VPN Hole Punching)

Обеспечивает поддержку AD-VPN для случая, когда оба филиала располагаются за NAT

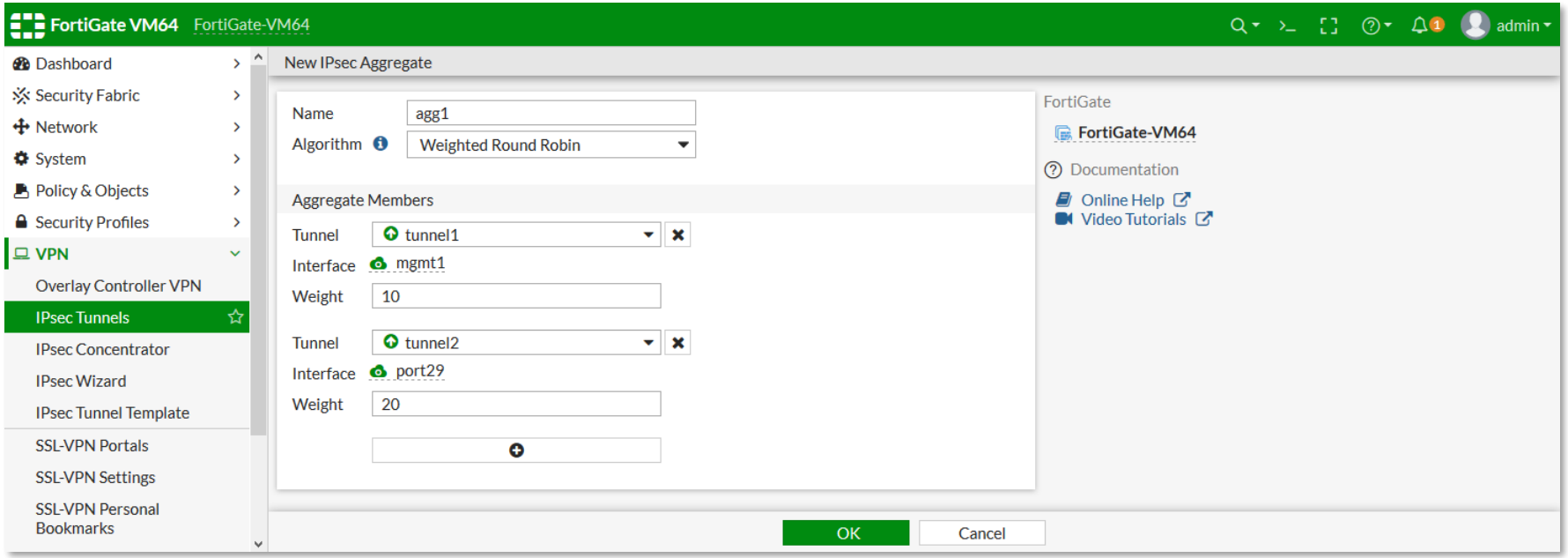
- Разрешается устанавливать прямые динамические оверлейные линки между филиалами с использованием техники UDP hole на NAT-устройствах
- NAT устройство должно поддерживать стандарт RFC4787 Endpoint-Independent Mapping



Security-driven Networking

Поддержка алгоритма Weighted Round Robin (WRR) для IPSec Aggregate

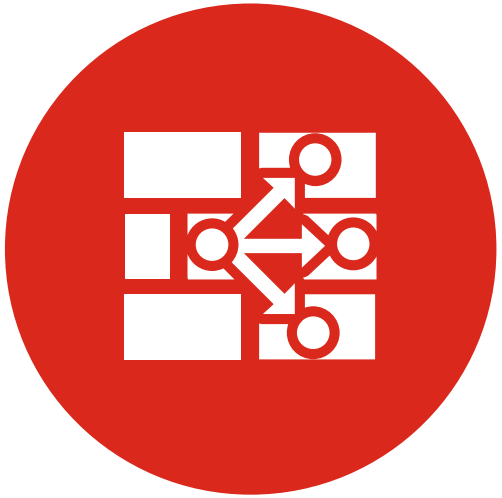
- Поддержка нового алгоритма WRR для обеспечения возможности неравнозначной балансировки по IPSec-туннелям, входящим в IPSec Aggregate (помимо L3/L4, Round-Robin, Redundant):



Security-driven Networking

Поддержка IBGP / EBGP в VRF

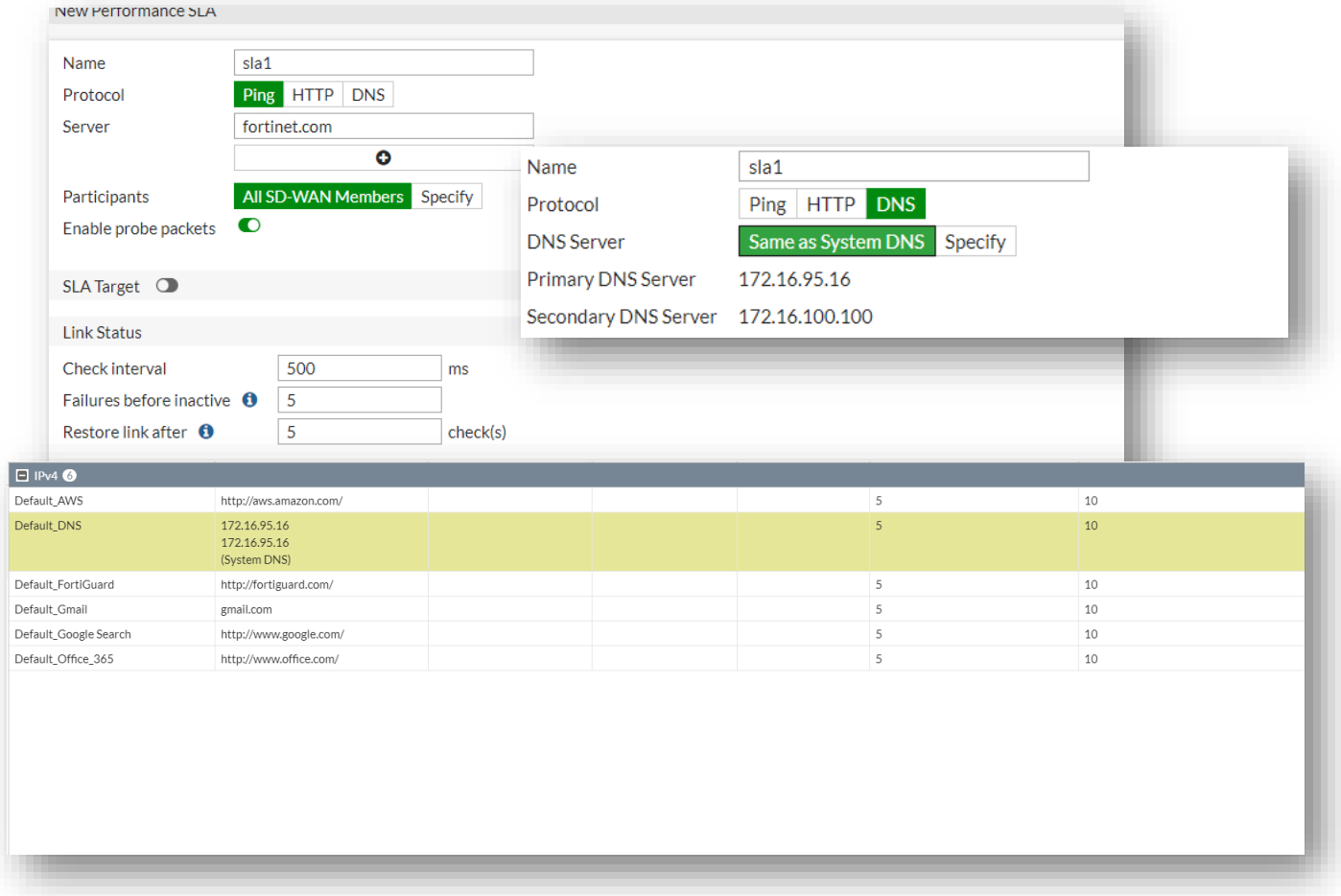
- Поддержка IBGP и EBGP в VRF, что является актуальным для ряда сценариев развертывания SD-WAN.
- Для разрешения установки соседства и обменом маршрутной информацией по EBGP / IBGP с другими FortiGate или маршрутизаторами поместите настройки VRF в соответствующие настройки соседства BGP.



Security-driven Networking

Улучшения в SD-WAN (заводские настройки)

- Поддержка DNS как нового протокола для SLA
- Возможность использования системного DNS в качестве SLA (один из готовых шаблонов SLA по умолчанию)
- Поддержка добавления всех членов SD-WAN ("All SD-WAN Members") в новые SLA по умолчанию



Security-driven Networking

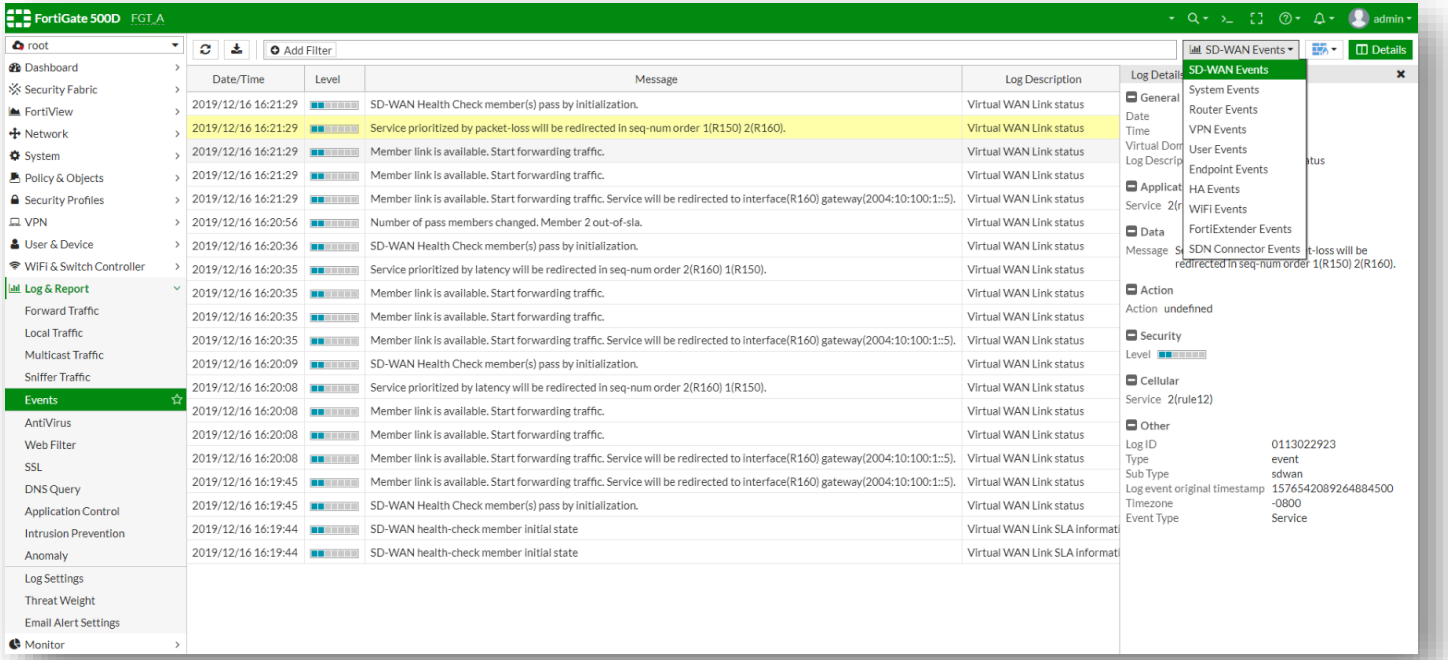
Улучшения в SD-WAN (журналирование)

