Обзор возможностей системы централизованного управления FortiManager

Андрей Терехов

инженер

aterekhov@fortinet.com

Введение

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

Центр управления Security Fabric - архитектура

FortiManager

Упрощенное Развертывание

Центральное Управление

FortiAnalyzer

Аналитика Security Fabric

Отчетность Compliance

Автоматизация Администрирования

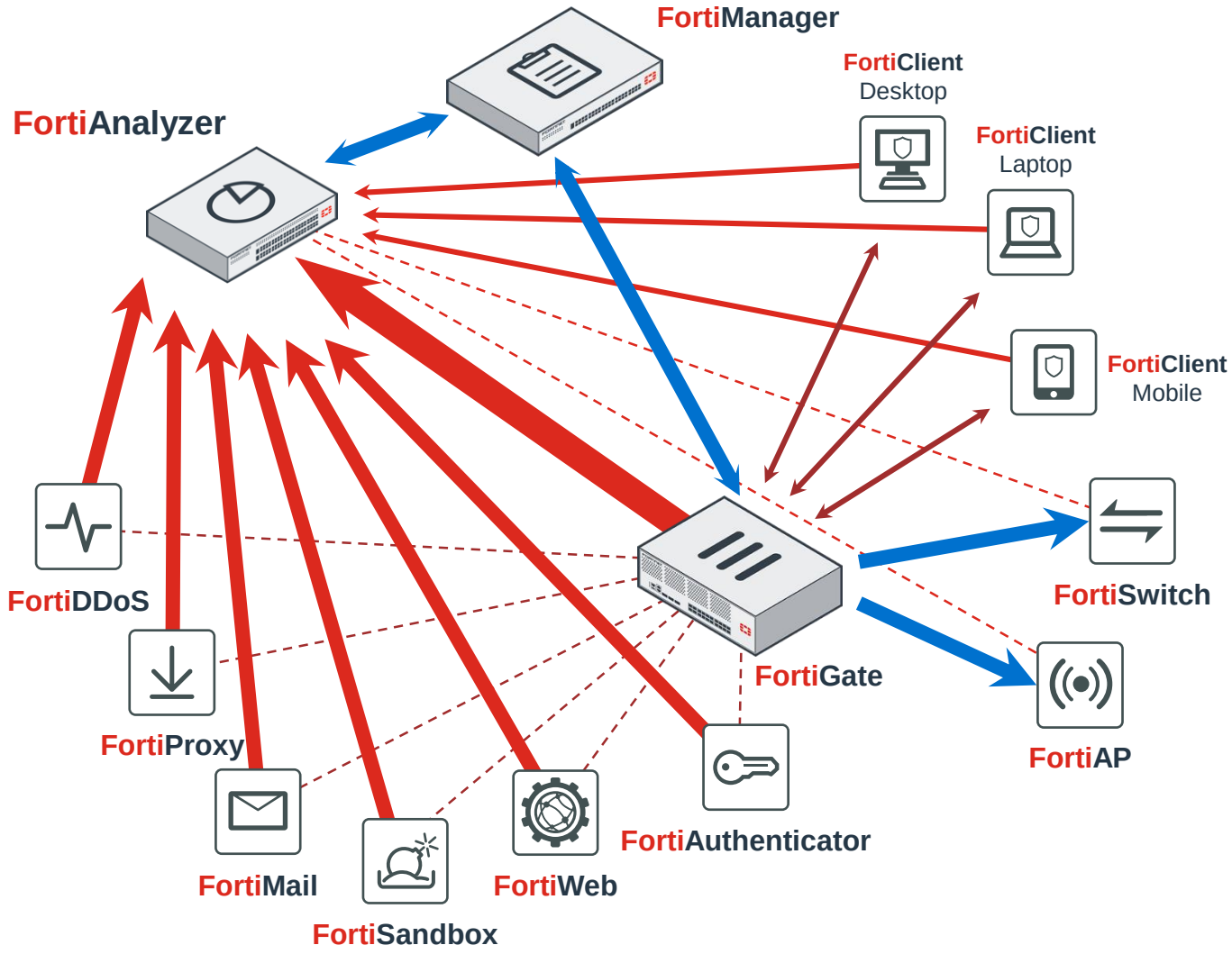
FortiManager & FortiAnalyzer

25K+ Пользователей

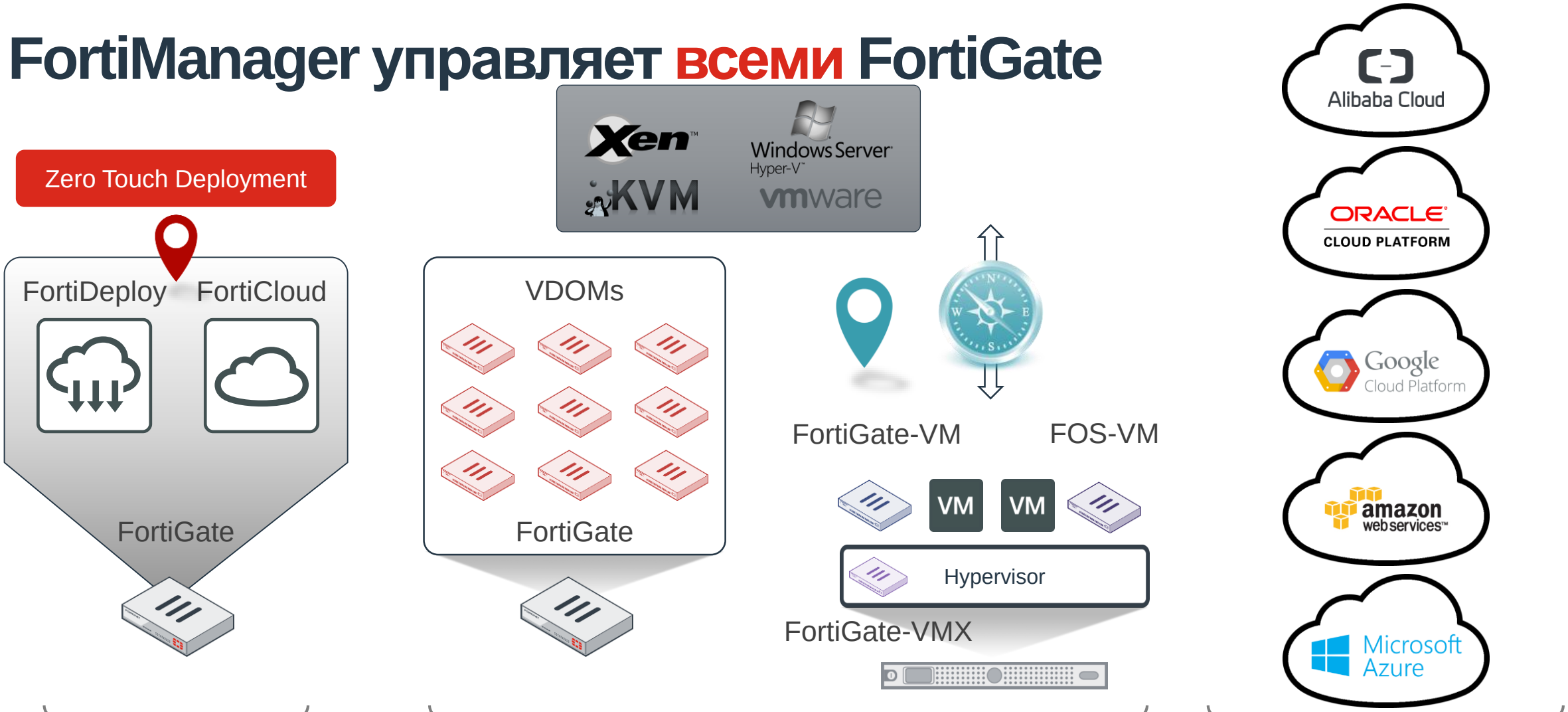
Gartner® Firewall & SD-WAN Магические Квадранты

ПАК | Виртуальная Машина | Облако | Безопасность как Сервис

Центр управления Security Fabric – схема взаимодействий

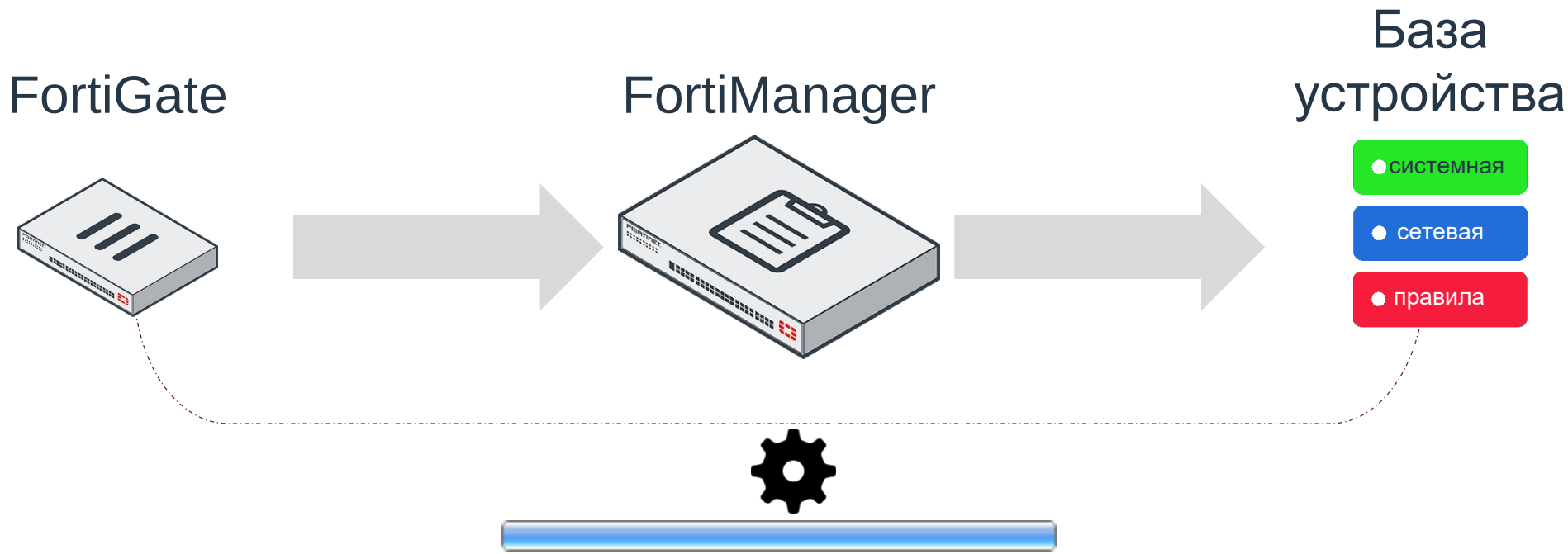


FortiManager управляет всеми FortiGate



FortiManager управляет всей конфигурацией FortiGate

Конфигурация: системная, сетевая, правила доступа



1. Упрощенное Развертывание

1. Упрощенное Развертывание

Легкий запуск в работу

Цели

Минимизировать трудозатраты и максимально задействовать существующий персонал

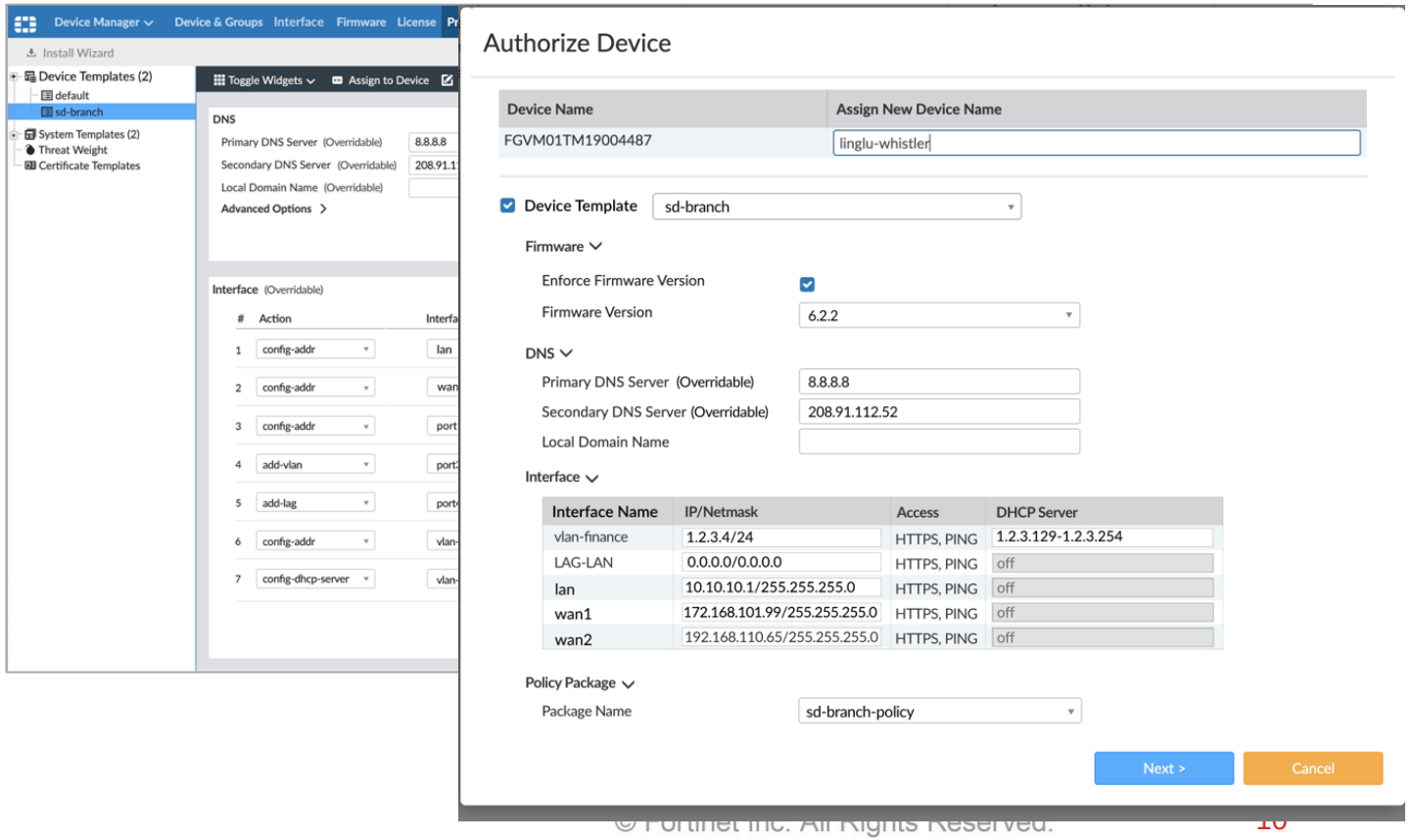
Ключевые возможности

- Простое развертывание за несколько минут (<6 по отчету NSS Labs)
- Шаблоны политик SD-WAN и NGFW
- Центральная консоль управления
- Сценарии работы и примеры для DevOps
- Журнал ревизий конфигурации и политик

Zero Touch Provisioning

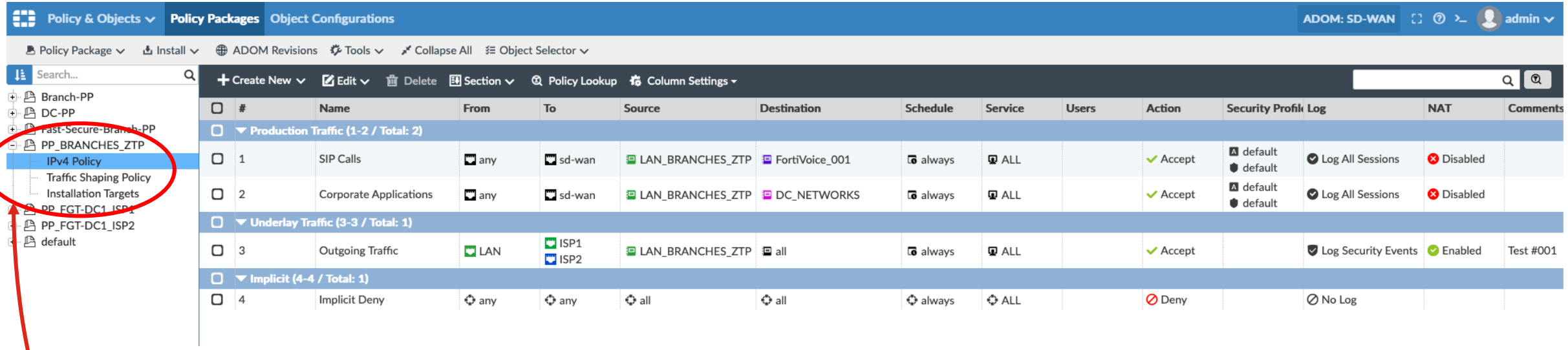
Расширения шаблонов для автоматизации развертывания

- Поддержка преднастройки интерфейсов
  - Настройка WAN/LAN интерфейсов
  - Конфигурация VLAN
  - Интерфейсы LAG
- Преднастройка статической маршрутизации и интерфейса SD-WAN (6.4.2)
- Шаблоны развертывания доступны при создании модели устройства



Повторно используемые объекты ZTP

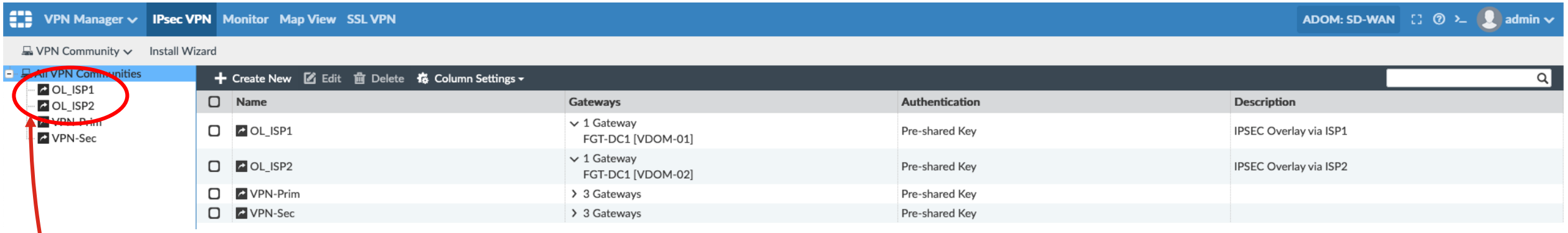
Policy Package (пакет политик и зависимые объекты)



Общий пакет Policy Package для всех ZTP шлюзов (настраиваемо)

Повторно используемые объекты ZTP

Настройки VPN

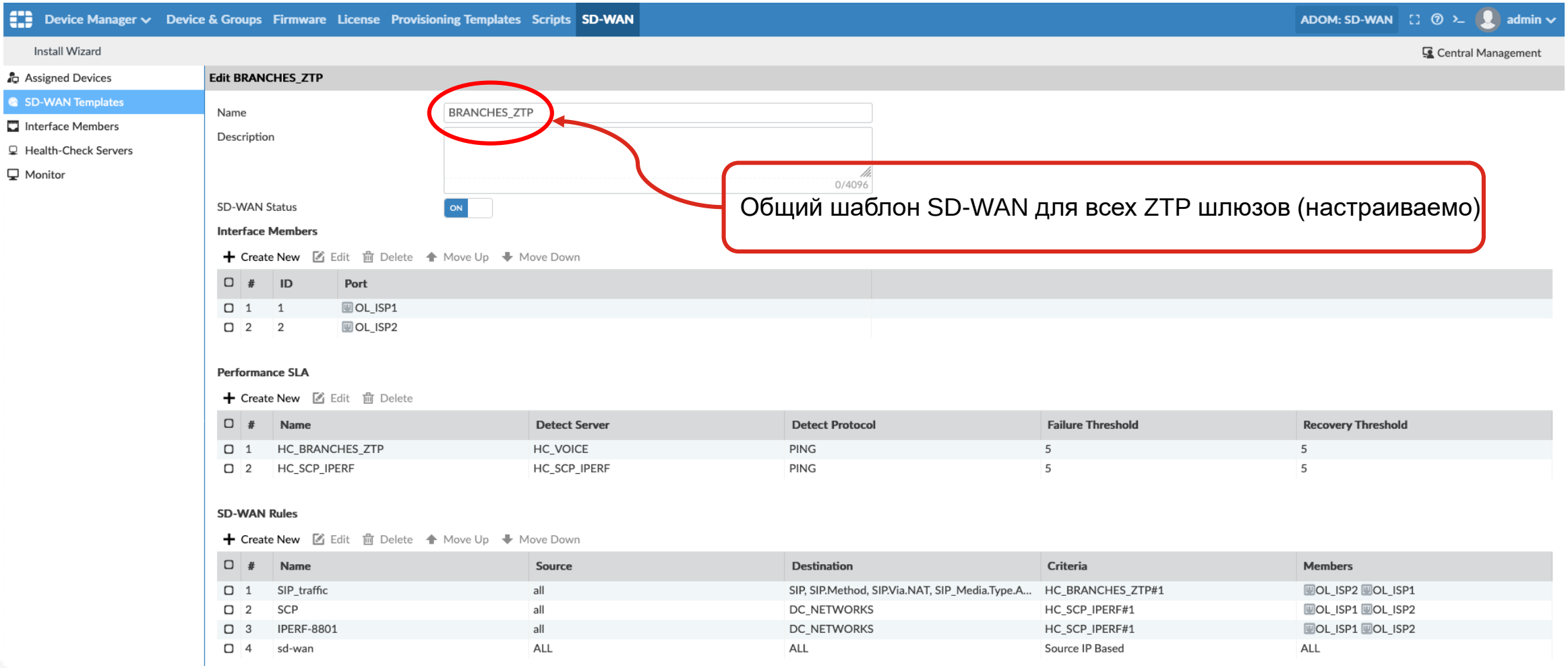


Общие топологии VPN для для всех ZTP шлюзов (настраиваемо)

- Начиная с 6.2.2 настройки можно назначить на группу устройств

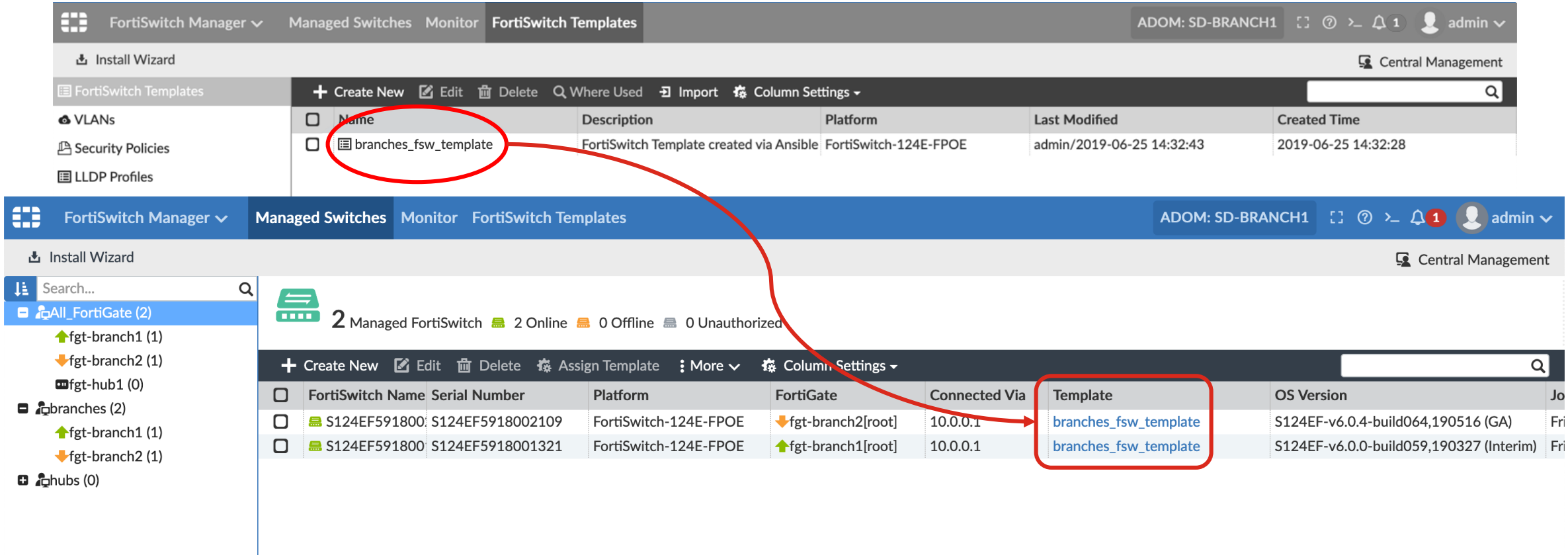
Повторно используемые объекты ZTP

Шаблон SD-WAN



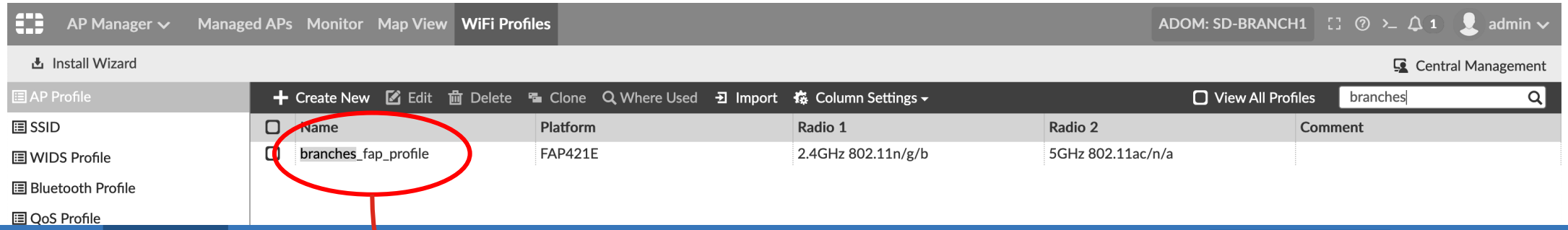
Повторно используемые объекты ZTP

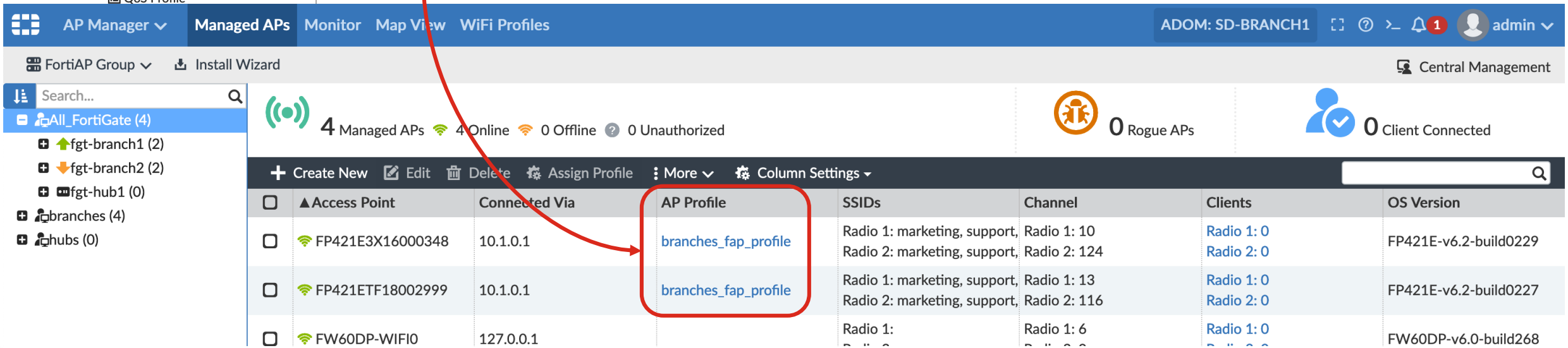
Шаблон настройки управляемых коммутаторов FortiSwitch



Повторно используемые объекты ZTP

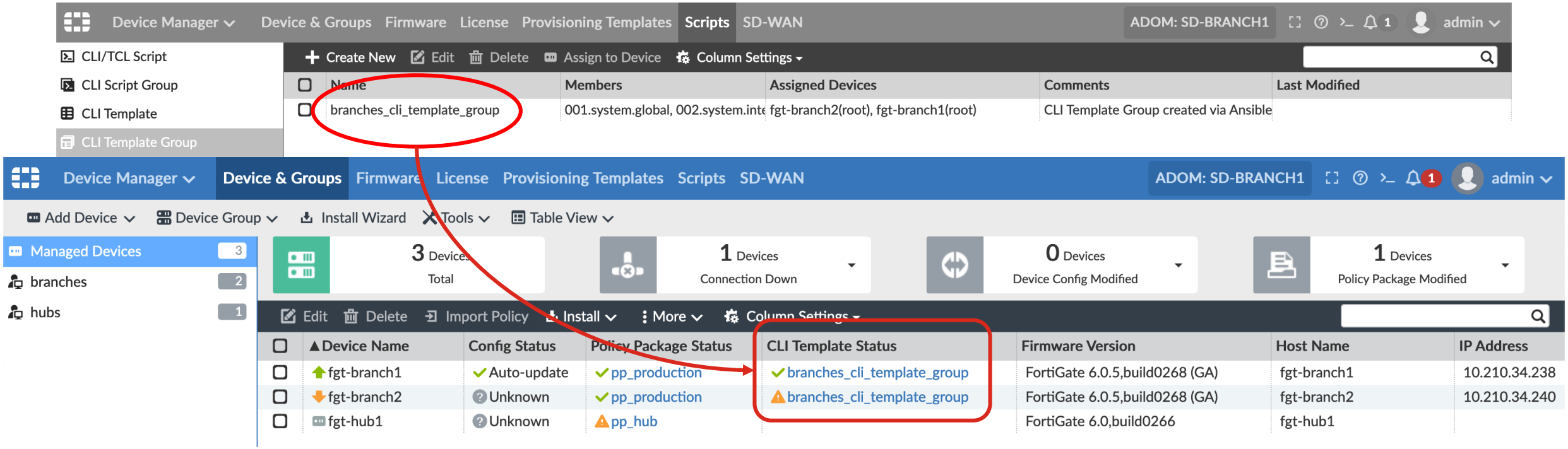
Шаблон настройки управляемых точек доступа FortiAP