Новый подтип события

- Отдельный подтип события для журналирования SD-WAN

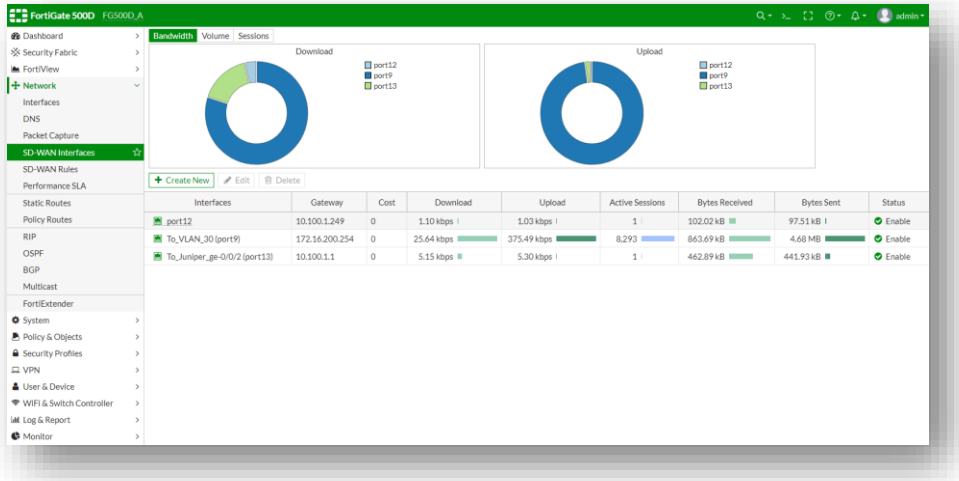
Улучшения в обработчиках событий и отчетах FortiAnalyzer (FAZ Event Handler and reports)

- Поддержка изменения, переименовывания и добавления новых полей журнала



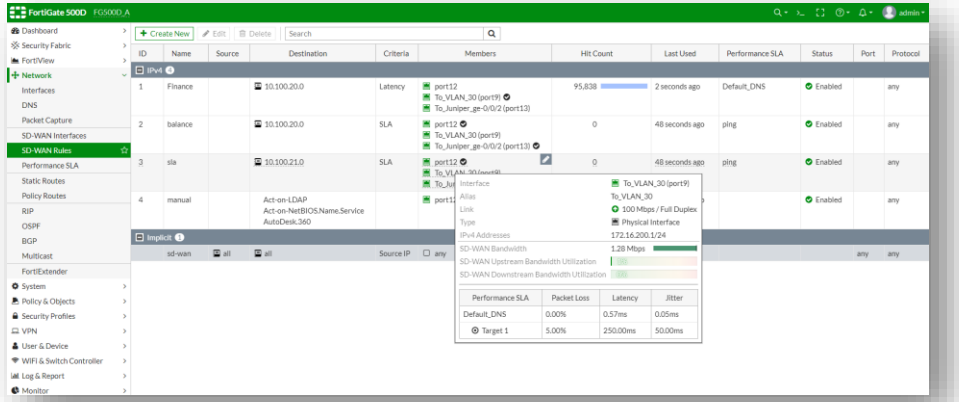
Security-driven Networking

Улучшения в SD-WAN GUI и мониторинге SD-WAN



Интерфейсы SD-WAN (SD-WAN interfaces)

- Круговые диаграммы
- Больше информации по каждому интерфейсу в таблице, включая количество сессий и количество отправленных / принятых байт



Правила SD-WAN (SD-WAN rules)

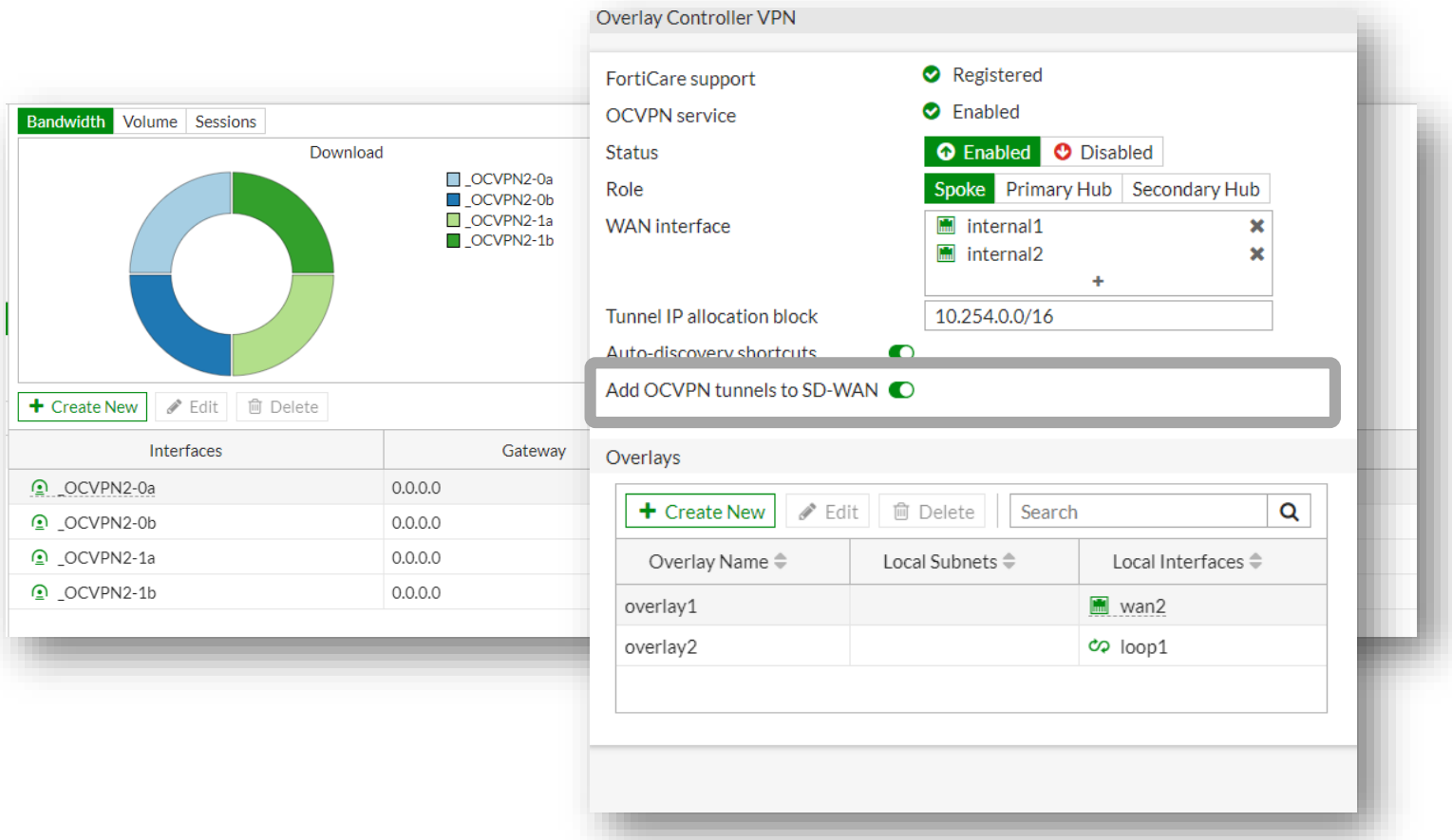
- Курсор поверх отметки на интерфейсе показывает подсказку о причине выбора данного интерфейса
- Более подробная информация выводится в подсказке, выводимая при пролете над именем интерфейса SD-WAN

Security-driven Networking

Поддержка интеграции SD-WAN с OCVPN

SD-WAN поддерживает добавление динамических туннелей OCVPN в качестве членов SD-WAN

- Что позволяет SD-WAN осуществлять проверку SLA и направлять сетевой трафик через туннели OCVPN

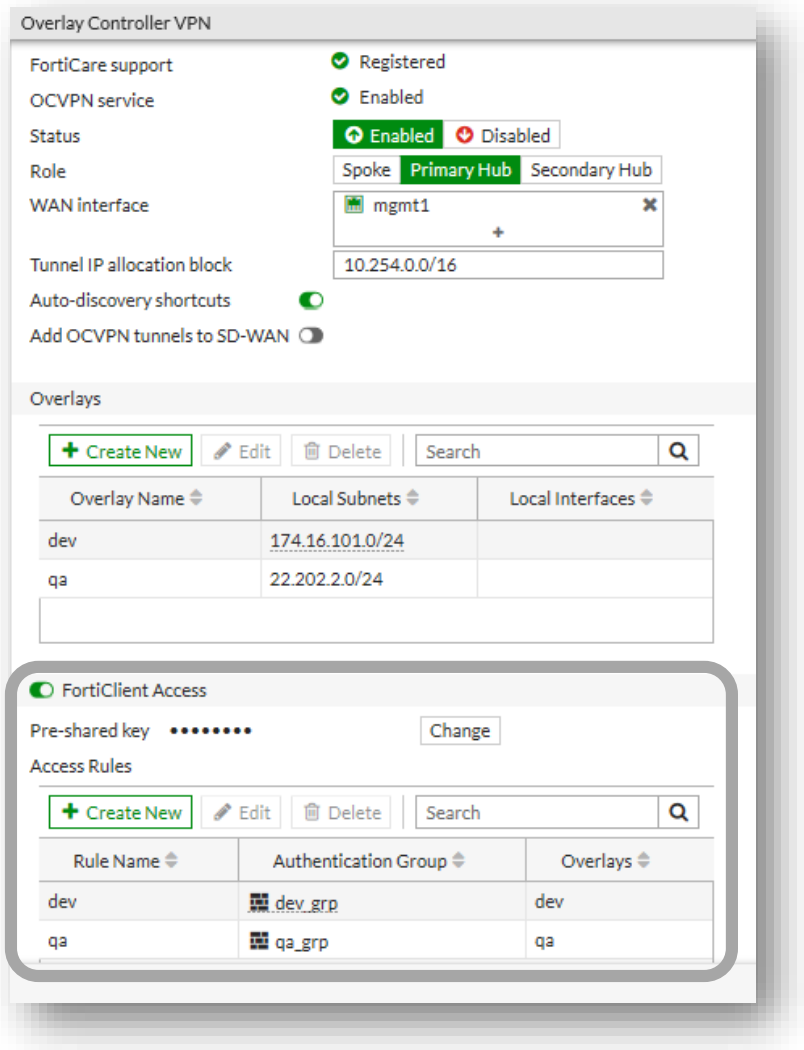


Security-driven Networking

Поддержка FortiClient для OCVPN

Обеспечивает возможность настройки удаленного подключения для FortiClient к OCVPN hub

- Доступ FortiClient поддерживается только для FGT с ролью OCVPN Hub.



Security-driven Networking

Поддержка маркировки поля DSCP для SLA/Health Check probes

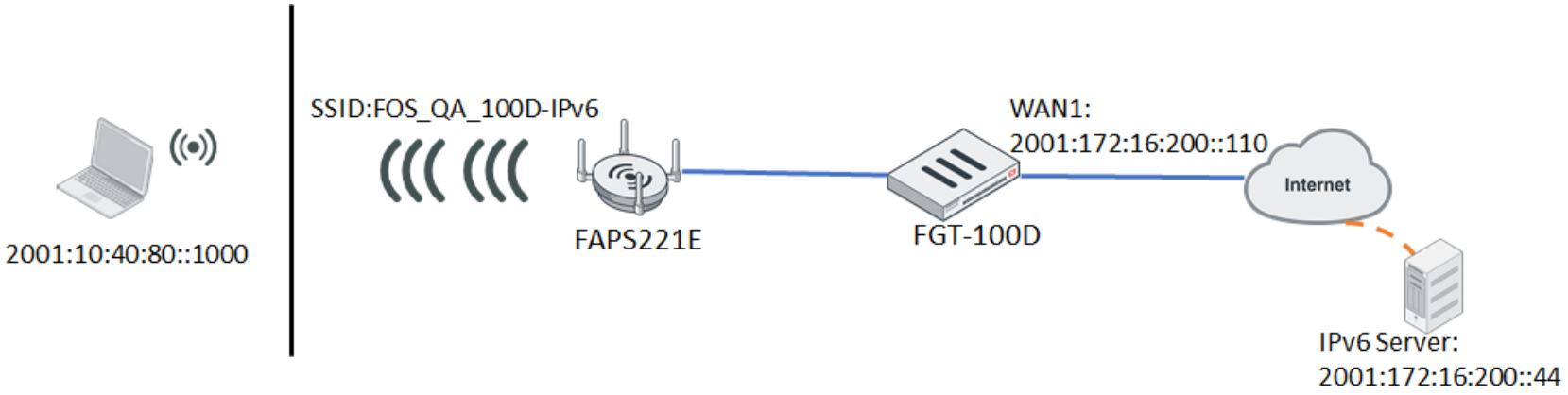
- SD-WAN поддерживает маркировку поля DSCP для пакетов health check
- Health Check пакеты могут отправляться с тем же приоритетом как и приложение
- Более точная оценка качества линков

```
config system virtual-wan-link
  config health-check
    edit <name>
      set diffservcode <6 bits binary, range 000000-
111111>
    next
  end
end
```

Security-driven Networking

Поддержка Wireless IPv6

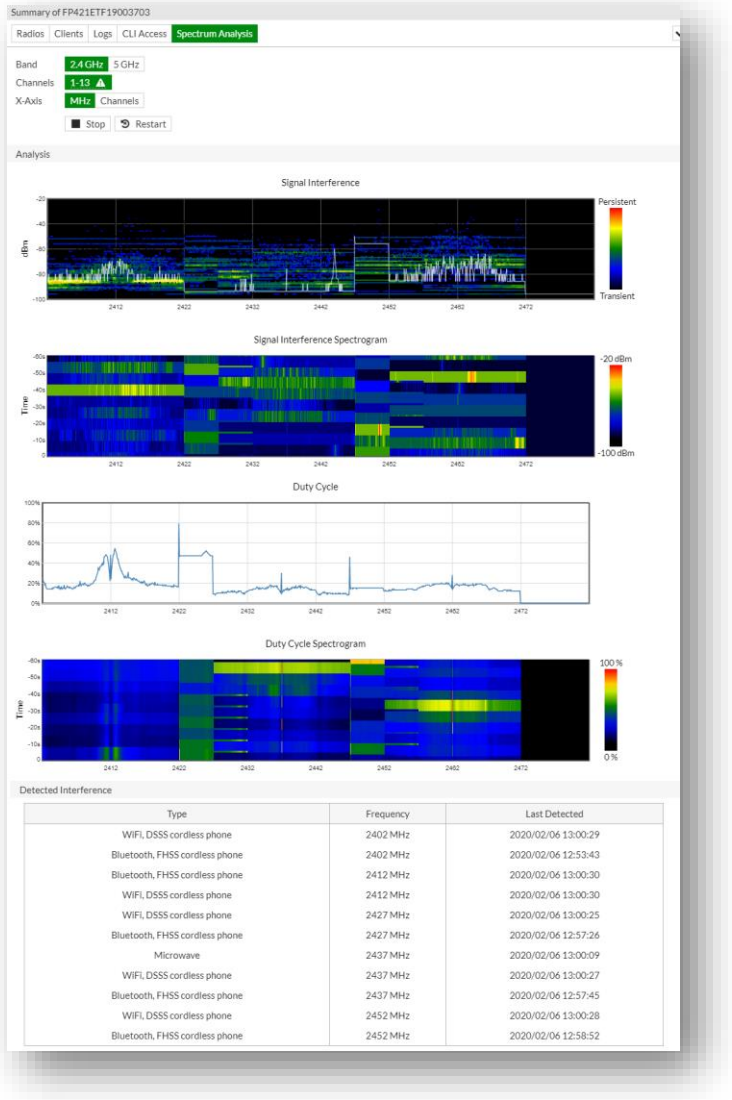
- IPv6 трафик беспроводных клиентов поддерживается как в туннельном режиме так и режиме local bridge SSID



Security-driven Networking

Встроенный анализатор спектра в GUI

- Поддержка для FAP E-series (ПО FAP 6.4)
- Радиомодули беспроводной точки доступа должны быть в режиме Dedicated Monitor
- Включает информацию:
  - Интерференция сигнала, спектрограмма интерференции сигнала
  - Занятость частотных каналов, спектрограмма занятости частотных каналов
  - Список обнаруженных объектов по интерференции



Security-driven Networking

Поддержка ACL на беспроводных точках доступа

Возможность централизованно создавать в CLI списки доступа (ACL) на беспроводных точках доступа для беспроводных клиентов на основании SRC/DST IP/PORT и протокола

- Поддержка только для беспроводных точек доступа управляемых с FortiGate
- ACL применяются к VAP (Virtual Access Point)

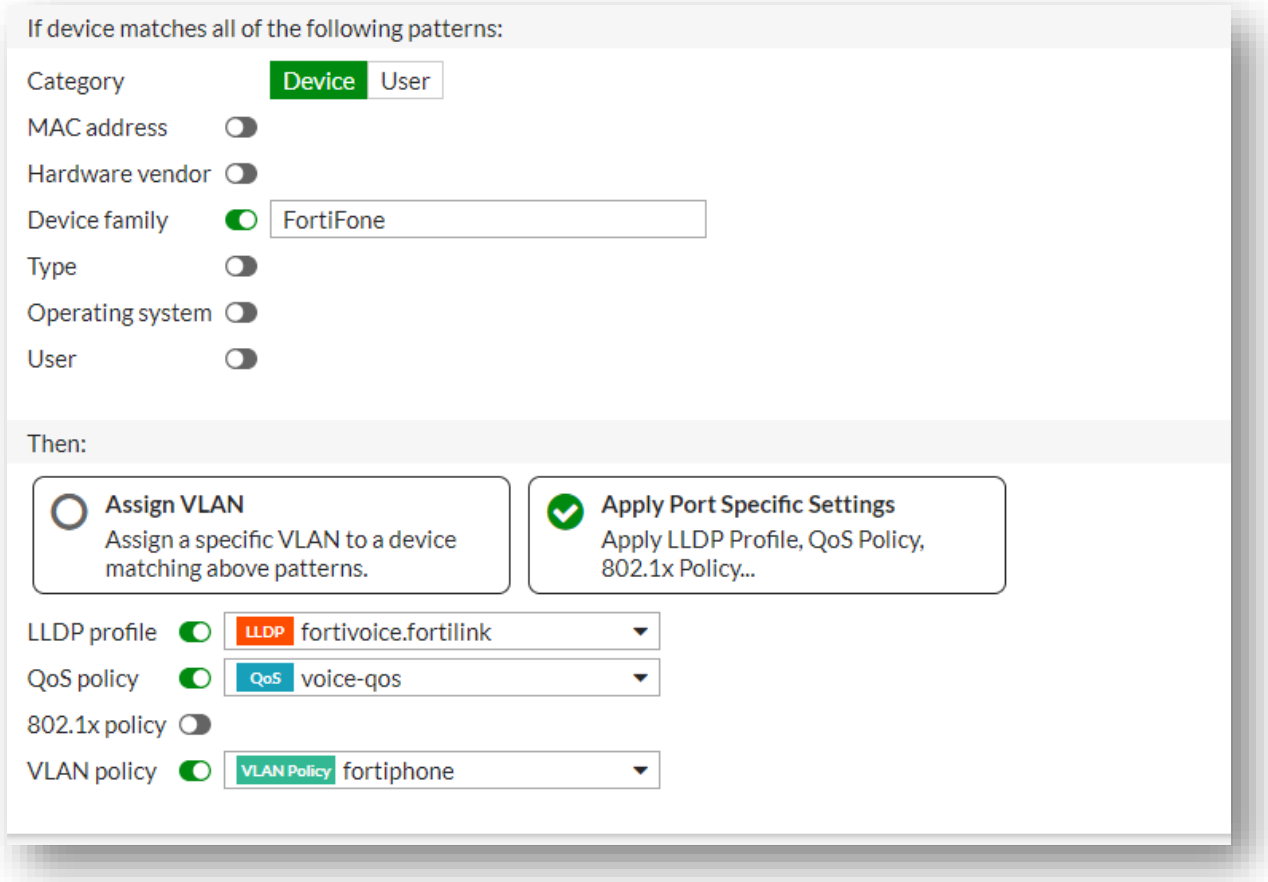
```
config wireless-controller access-control-list
    edit "ACL-1"
        config layer3-ipv4-rules
            edit 10
                set dstaddr 172.16.200.44/255.255.255.255
                set action deny
            next
            edit 20
                set protocol 1
                set action deny
            next
            edit 30
                set dstport 21
                set action deny
            next
        end
end
```

Security-driven Networking

Поддержка определения Voice устройств с помощью LLDP-MED

Новая возможность парсинга сообщений LLDP от Voice устройств на FortiGate Switch Controller / FortiSwitch и использование этой информации для обеспечения детектирования.