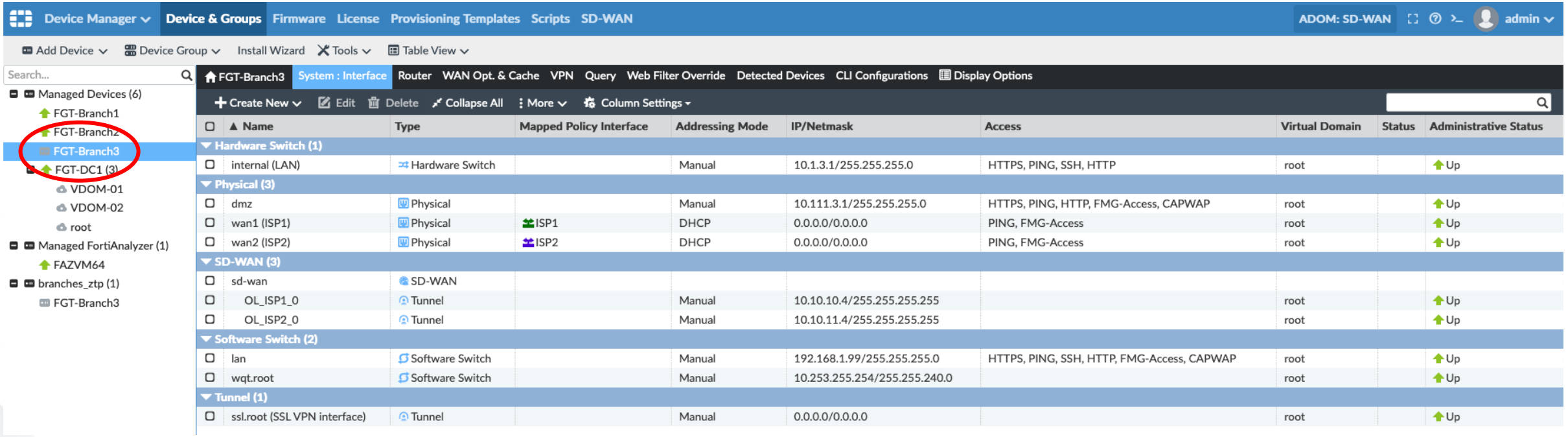
Re-Usable Object Example

Шаблон (или групп) типовых повторяемых настроек - CLI Template



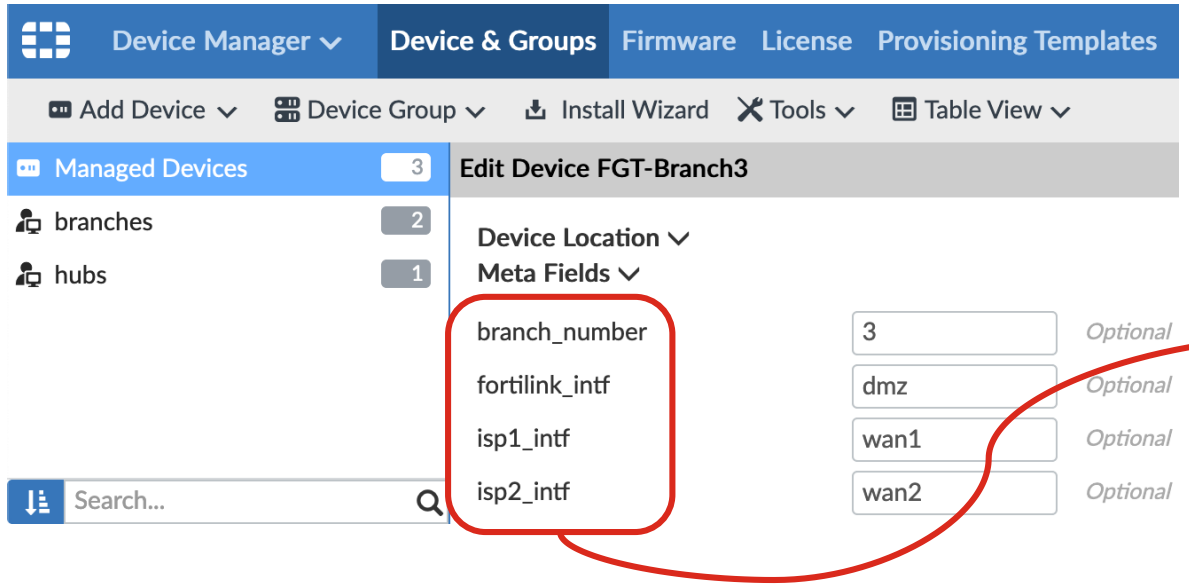
Ключевой элемент ZTP – модель устройства

- Ещё не развернутое и не настроенное устройство
- …которое можно заранее настроить в FortiManager в виде прототипа



Ключевой элемент ZTP – атрибуты модели

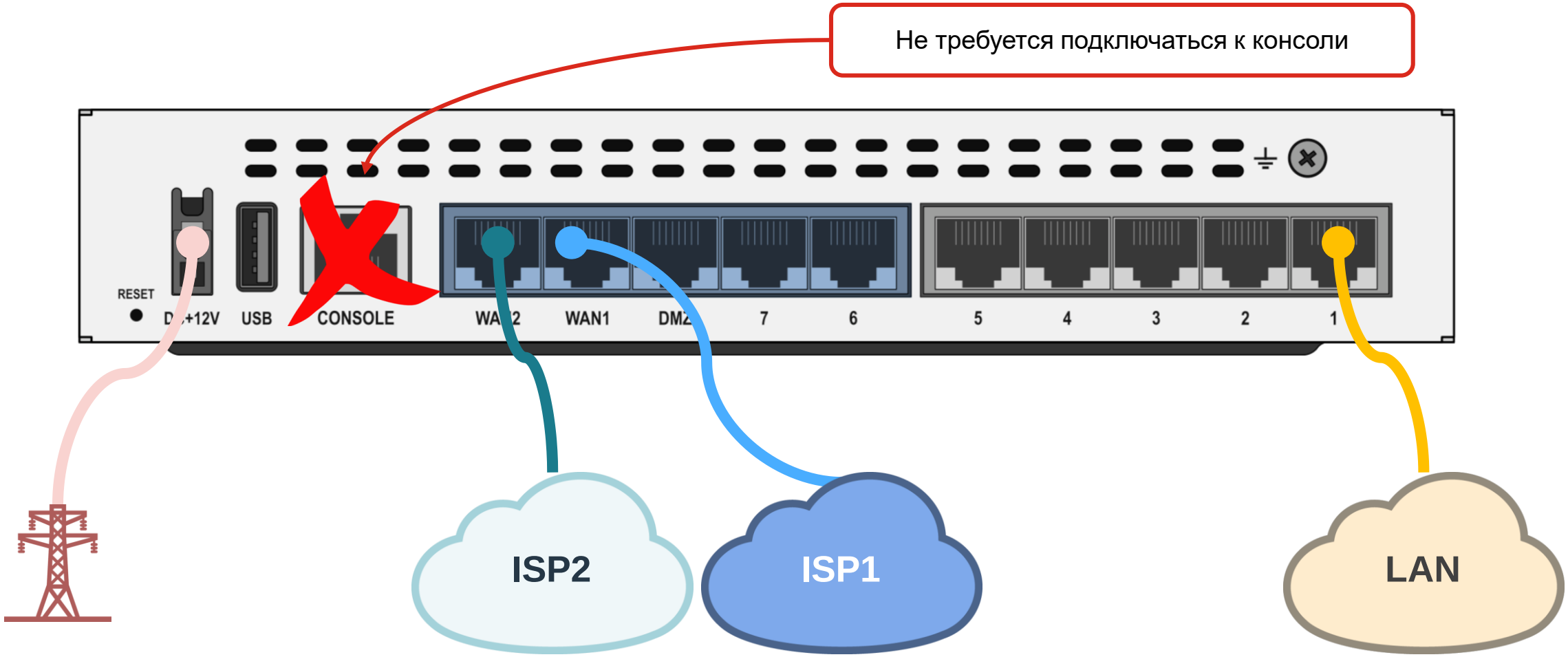
Взаимосвязь с CLI Template



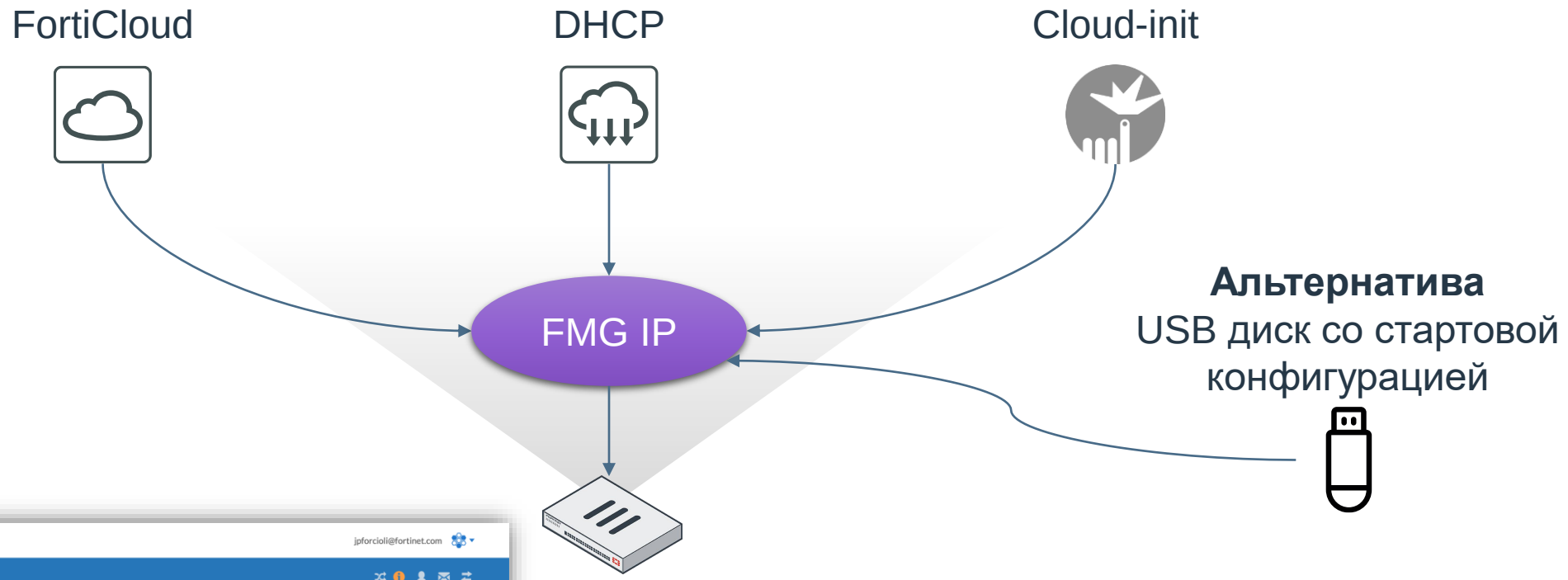

```
[…]
config system global
set timezone 28
set hostname FGT-Branch$(branch_number)
end

config system interface
edit $(isp1_intf)
append allowaccess https
next
edit $(fortilink_intf)
set ip 10.0.0.99 255.255.255.0
next
end

config firewall address
edit LAN_BRANCHES_ZTP
Set subnet 10.$(branch_number).0.0/24
next
end
[…]
```

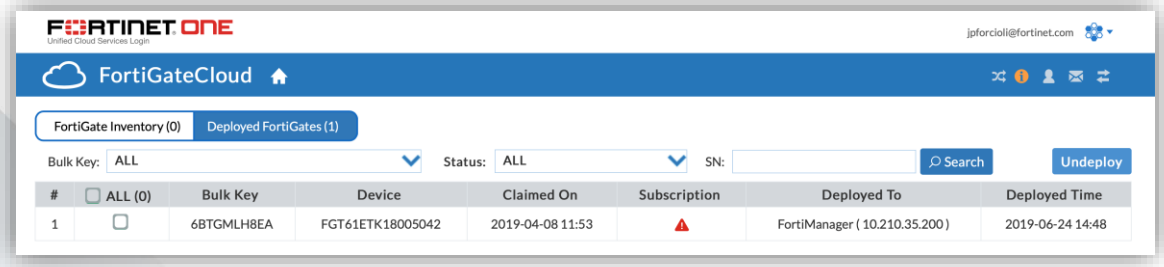
Процесс ZTP

Подготовка устройства – подключение интерфейсов



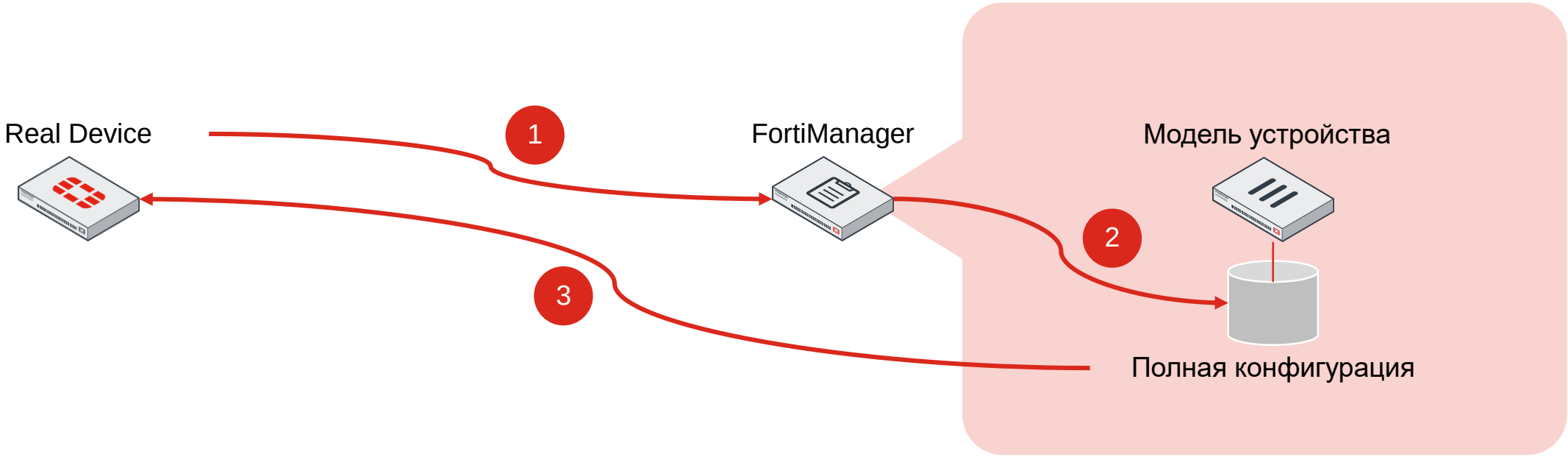
Процесс ZTP – определение адреса FortiManager





Процесс ZTP – автоматическая конфигурация

Auto-link Process



1. Устройство устанавливает защищенный канал
2. FortiManager находит подходящую модель (по номеру или секрету)
3. Auto-link процесс: FortiManager полную конфигурацию
   (опция - предварительно обновить ПО)