- В союзе с возможностями NAC, Voice устройство может быть автоматически определено в VLAN согласно политике NAC (NAC policy) на FortiGate



Security-driven Networking

Увеличение количества поддерживаемых FortiSwitch и FortiAP

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

Zero-Trust
Network Access

Идентификация и обеспечение безопасности
пользователей и устройств внутри и вовне сети

Zero-Trust Network Access

FortiOS 6.4

Обеспечение лучшего контроля доступа в сеть с новыми возможностями NAC

Конечные узлы

NAC

- **Новый сервис FortiGuard (IoT Security service)**
- **Встроенные возможности NAC на FortiSwitch**
- **FortiSwitch запрашивает IoT Security service для получения дополнительной информации по устройству**

Идентификация

Zero-Trust Network Access

FortiSwitch и FortiAP под управлением FortiGate

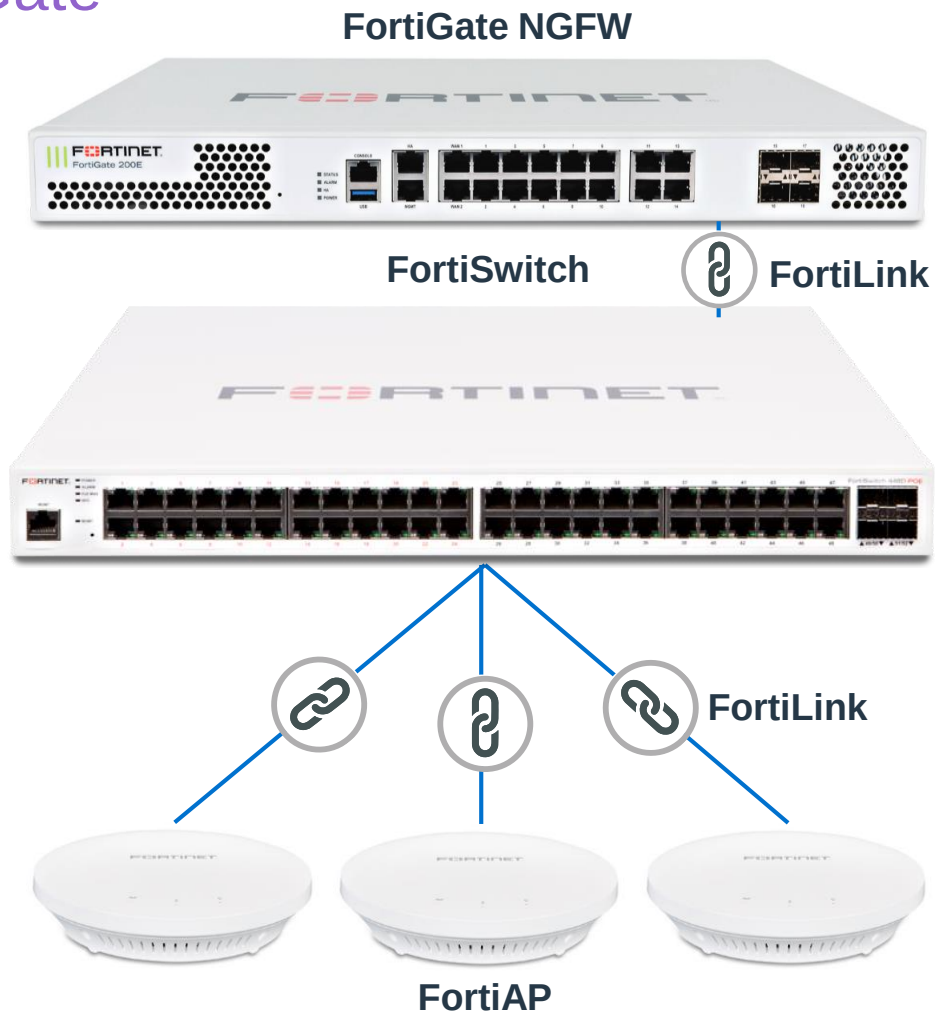
Простота управления

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

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



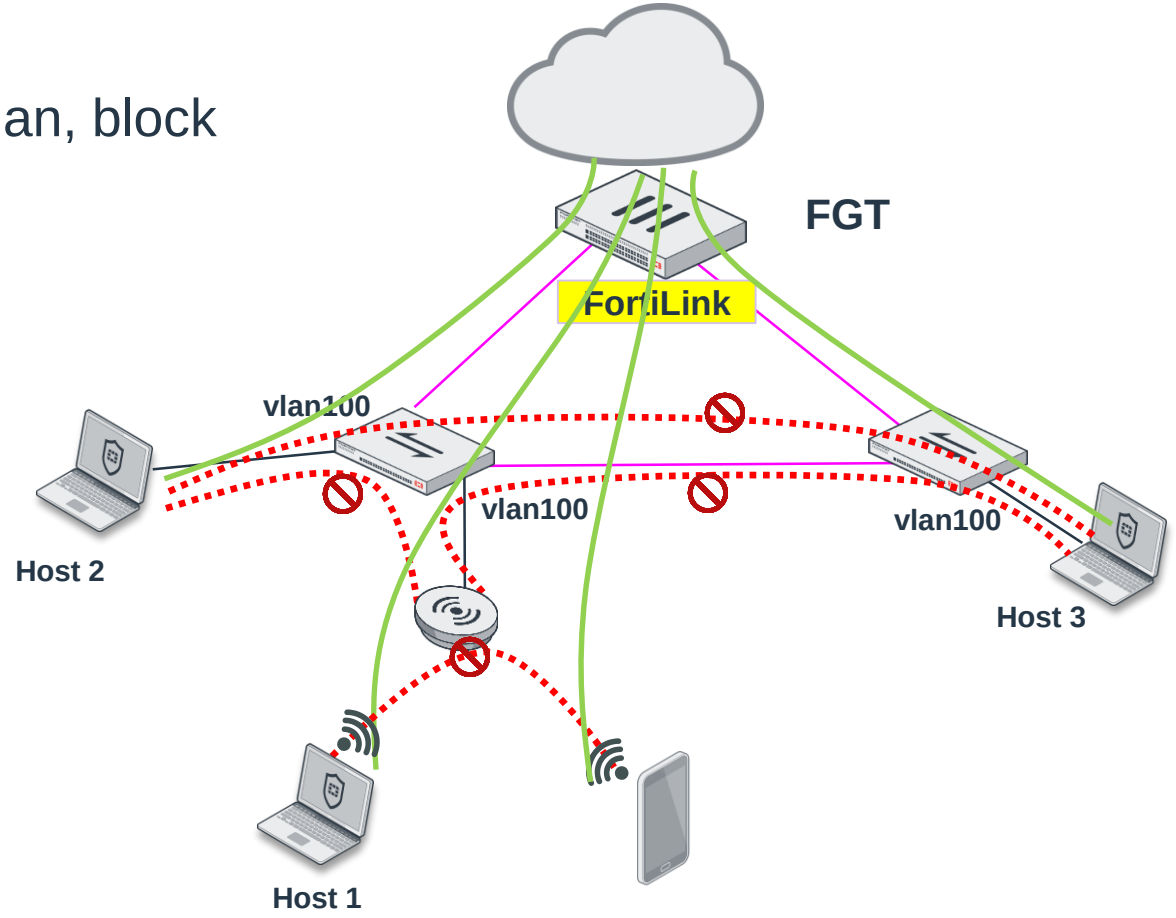
Zero-Trust Network Access

Микросегментация в пределах широковещательного домена

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

в одном широковещательном домене (access vlan, block intra-ssid)

- **Скомпрометированные хосты не могут инфицировать остальных**
- Дополнительная безопасность на уровне доступа:
  - Нет прямой коммуникации между хостами
  - Хост имеет связь только с FGT

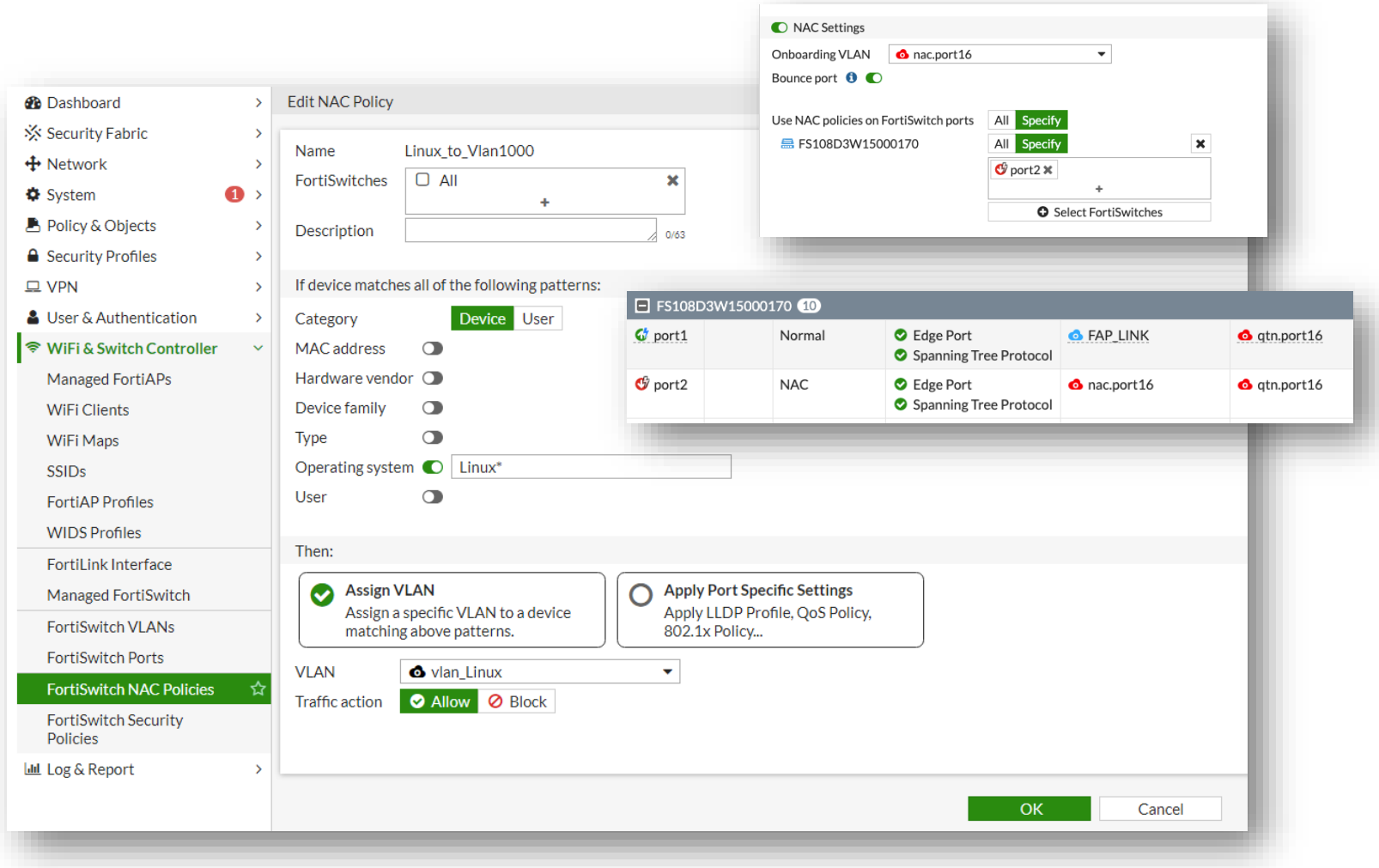


Zero-Trust Network Access

Встроенные возможности FortiSwitch NAC

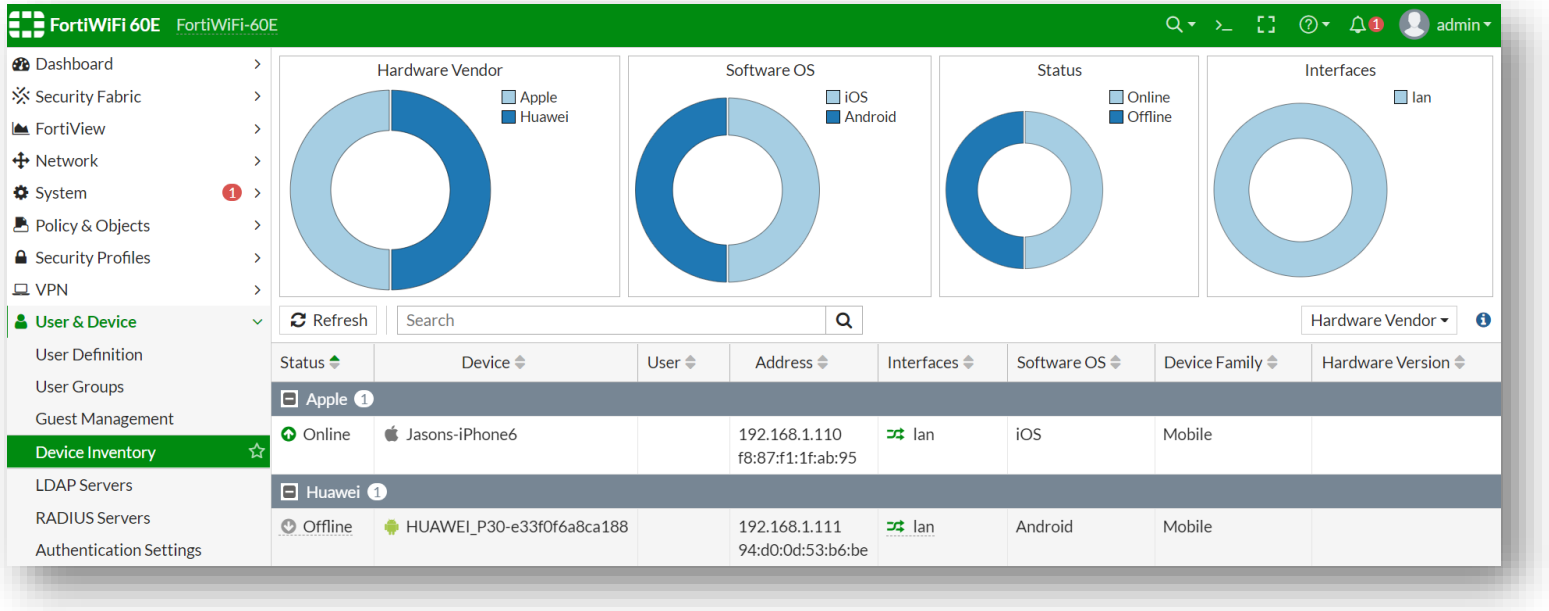
Устройство подключенное к определенным портам FortiSwitch будет помещено в предварительный VLAN (onboarding VLAN), для определения соответствия политикам NAC

- NAC может быть применен к определенному коммутатору и/или портам
- Режим Access на таких портах будет сменен с “Normal” на “NAC”, в том время как Native VLAN станет onboarding VLAN
- Поддержка различных способов проверки соответствия с возможностью
  - Назначения в определенный VLAN
  - Смены настроек на уровне порта (LLDP, QoS, 802.1x…)
- Подробности по устройству можно увидеть в NAC policy



Zero-Trust Network Access

IoT Security service



Новый сервис (подписка) – позволяет FortiGate запрашивать серверы FortiGuard для получения большей информации о подключенном устройстве

- Работает в дополнение к локальной базе устройств (требуется сервисный контракт FortiCare), на этой стадии запрашивается информация только о неизвестных устройствах
- Доступна как часть Enterprise и 360 bundle, или может быть приобретена по отдельности

Zero-Trust Network Access

Поддержка разгрузки детекции устройств на FortiSwitch

FortiSwitch помогает в обнаружении IoT путем захвата данных для нового сервиса IoT

Обеспечивается более точное обнаружение IoT так как не весь сетевой трафик может передаваться через FortiGate

- Помогает снизить загрузку FortiGate в отношении обнаружения устройств
- Периодически сканирует MAC адреса в локальной таблице MAC, может вызывать автоматический перехват трафика (sniffer scan)
- Перехваченный трафик отправляется на FortiGate для дальнейшей обработки. Перехваченный трафик с FortiGate направляется в облачный сервис FortiGuard service for IOT для сигнатурной идентификации и направления результатов обратно на FortiGate для обогащения локальной базы данных устройств результатами запроса в IoT Service.

```
FGT_A (global) # config switch-controller system
FGT_A (system) # get
iot-weight-threshold: 80
iot-scan-interval   : 30
iot-holdoff         : 5
iot-mac-idle        : 1440
```


AI-driven
Security Operations
Автоматическое обнаружение, предотвращение,
реагирование на киберугрозы

AI-driven Security Operations

FortiOS 6.4

Новые возможности в интеграции

- ATP

- SOAR

- SIEM

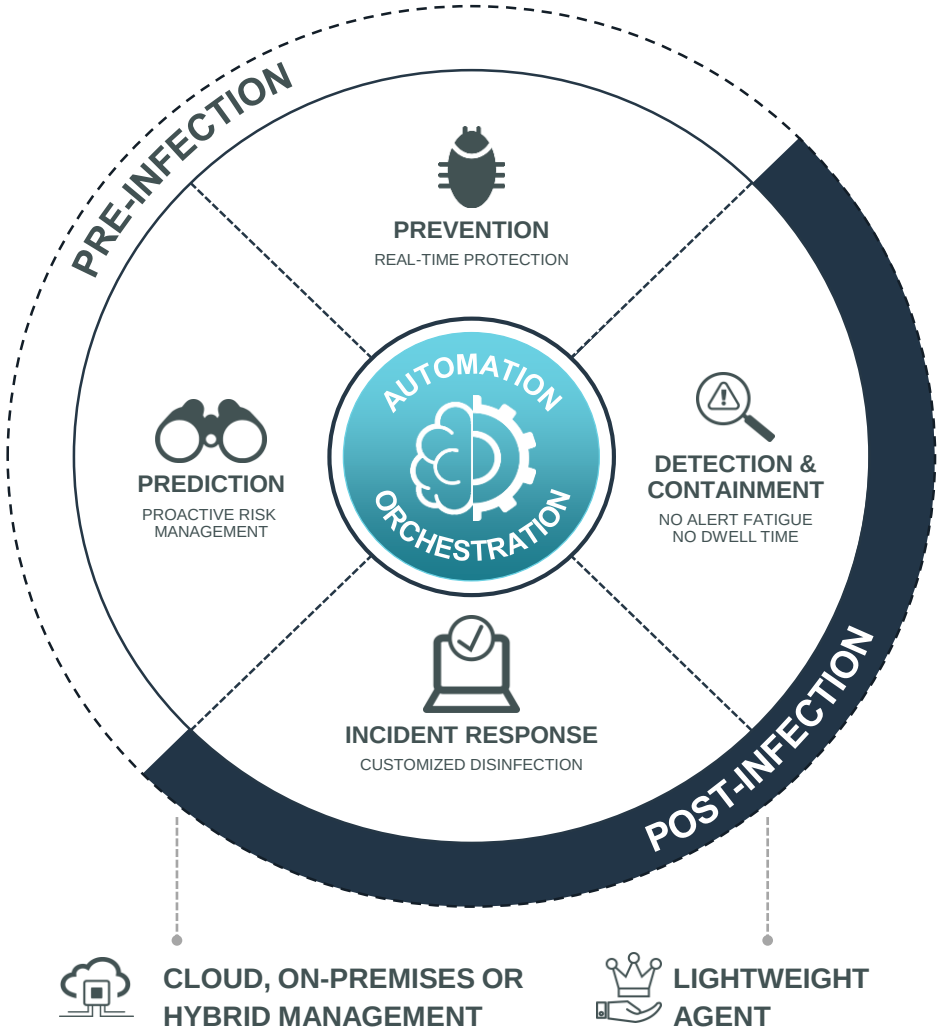
Расширение ISDB включает известные списки Mac Address