2. Центральное Управление

2. Центральное Управление

Простое масштабирование задач администрирования

Цели

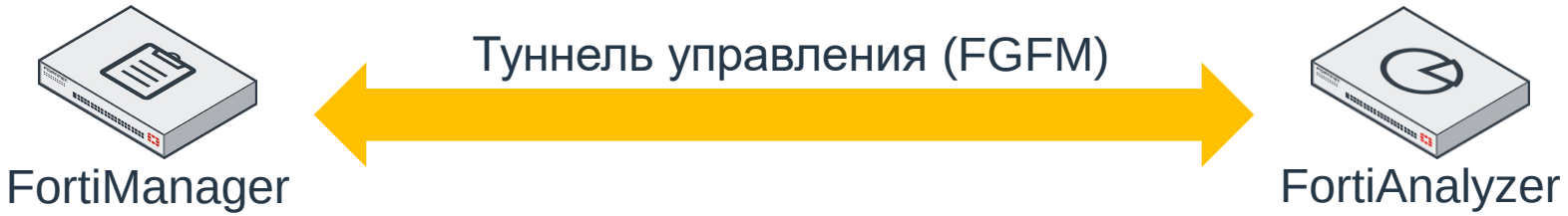
Снизить трудозатраты на администрирование за счёт использования единой консоли управления для различных задач

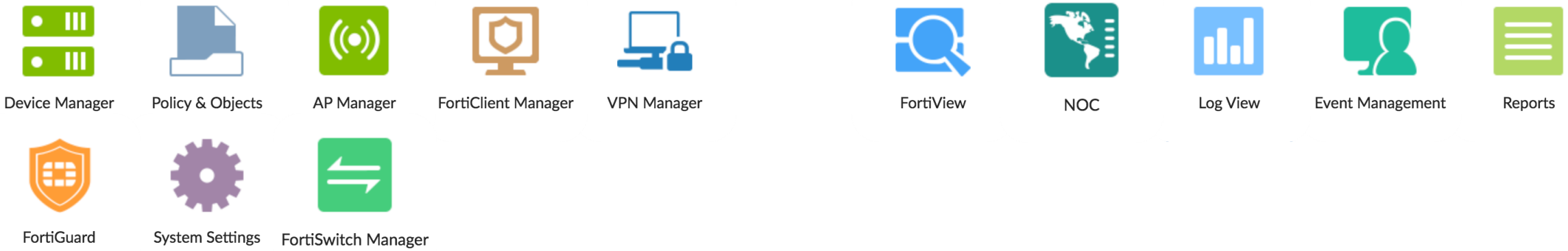
Ключевые Возможности

- Масштабирование до 100 тысяч FortiGate и выше
- Расширения управления Security Fabric
- Шаблоны политик SD-WAN и NGFW
- Централизованное журналирование и отчетность
- Ролевое разграничение доступа

Объединенная консоль управления и мониторинга

Единая панель управления для NOC и SOC





Объединенная консоль управления и мониторинга

FortiManager использует FortiAnalyzer API …

Расширенная консоль управления (6.4)

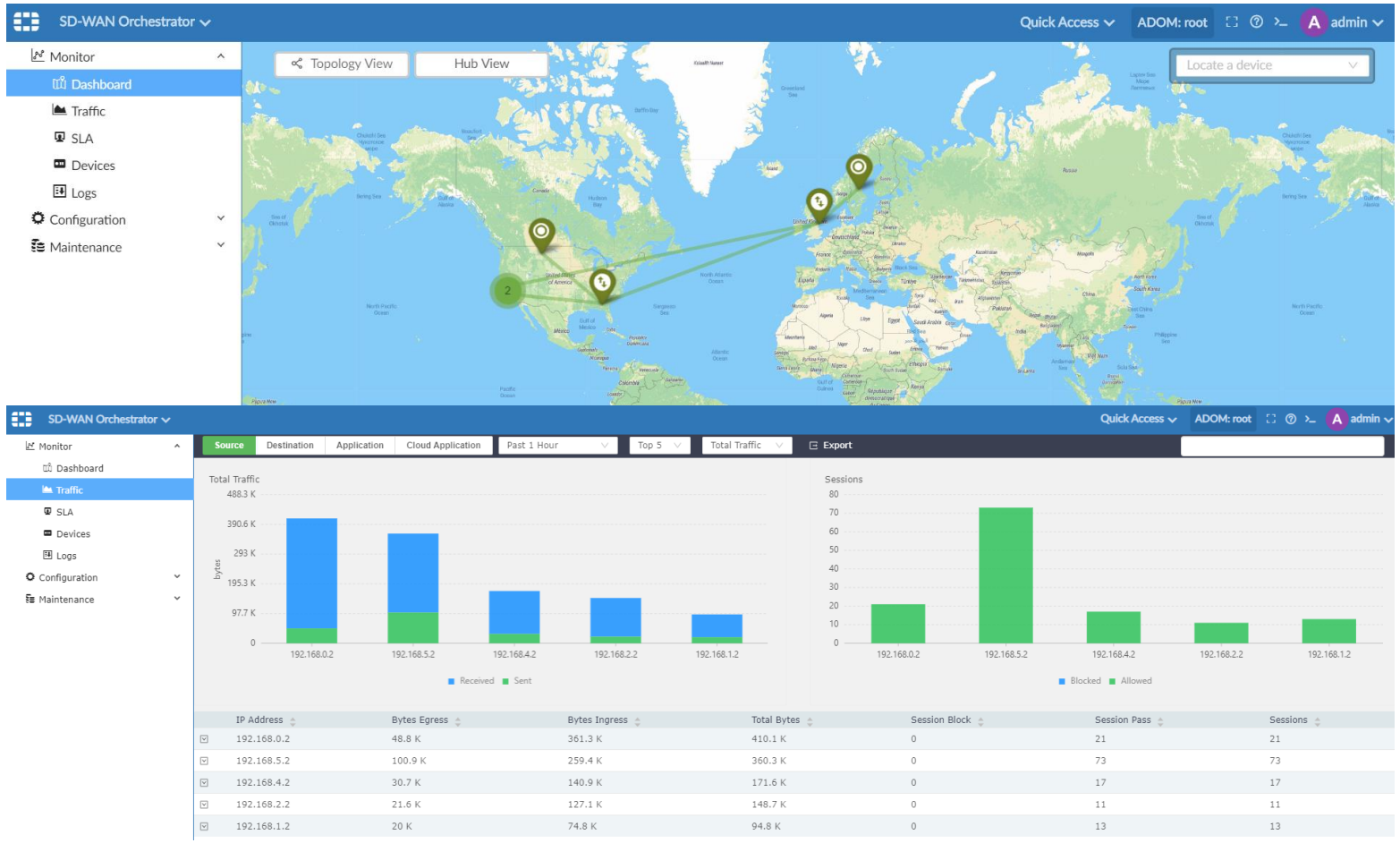
Возможность добавления расширенных возможностей управления

- Встроенный механизм для запуска контейнеров с расширениями возможностей управления
  - Только контейнеры от Fortinet (6.4)
  - Контейнеры загружаются в виде обновлений
  - Оповещение администраторов при возможности загрузки новых контейнеров
- Установка и удаление по запросу пользователей
- Может требоваться соответствующая подписка для использования некоторых контейнеров

FortiManager 6.4 – SD-WAN Orchestrator

Приложение для оркестрации SD-WAN

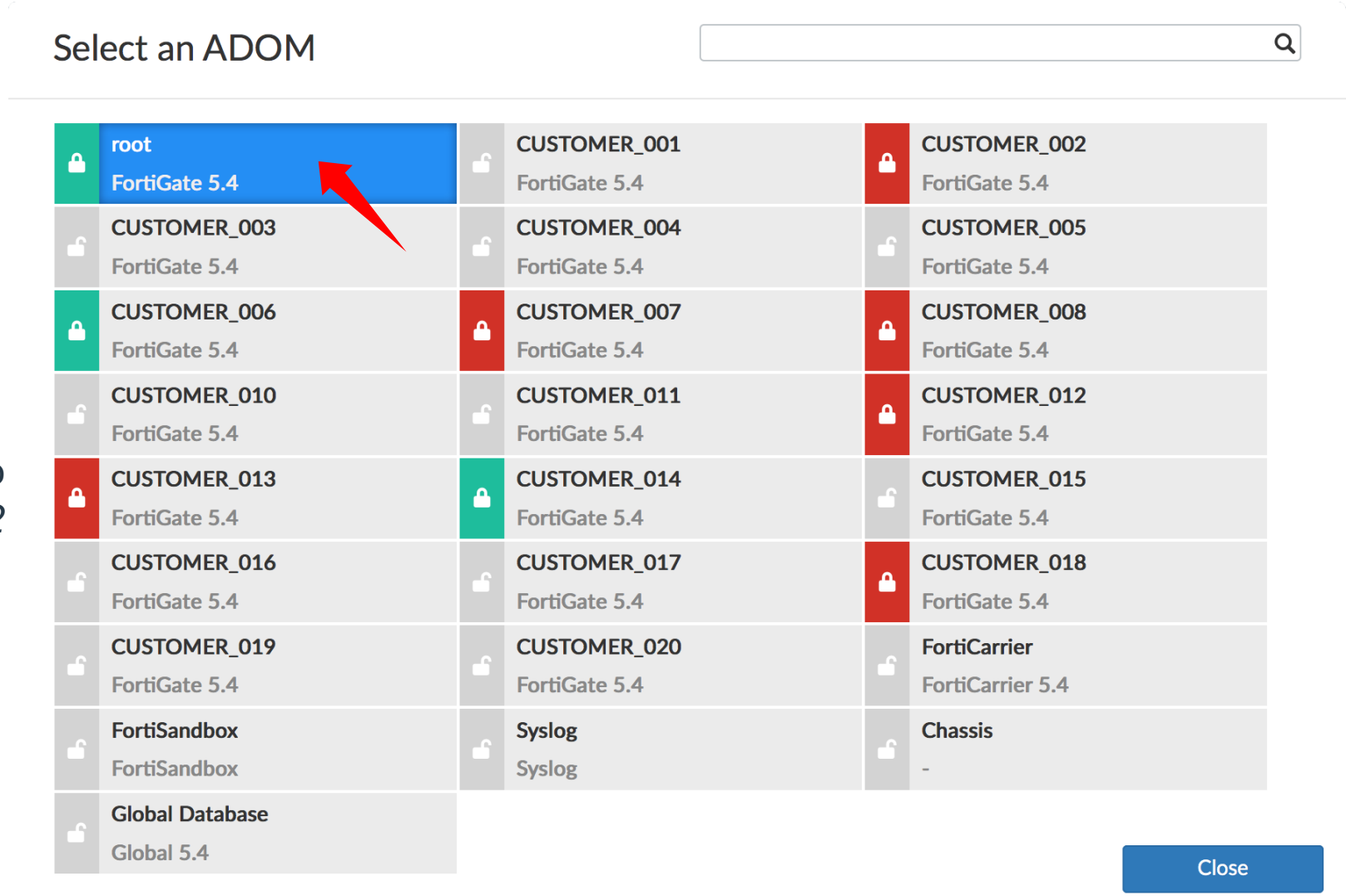
- Автоматизация типовых настроек и операций развертывания
- Конфигурация и мониторинг
- Требует подписки 360 на FortiGate
  - (все функции по управлению SD-WAN за пределами SD-WAN Orchestrator доступны без подписки)



Управление политиками – административные домены

Заблокировано MSSP: *admin1*

Заблокировано API: *user2*



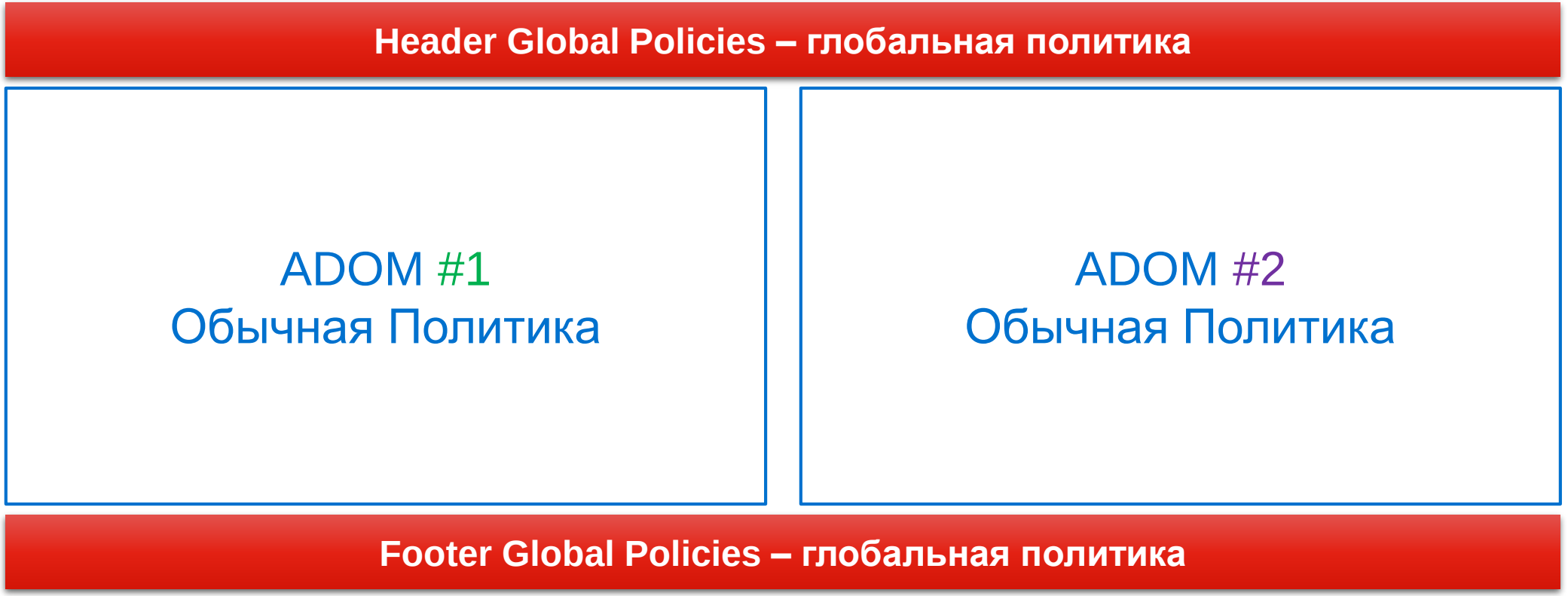
Заблокировано MSSP: *admin2*

Заблокировано CUSTOMER: *user1*

Заблокировано API: *user3*

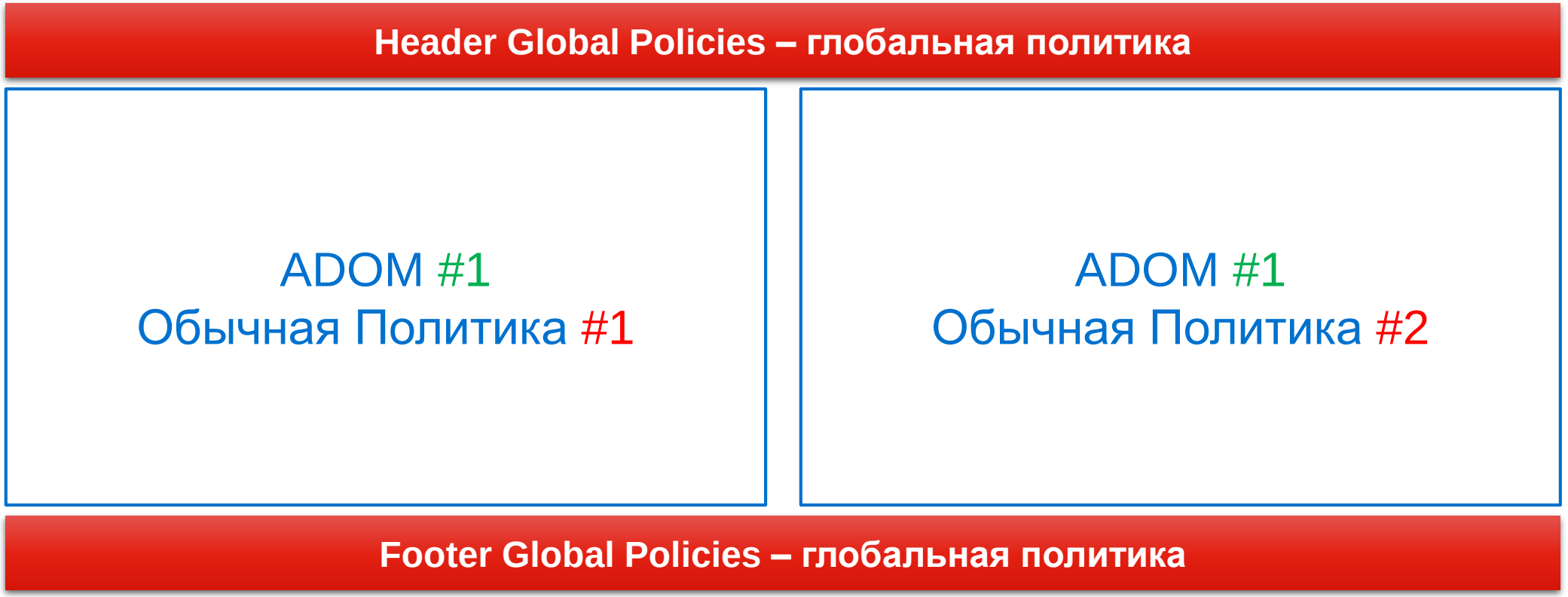
Управление политиками – глобальная политика