Новый сервис FortiSoC – встроенные возможности SOAR / SIEM в FortiAnalyzer 6.4

AI-driven Security Operations

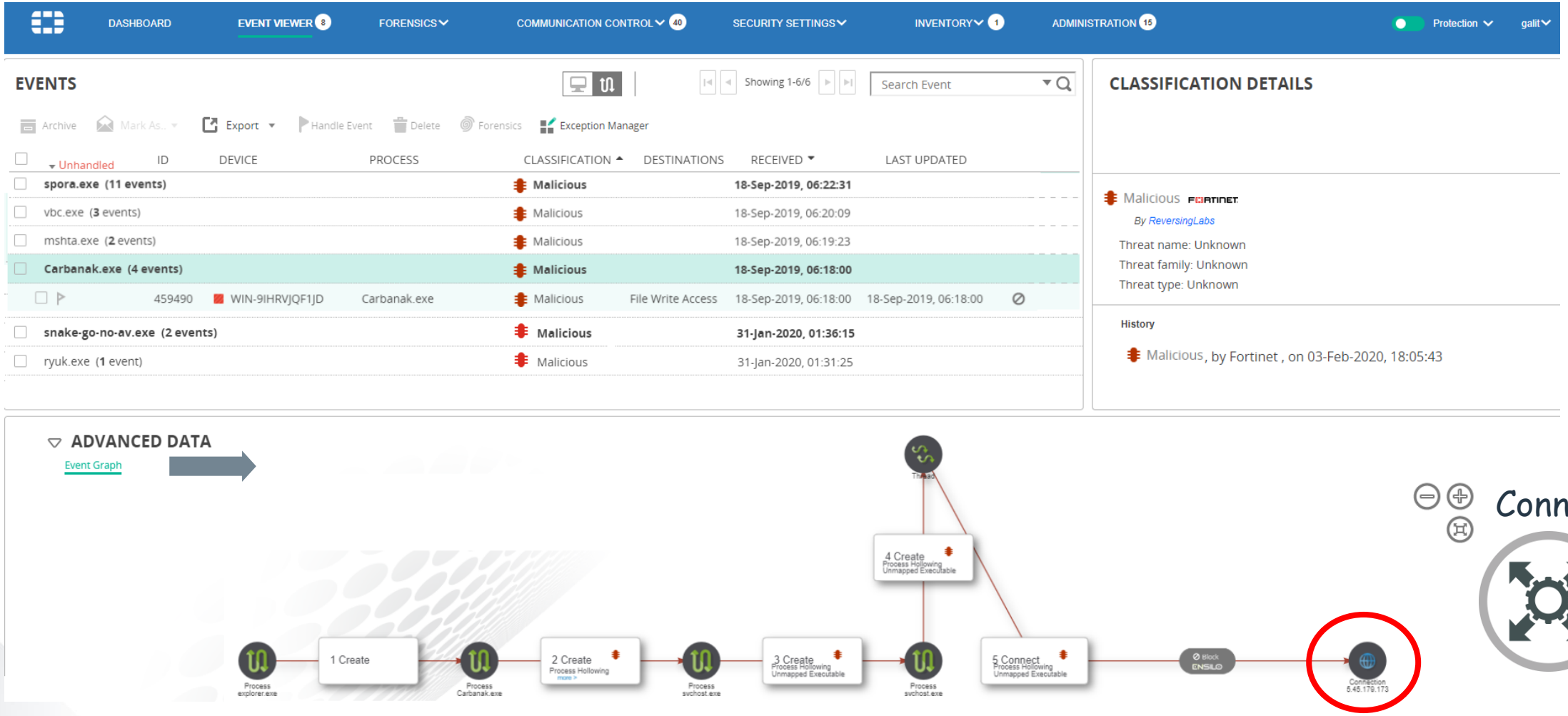
Интеграция FortiGate с FortiEDR (планируется)

- Коннектор FortiEDR позволяет поделиться данными Endpoint threat intelligence и информацией о приложениях с FortiGate.
- Модуль управления FortiEDR может проинструктировать FortiGate на выполнение определенных действий, таких как блокировка IP адресов для предотвращения подключения атакованного хоста к злоумышленнику.



AI-driven Security Operations

Интеграция FortiGate с FortiEDR (планируется)

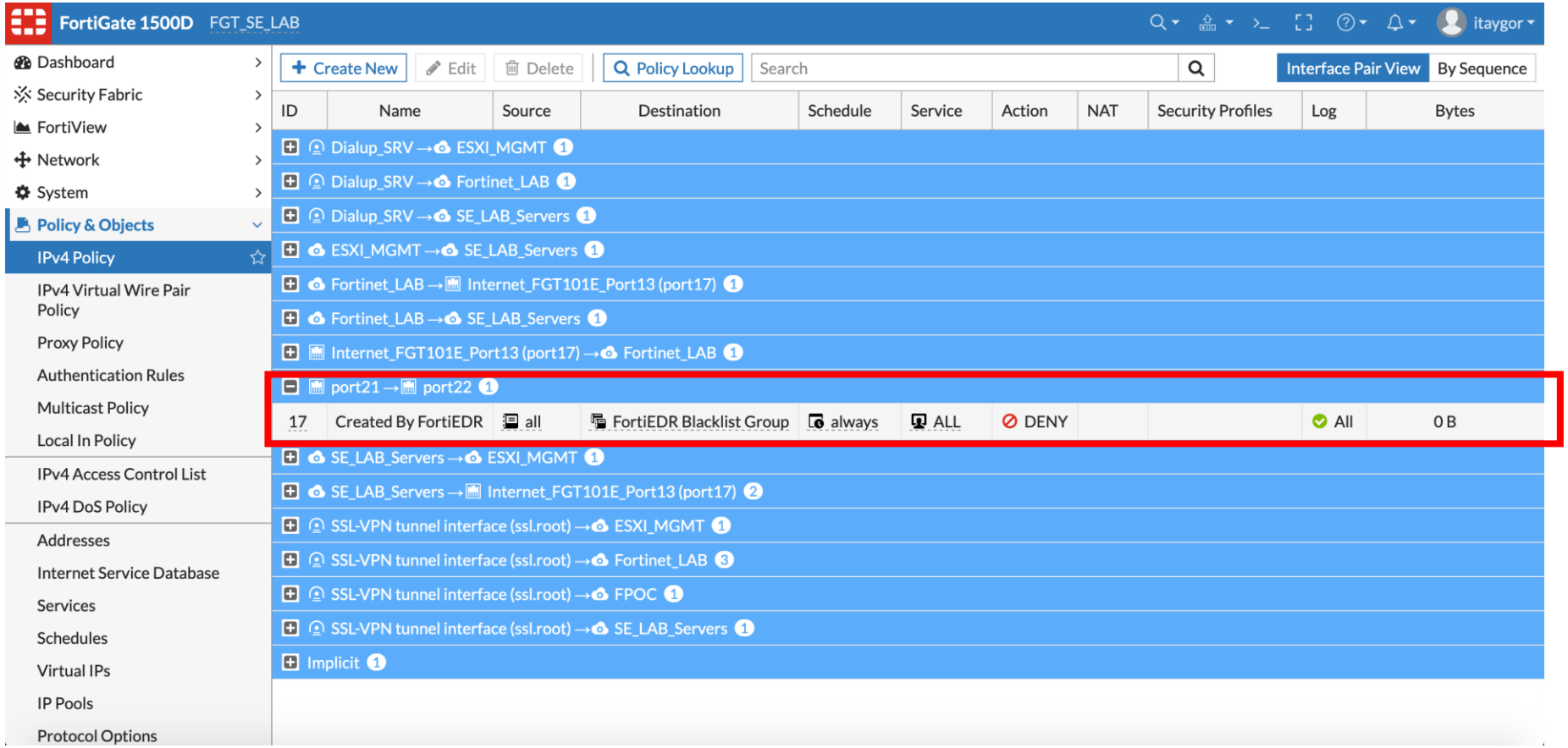


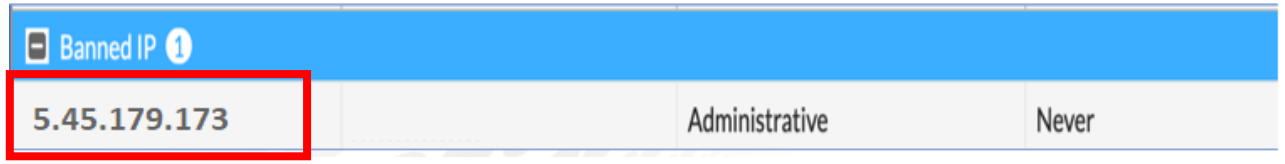
AI-driven Security Operations

Интеграция FortiGate с FortiEDR (планируется)

Connector

IP: 5.45.179.173



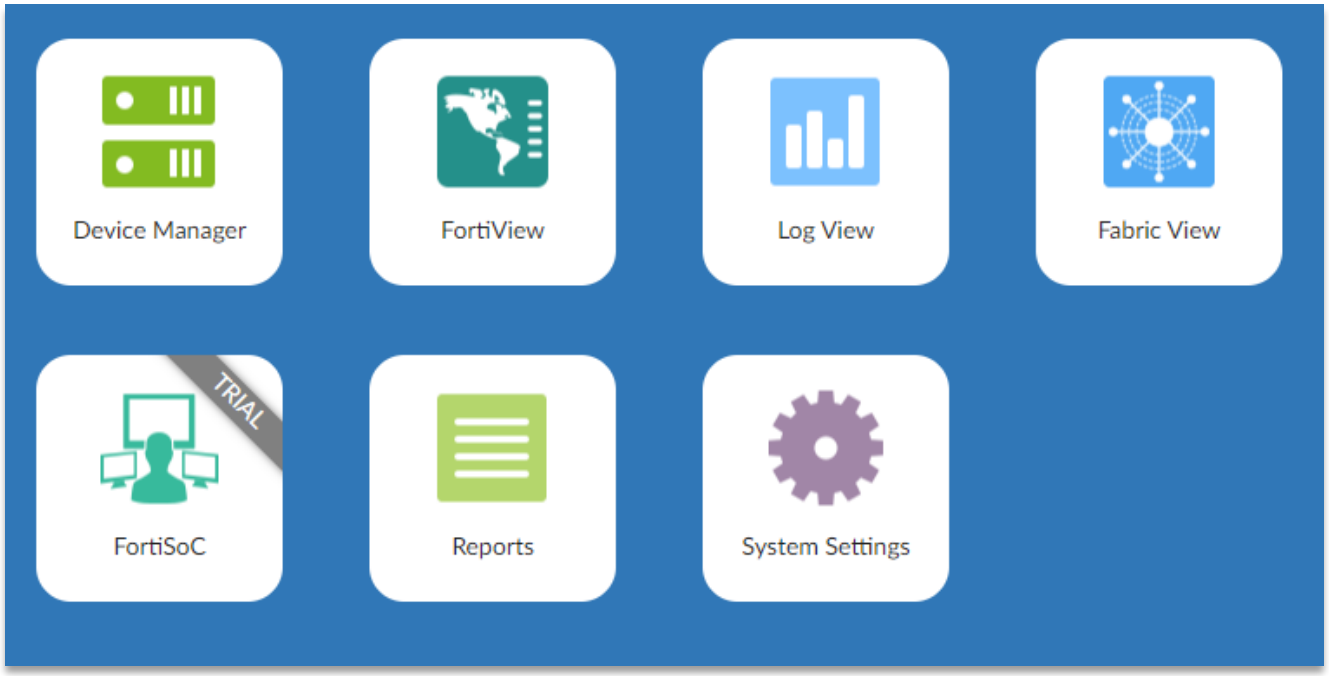


AI-driven Security Operations

Новый сервис FortiSoC в FortiAnalyzer 6.4

FortiSoC – новый сервис, включающий возможности оркестрации событиями безопасности, автоматизации и реагирования (SOAR) и возможности SIEM в FortiAnalyzer 6.4

- Лицензируется по модели подписка (subscription)
- SIEM-компонент FAZ автоматически разбирает (парсит), нормализует и коррелирует журналы с устройств Fortinet и журналы безопасности с хостов Windows / Linux (при интеграции с Fabric Agent) без ручного вмешательства администратора
- Логи SIEM = Fabric Logs в инструменте Log View

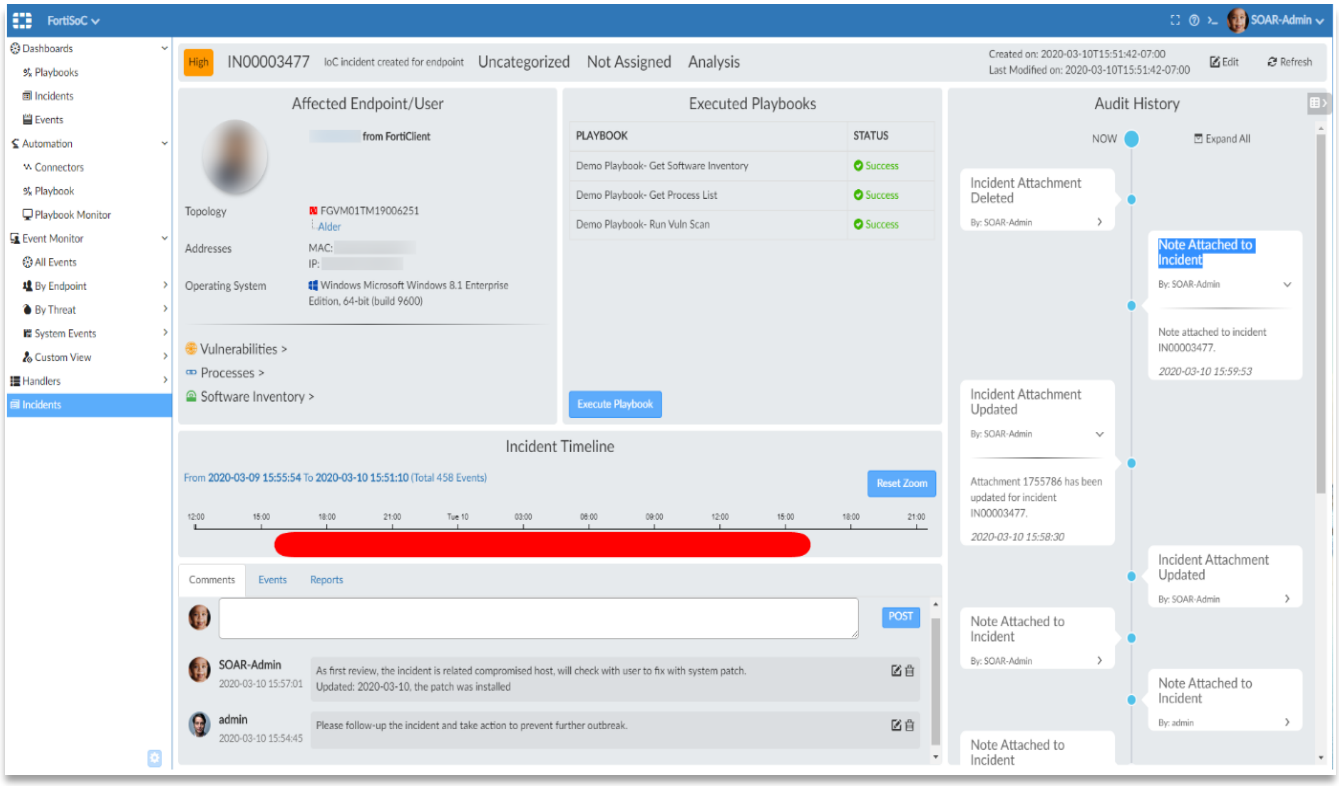


AI-driven Security Operations

Новый сервис FortiSoC в FortiAnalyzer 6.4

FortiSoC включает в себя управление инцидентами с возможностями по автоматизации для ускорения реакции на инциденты. Автоматизация задач в FortiSoC базируется на создании и использовании playbook, которые связываются с определенными триггерами срабатывания и последовательностью автоматических действий:

- Для работы необходима активная подписка
- Есть предопределенные шаблоны Playbook
- Возможно создавать свои Playbook на основе шаблонов и полностью с нуля (from scratch)
- Fabric Connector позволяют выполнять задачи на подключенных FortiGate и FortiClient EMS