Глобальные политики



Управление политиками – общие фрагменты политики

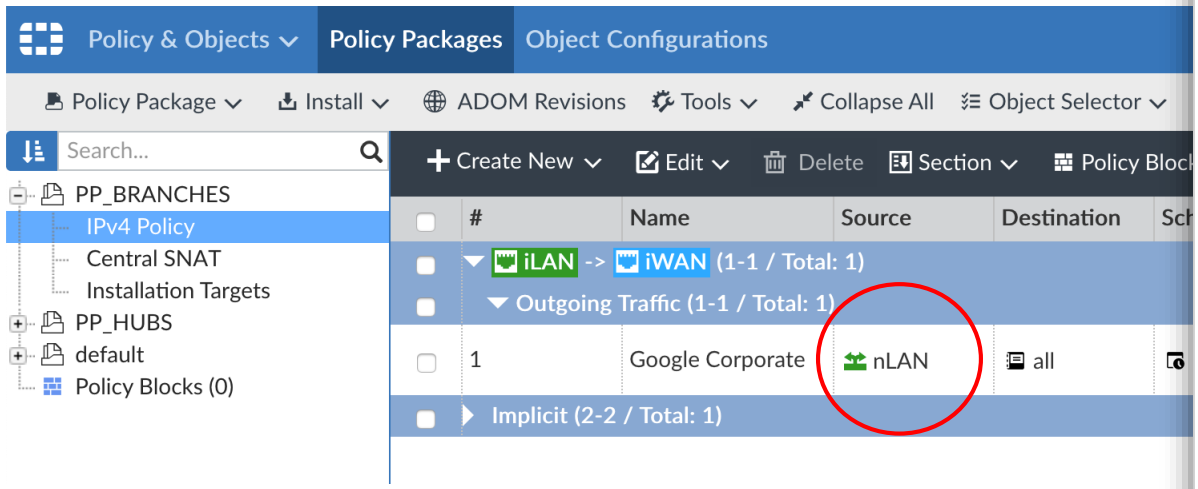
Блоки политик

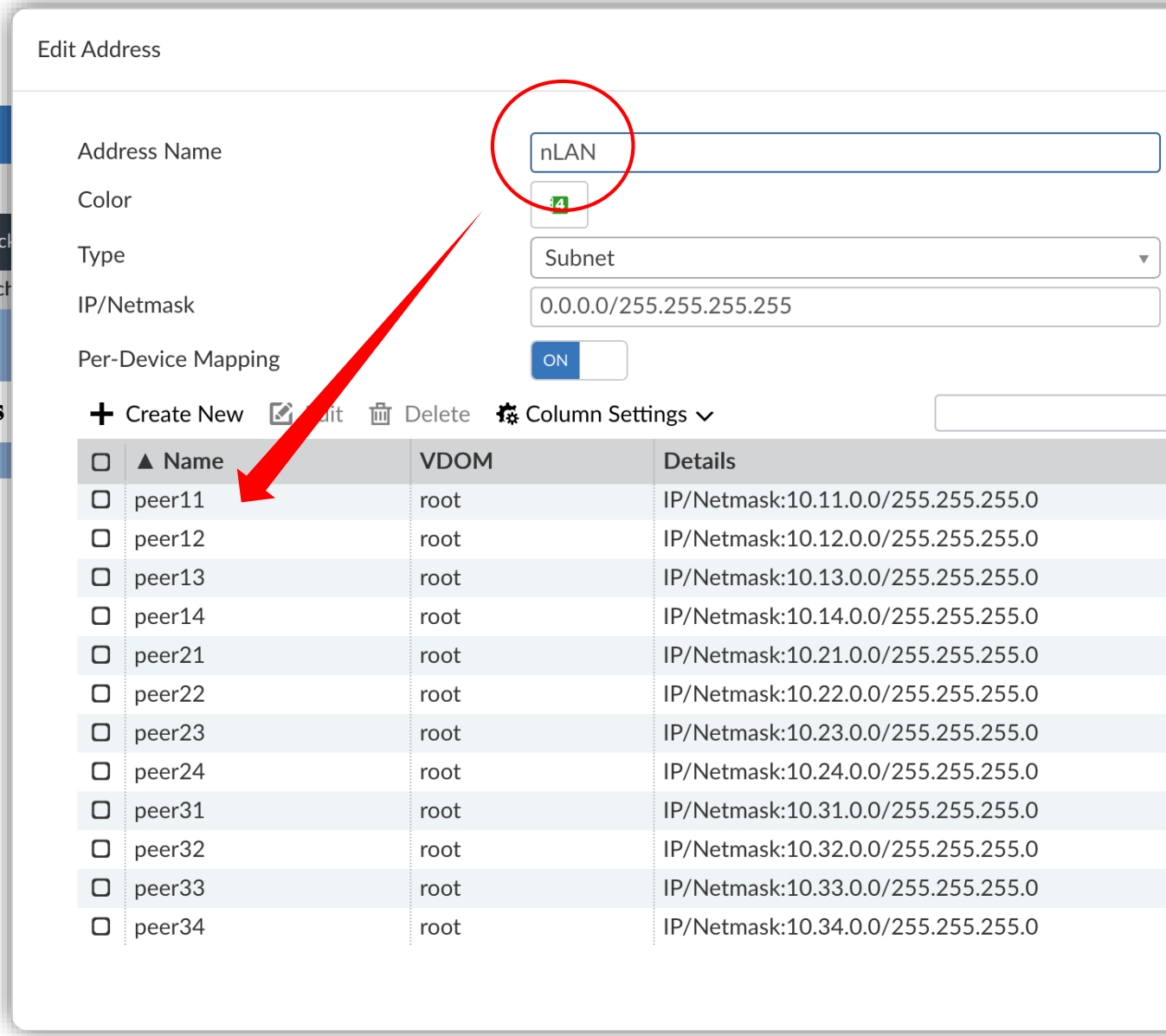


Управление политиками – общие фрагменты политики

Блоки политик

Управление политиками – общие объекты



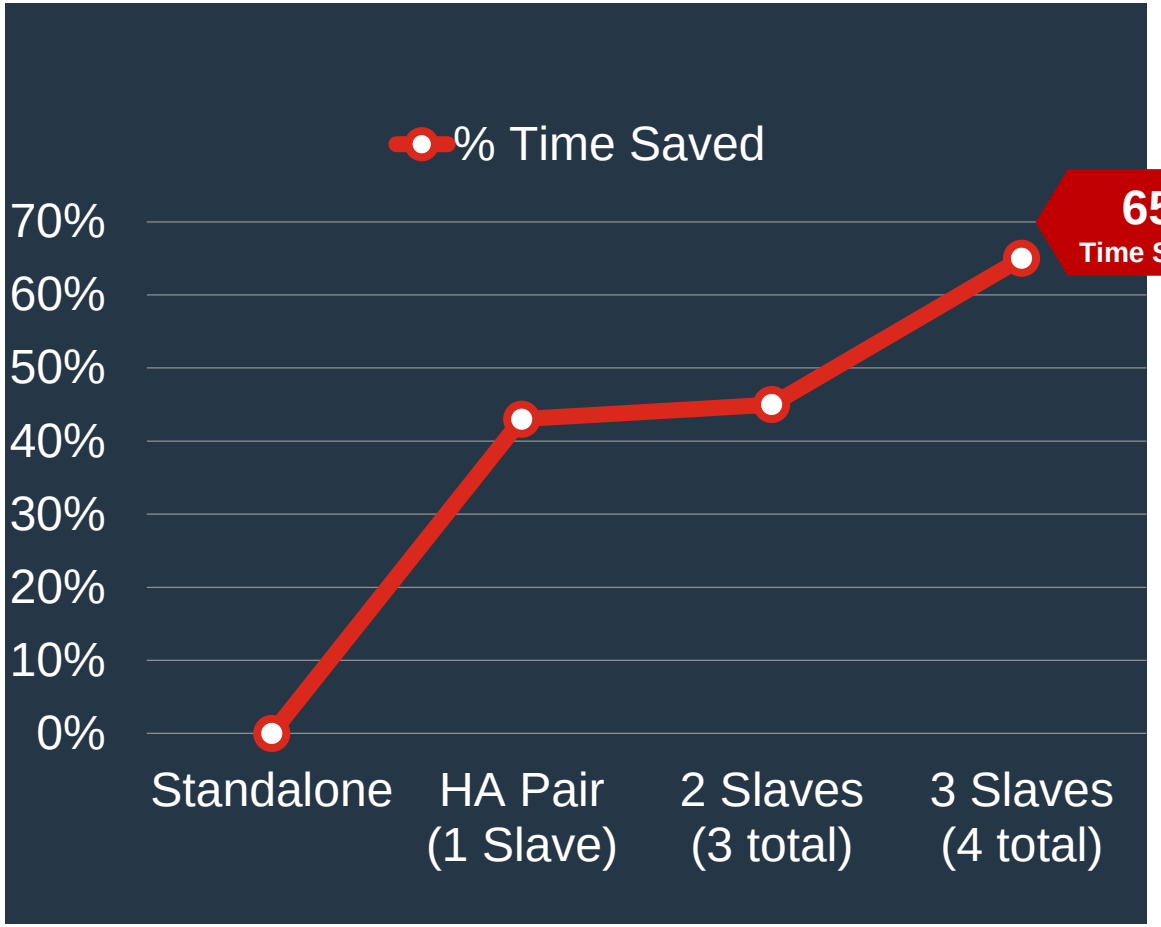


FORTINET

Балансировка нагрузки при установке политики

Результат внутреннего тестирования - время установки политики с нуля на 1000 управляемых устройств

- Самостоятельный FortiManager - 51 мин
- 1 подчиненный FortiManager - 29 мин
- 2 подчиненных FortiManager - 28 мин
- 3 подчиненных FortiManager - 18 мин



3. Аналитика Security Fabric

3. Аналитика Security Fabric

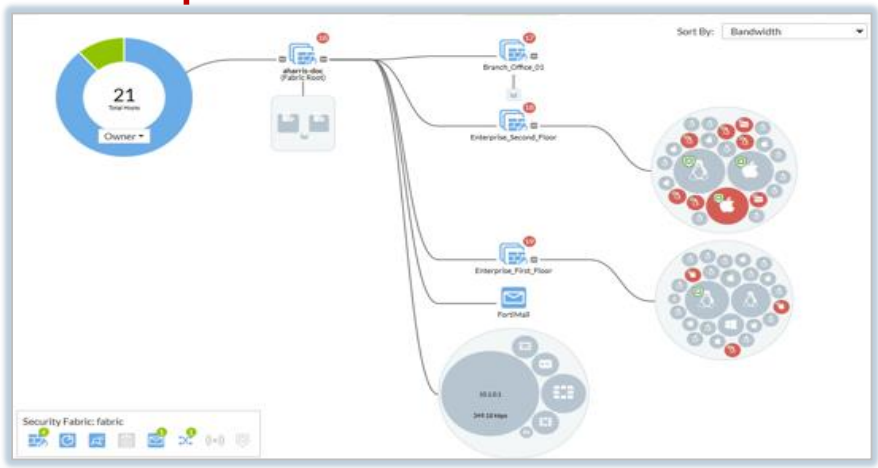
Информация о сети и защите в реальном времени

Цели

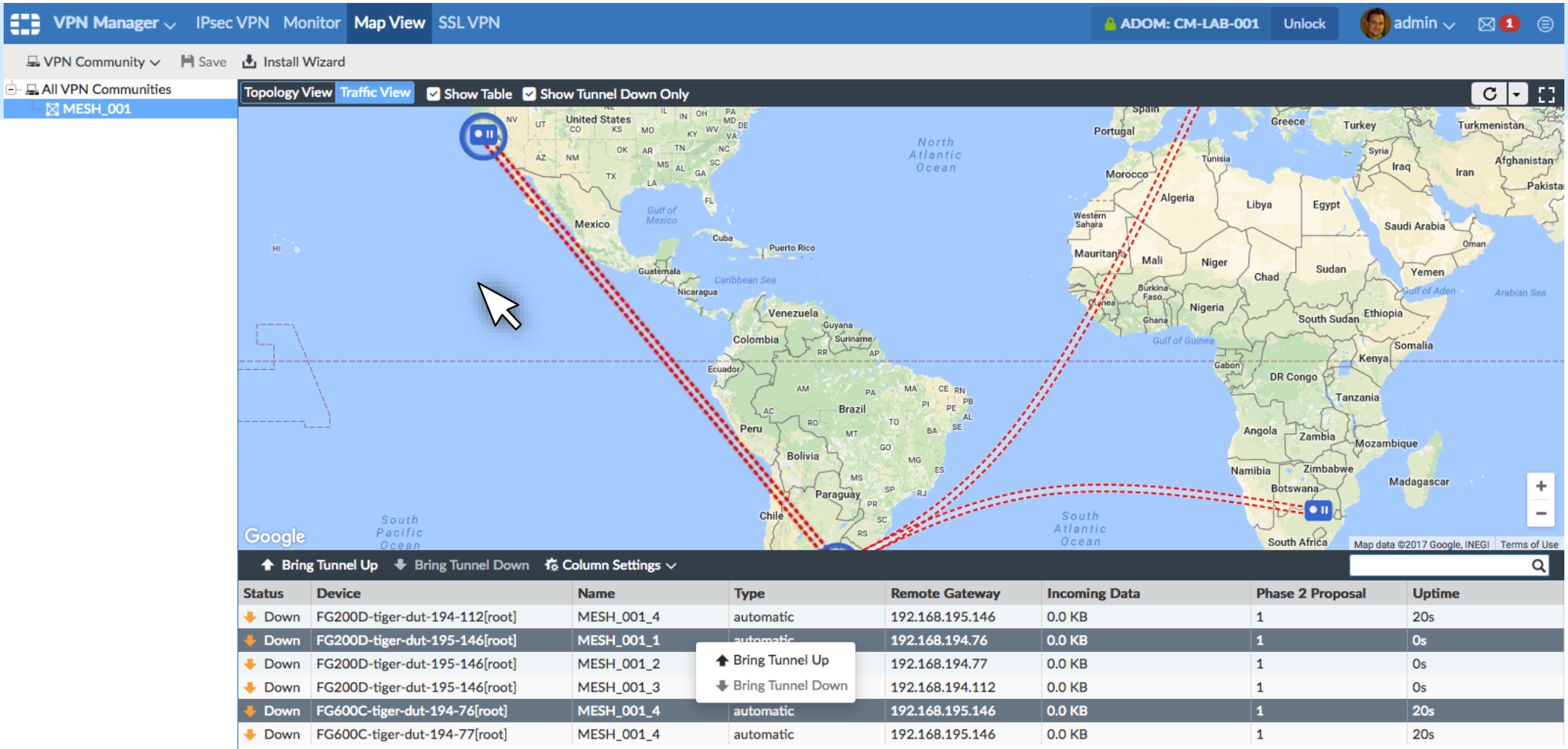
Противодействие угрозам за счёт идентификации рисков безопасности и эксплуатации в реальном времени