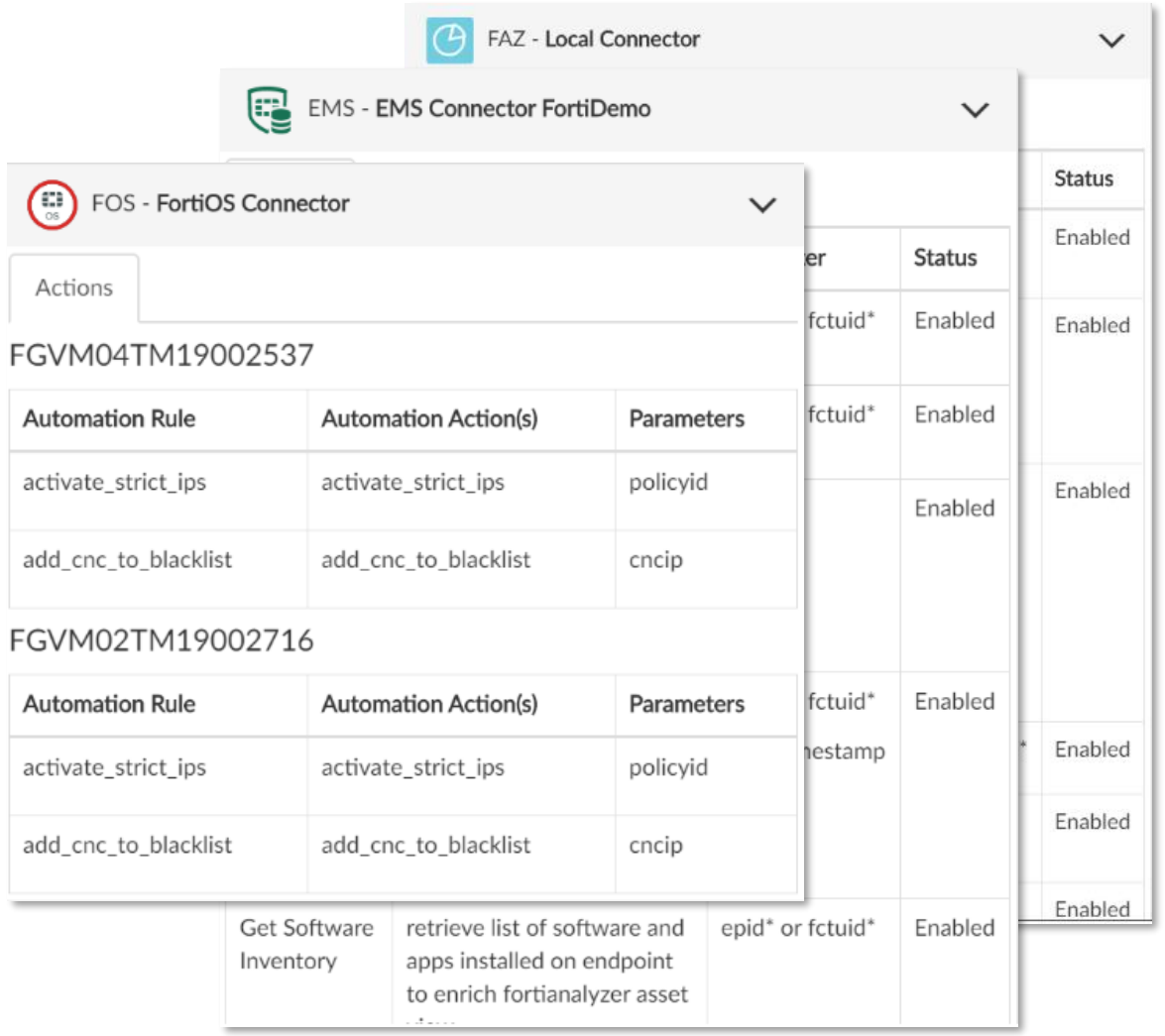


AI-driven Security Operations

Новый сервис FortiSoC в FortiAnalyzer 6.4 – автоматизация с помощью Playbook

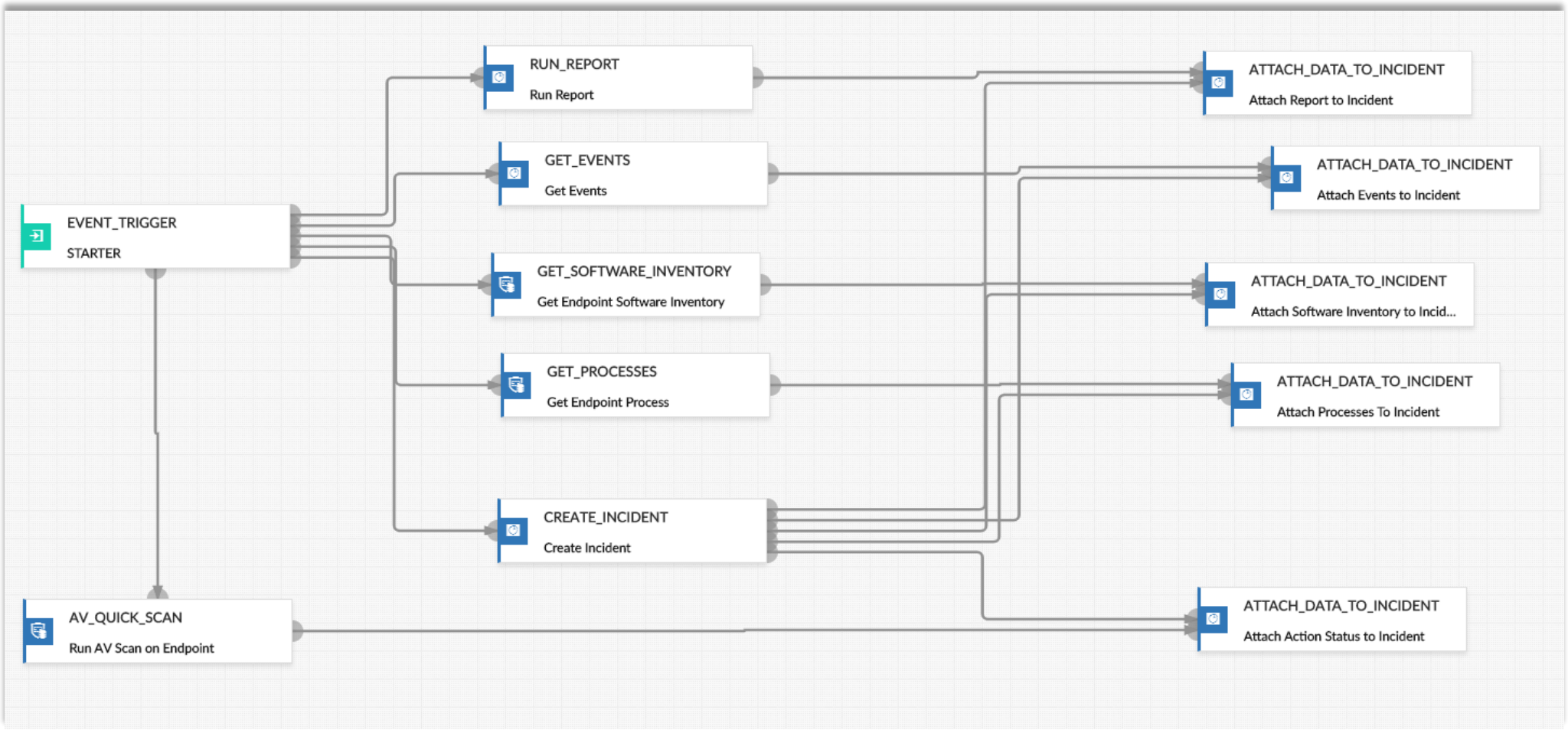
Playbook – набор действий автоматизации в одном сценарии, которые могут выполняться вручную либо автоматически, состоит из

- Триггера срабатывания (Incident, Event, Schedule, On-Demand)
- Набора действий автоматизации, который может использовать либо данные с триггера либо с предшествующих действий автоматизации. Действия могут быть выбираться из:
  - Локальных действий на FortiAnalyzer
  - Действия с коннекторов FortiGate (Automation Rule / Incoming Web Hook), FortiClient EMS



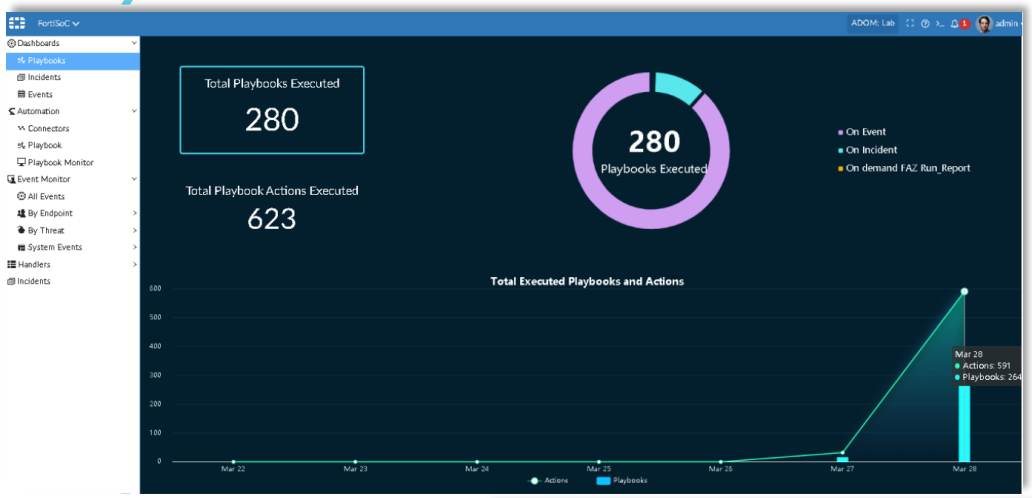
AI-driven Security Operations

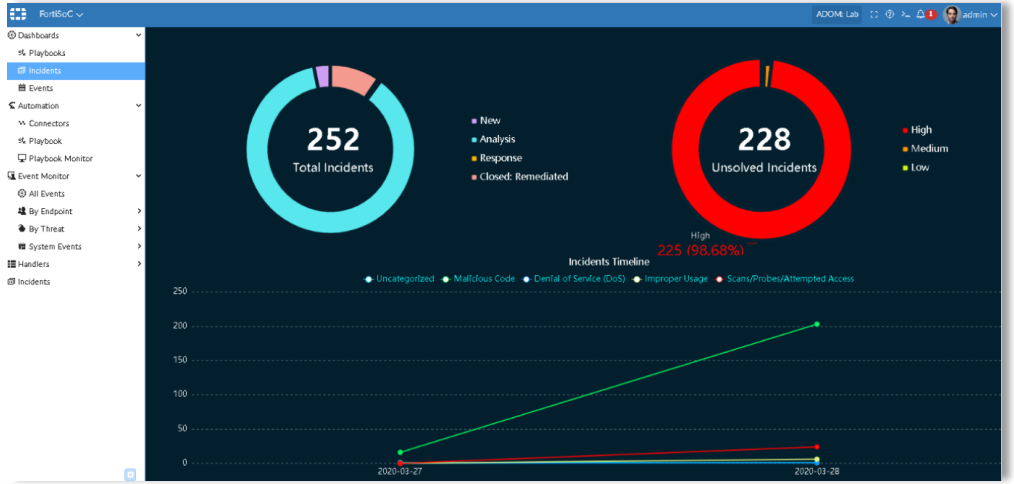
Новый сервис FortiSoC в FortiAnalyzer 6.4 – конструктор Playbook

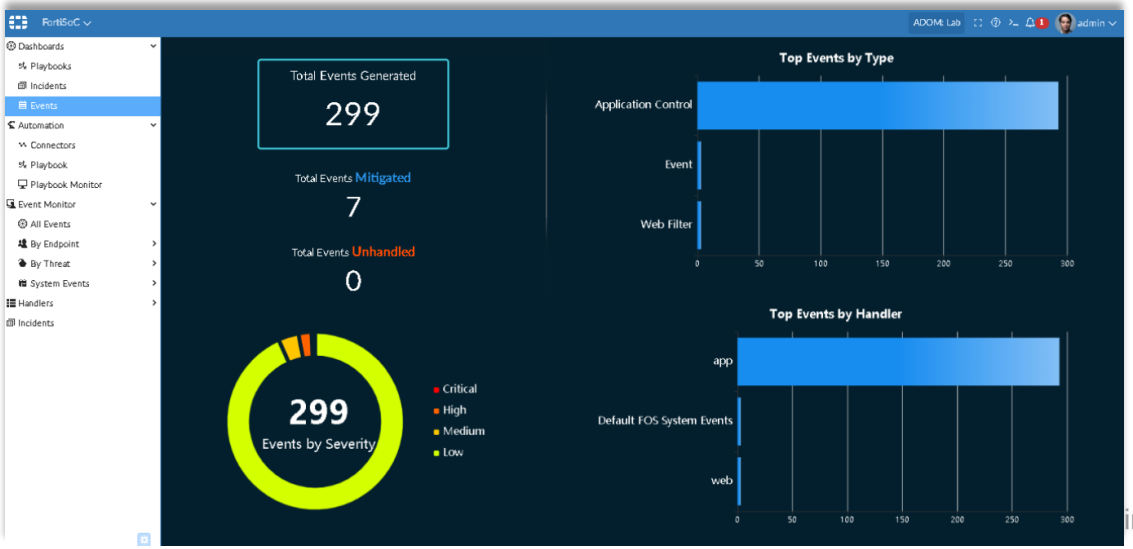


AI-driven Security Operations

Новый сервис FortiSoC в FortiAnalyzer 6.4 – Dashboards (Playbooks, Incidents, Events)







Лицензирование

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.4

	Threat Protection	Unified Threat Protection	Enterprise Protection	360
FortiManager Cloud				•
FortiAnalyzer Cloud				•
SD-WAN Overlay Controller VPN Service				•
SD-WAN Cloud Assisted Monitoring				•
SD-WAN Orchestrator Entitlement [2]				•
IPAM Cloud [2]				•
FortiConverter Service			•	•
FortiGuard IoT Detection Service [2]			•	•
FortiGuard Industrial Service			•	•
FortiGuard Security Rating Service			•	•
FortiGuard Anti-Spam Service		•	•	•
FortiGuard Web Filtering Service		•	•	•
FortiGuard Advanced Malware Protection (AMP) - Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard App Control Service	•	•	•	•
FortiCare (incl. Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, URL Whitelist DB)	*24x7*	*24x7*	*24x7*	*ASE [1]*
Bundles	**Threat Protection**	**Unified Threat Protection**	**Enterprise Protection**	**360**

FORTINET

Новые сервисы и лицензии

• FortiGuard IoT Detection

- Обеспечивает обнаружение устройств на FortiGate путем запроса в облачный сервис сигнатур IoT
- Доступен как по отдельности (standalone SKU), так включен в подписки ENT и 360 Bundles

• SD-WAN Orchestrator Entitlement

- Ежегодная подписка на каждый FortiGate, работающий под управлением модуля SD-WAN Orchestrator в FortiManager
- Доступен как по отдельности (standalone SKU), так включен в подписку 360 Bundle

• IPAM Cloud

- Обеспечивает возможность для FortiGate автомататически назначать диапазоны IP адресов с помощью DHCP для всех интерфейсов с ролью LAN в Security Fabric
- Доступен как по отдельности (standalone SKU), так включен в подписку 360 Bundle

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