Ключевые возможности

- Видимость состояния сети
- Отчетность о SLA SD-WAN
- Historic SLA Reporting
- Отчеты об использовании сетевых приложений
- Адаптивное реагирование на события

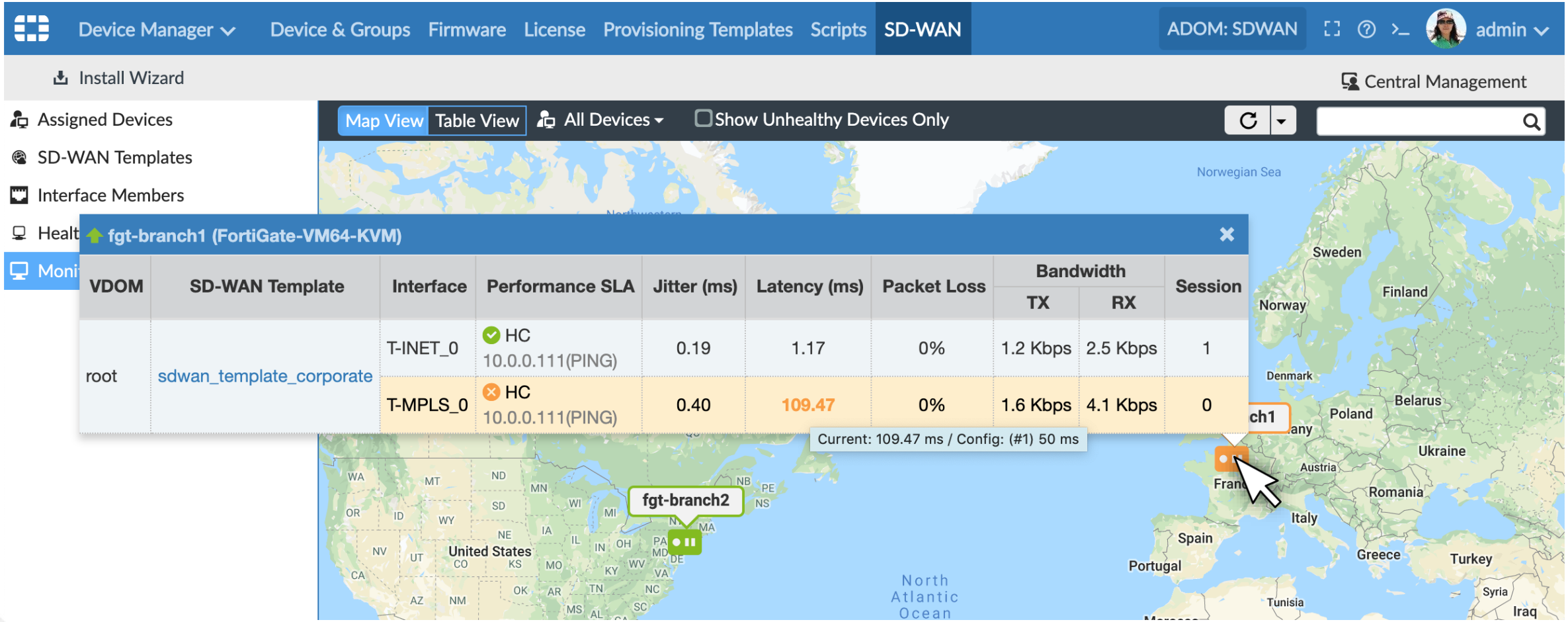


Мониторинг VPN



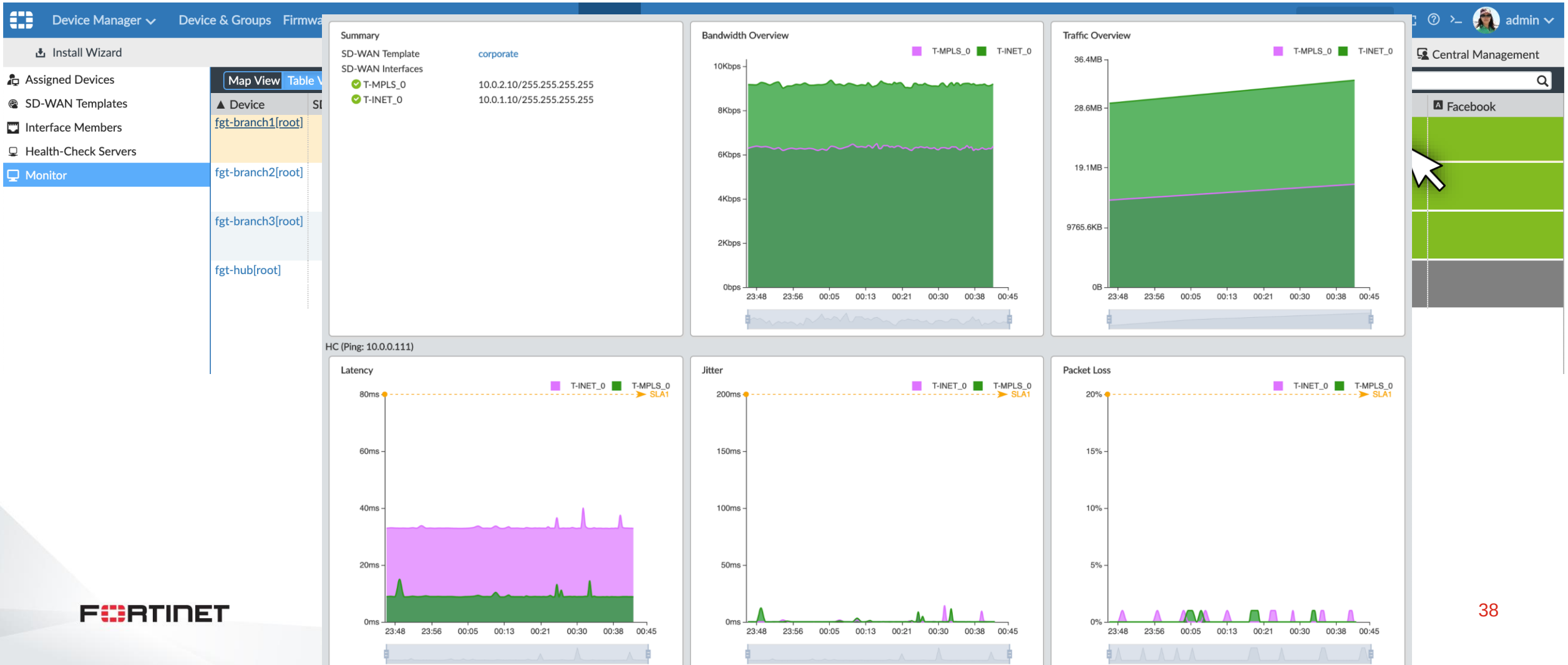
Мониторинг SD-WAN

Представление в виде карты

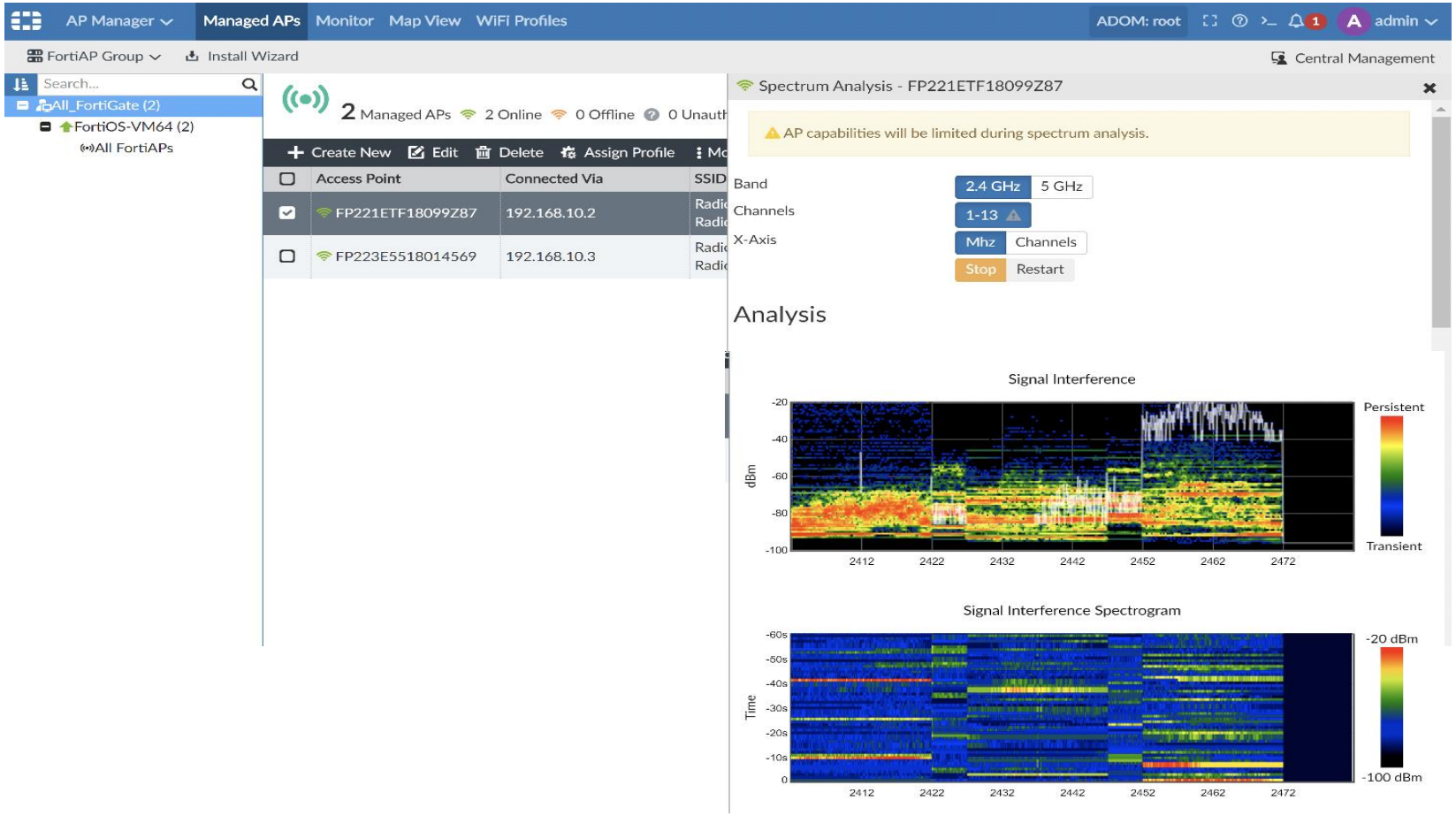


Мониторинг SD-WAN

Представление в виде таблицы



Мониторинг сети в реальном времени



FortiManager

- Понимание использования полосы
- Информация об SLA
- Мониторинг в реальном времени:
  - Точек доступа
  - Коммутаторов

4. Отчетность Compliance

4. Отчетность Compliance

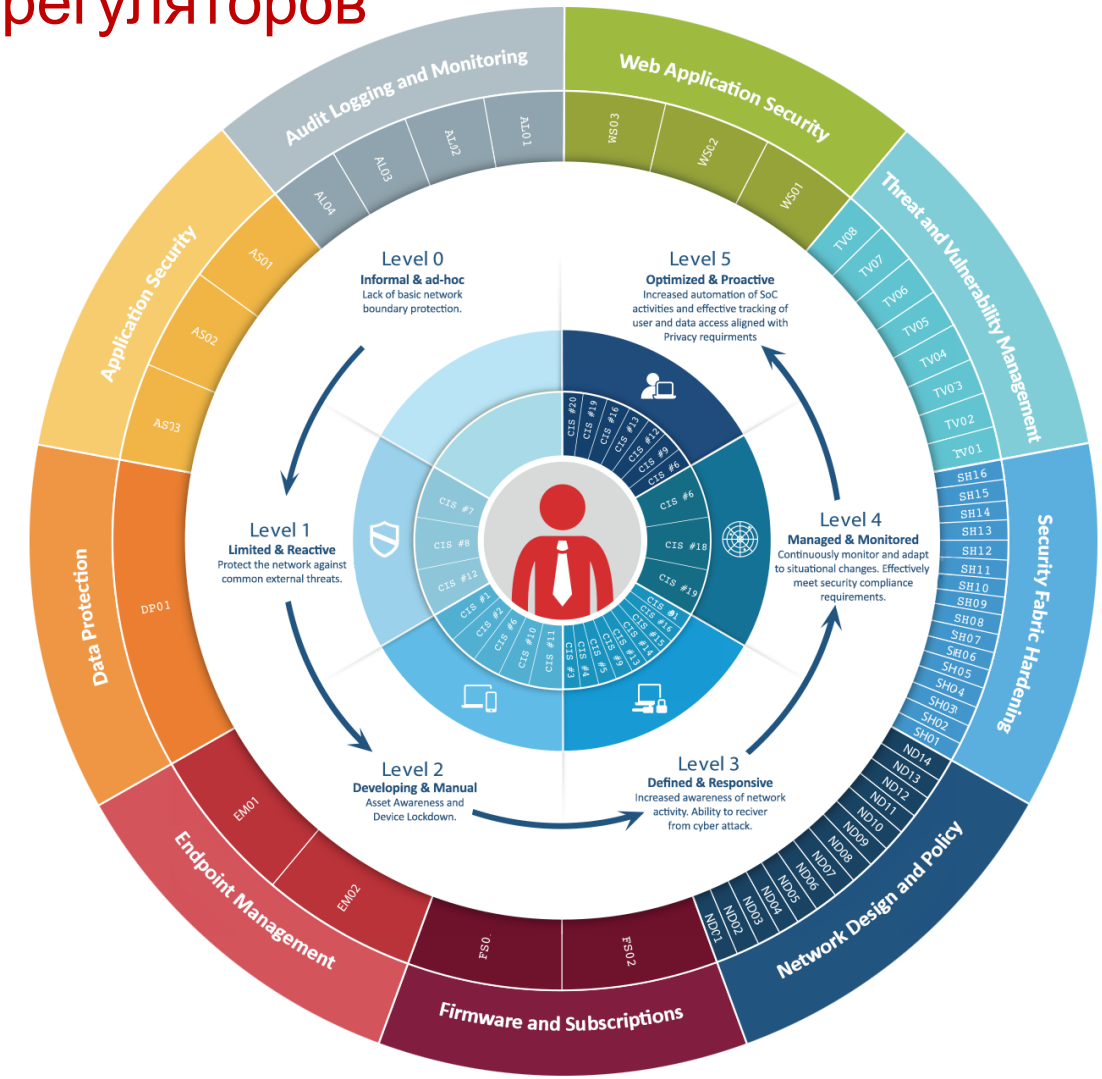
Упрощение соответствия требованиям регуляторов

Цели

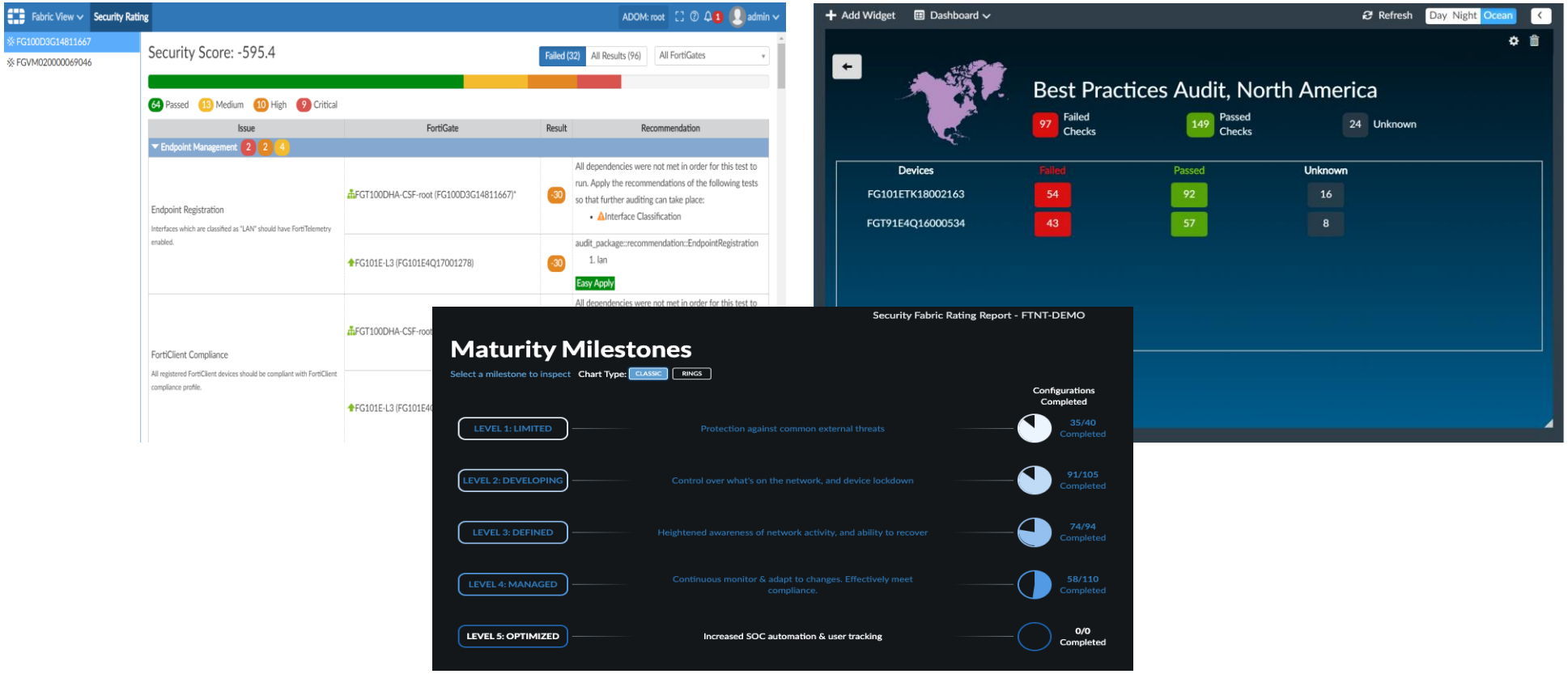
Снижение стоимости и сложности обеспечения соответствия требованиям регуляторов

Ключевые Возможности

- Отчеты о PCI DSS Compliance
- Скоринг на соответствие лучшим практикам Fortinet
- Кастомизируемые шаблоны оценки соответствия
- Двухфакторная аутентификация административного доступа
- Интеграция со сторонними решениями SIEM / Compliance



Security Rating – оценка конфигурации FortiGate



FortiManager FortiAnalyzer

Security Rating – отдельная подписка на FortiGate (входит в Enterprise и 360 bundles).
FortiManager предоставляет центральную консоль работы с результатами оценки

5. Автоматизация Администрирования

5. Автоматизация Администрирования

Интегрированные процессы

Цели

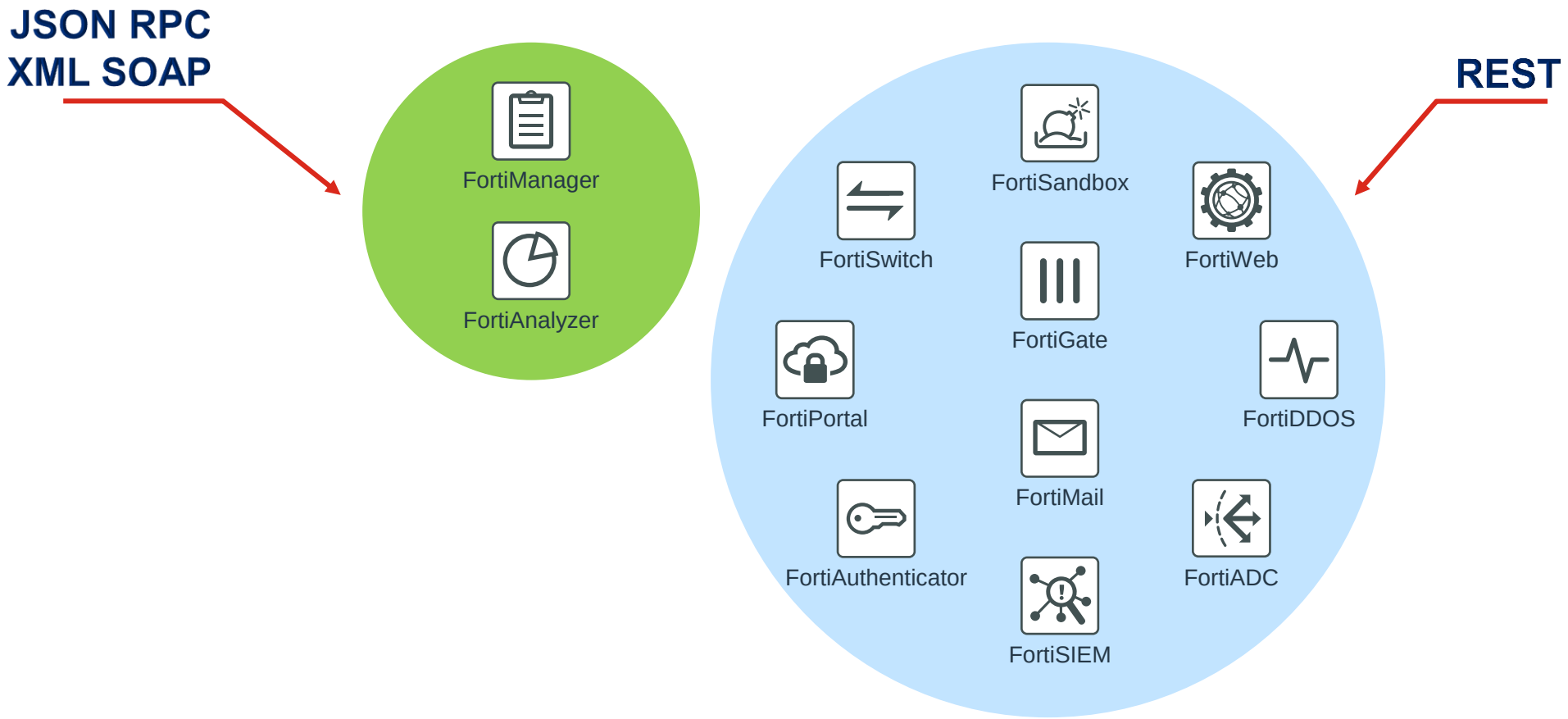
Автоматизировать типовые операции и интегрироваться с существующими процессами

Ключевые Возможности

- Сопряжение (Connectors) с SDN и общими облаками (AWS/Azure/...)
- Интеграция с IT Service Management (ServiceNow)
- REST API и инструменты для автоматизации (fndn.fortinet.net)
- Возможность использования инструментов DevOps: Ansible, Teraform, и т.п.

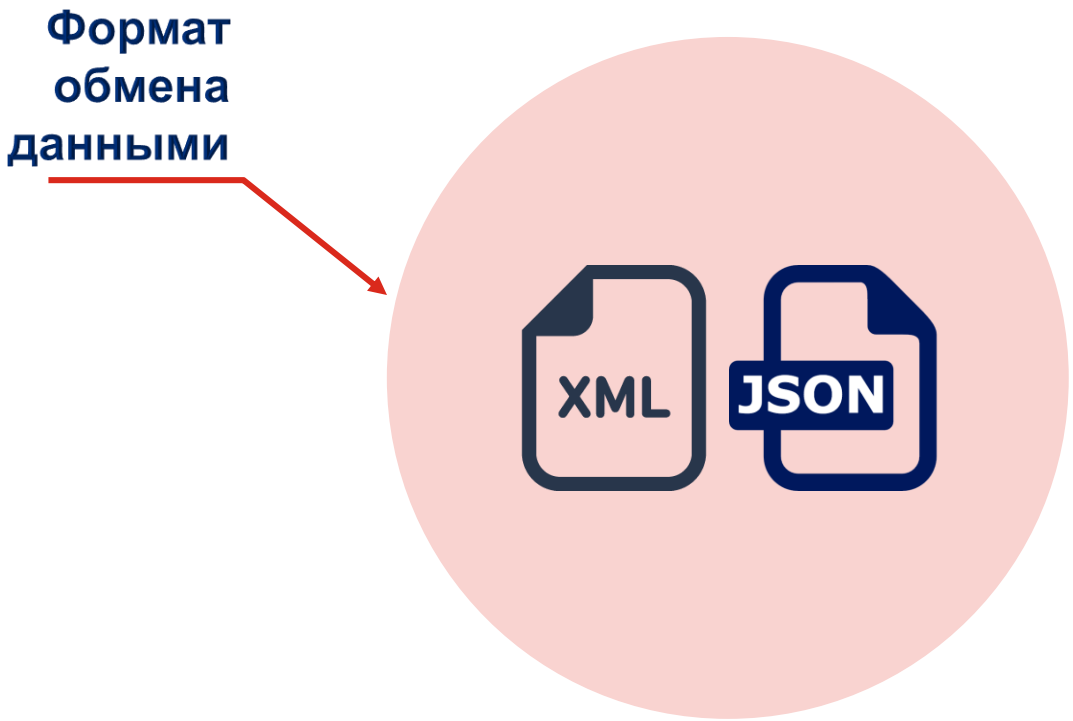
Один продукт Fortinet = один API!

Все API работают поверх HTTP/HTTPS!



Один продукт Fortinet = один API!

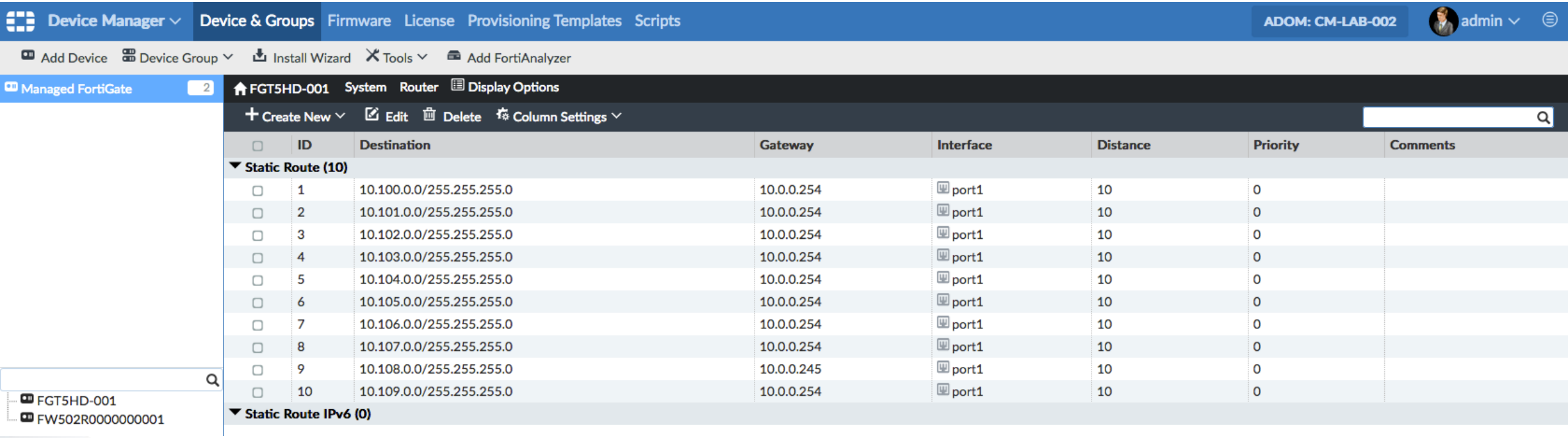
Все API работают поверх HTTP/HTTPS!



Зачем нужен API

Настройка вручную медленная

Кликов **60** *Восприятие* **120 sec** Время



Зачем нужен API (2)

Настройка с API гораздо быстрее

Время на добавление 10 статических маршрутов

GUI

120

сек

API

```
$ ./add-static-routes.py
Adding static route to 10.100.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.101.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.102.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.103.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.104.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.105.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.106.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.107.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.108.0.0/24, IF: port1, GW: 10.0.0.254
Adding static route to 10.109.0.0/24, IF: port1, GW: 10.0.0.254
Execution time: 0.150309 sec
```

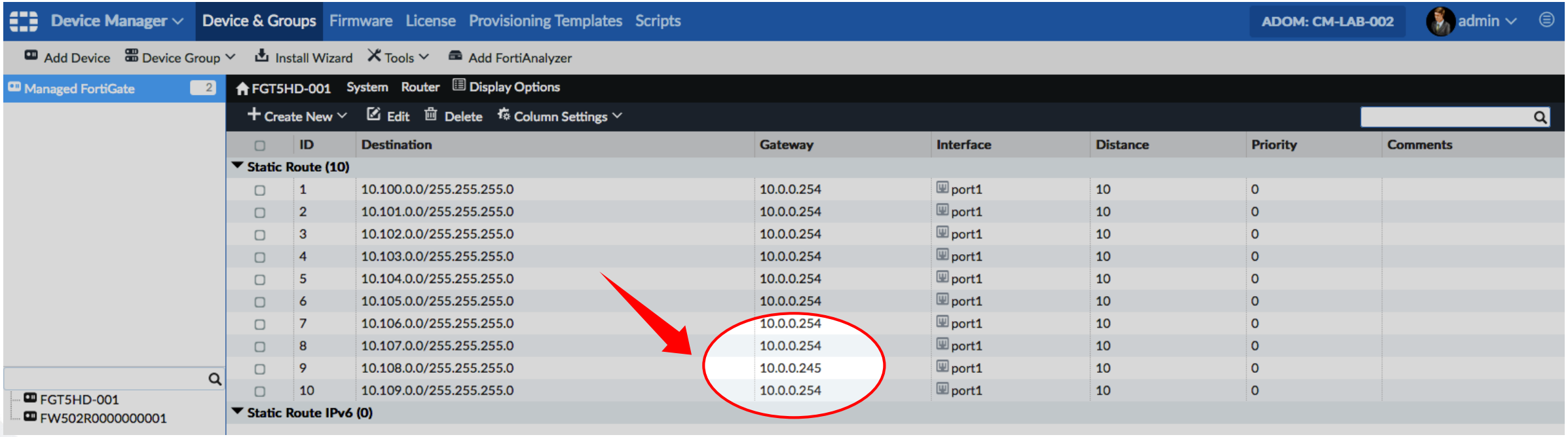
0.15

сек

Зачем нужен API (3)

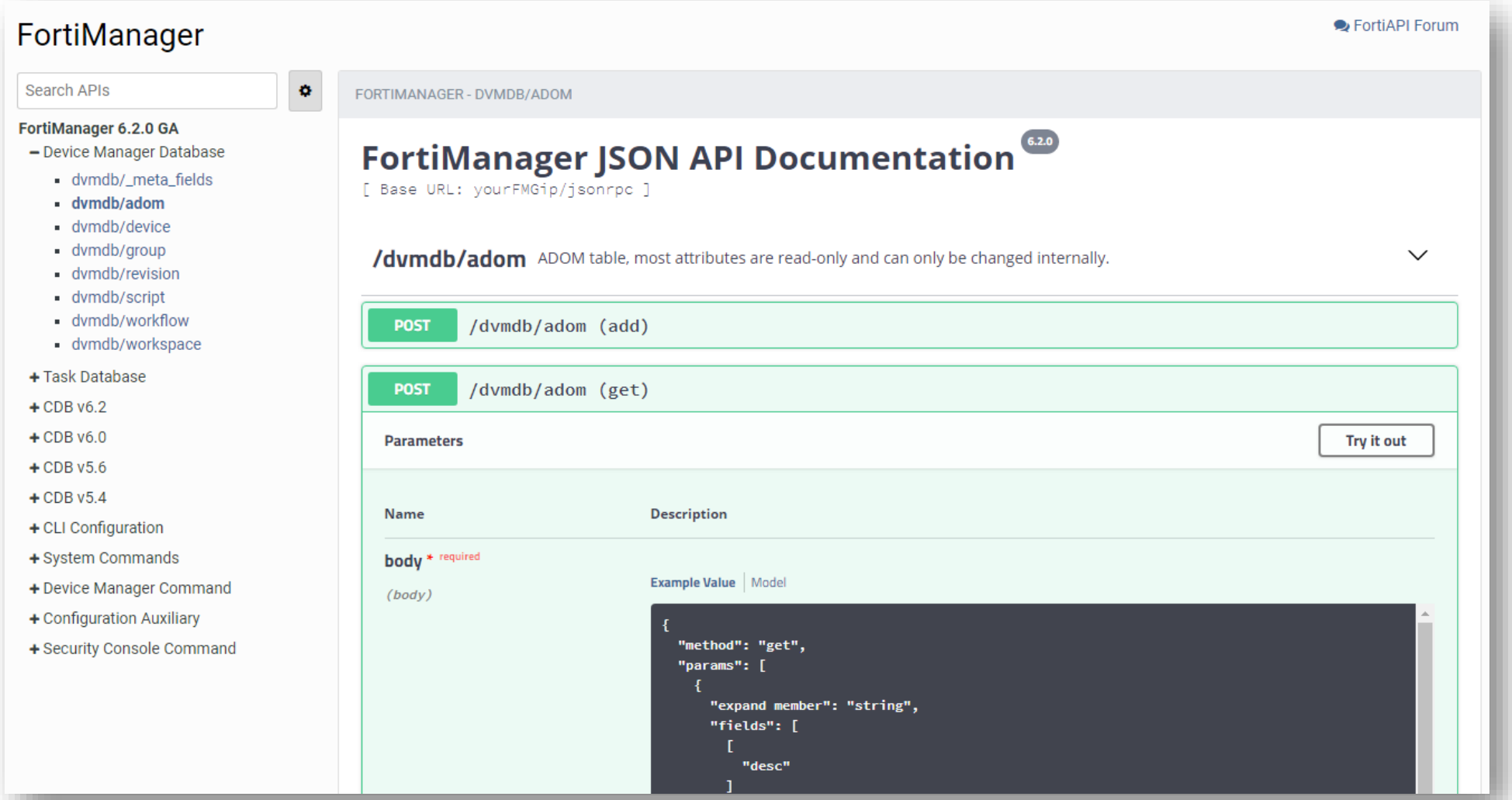
Настройка с API менее подвержена ошибкам

Найдите ошибку



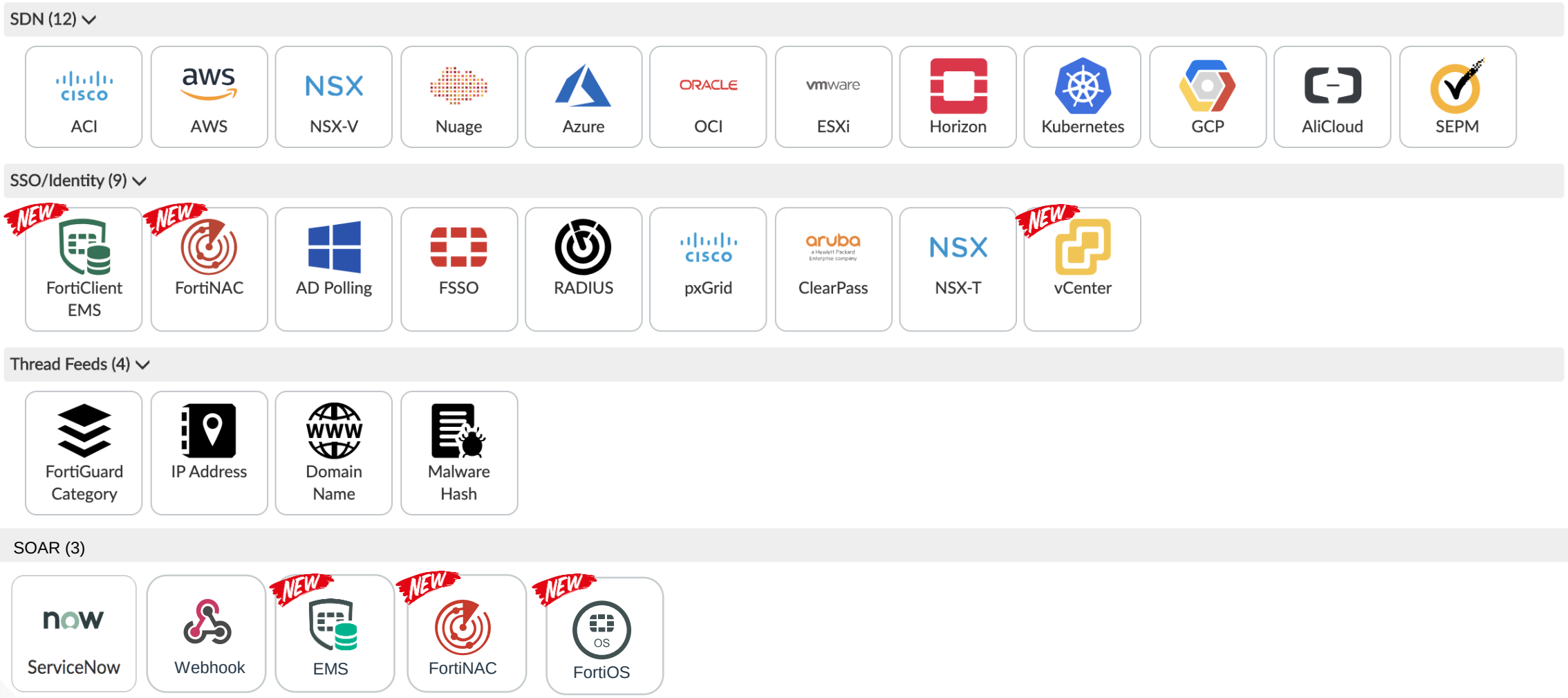
Описание функций API

- Справочное руководство доступно на ресурсе FNDN (fndn.fortinet.net) - FortiAPI



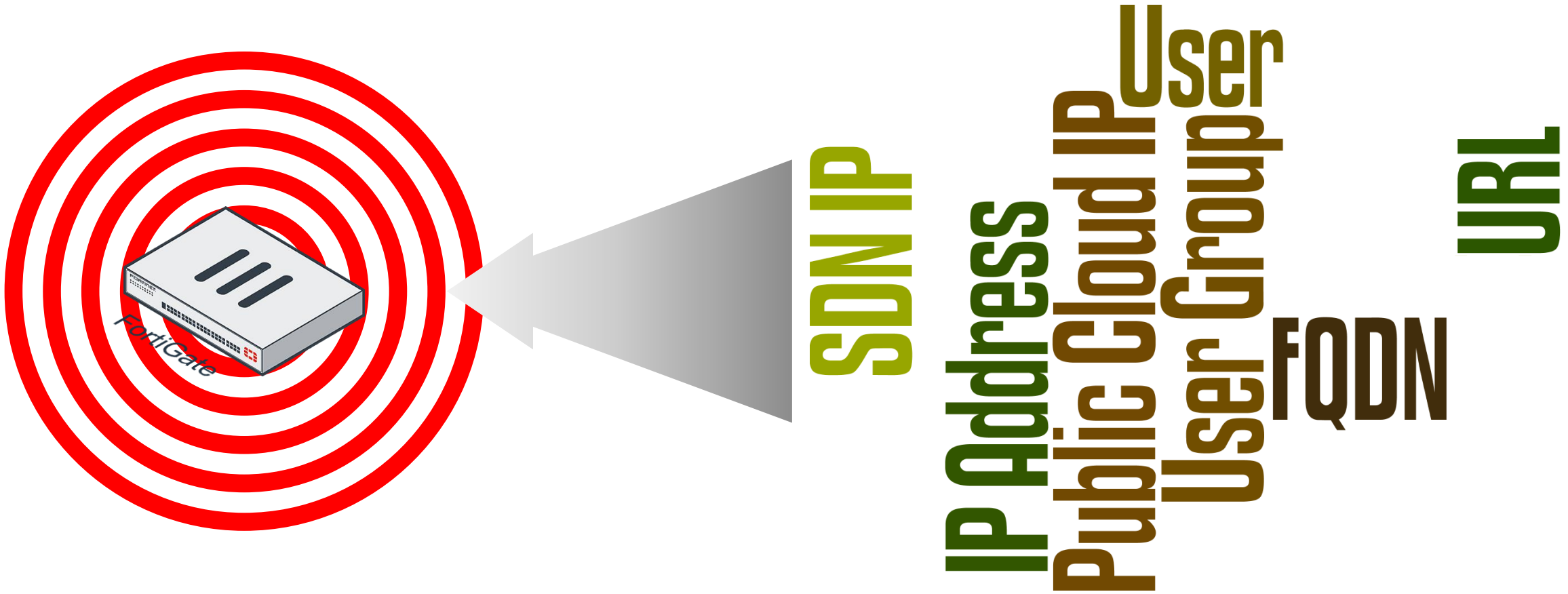
Инструмены сопряжения (Fabric Connectors)

Новые Fabric Connectors



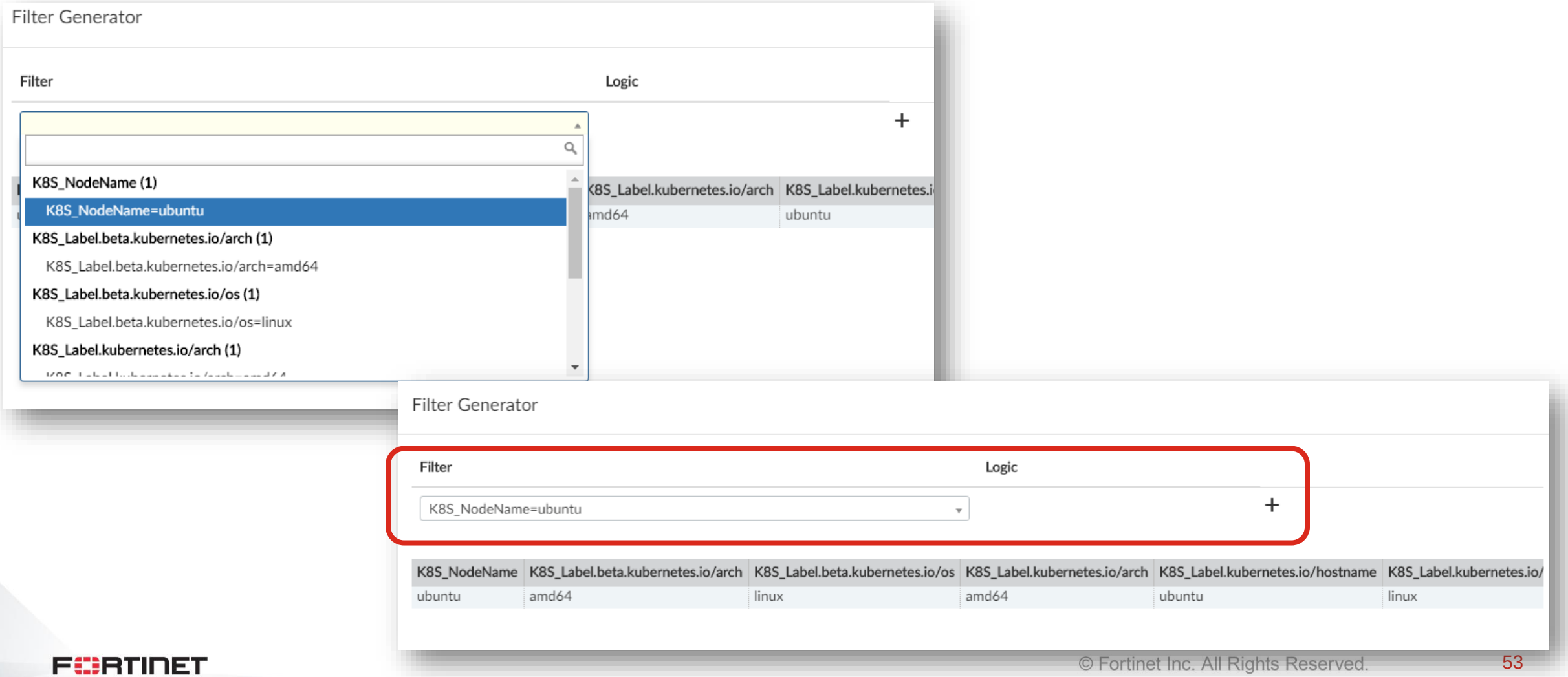
Зачем нужны Fabric Connectors

Лучше осведомленность => выше эффективность

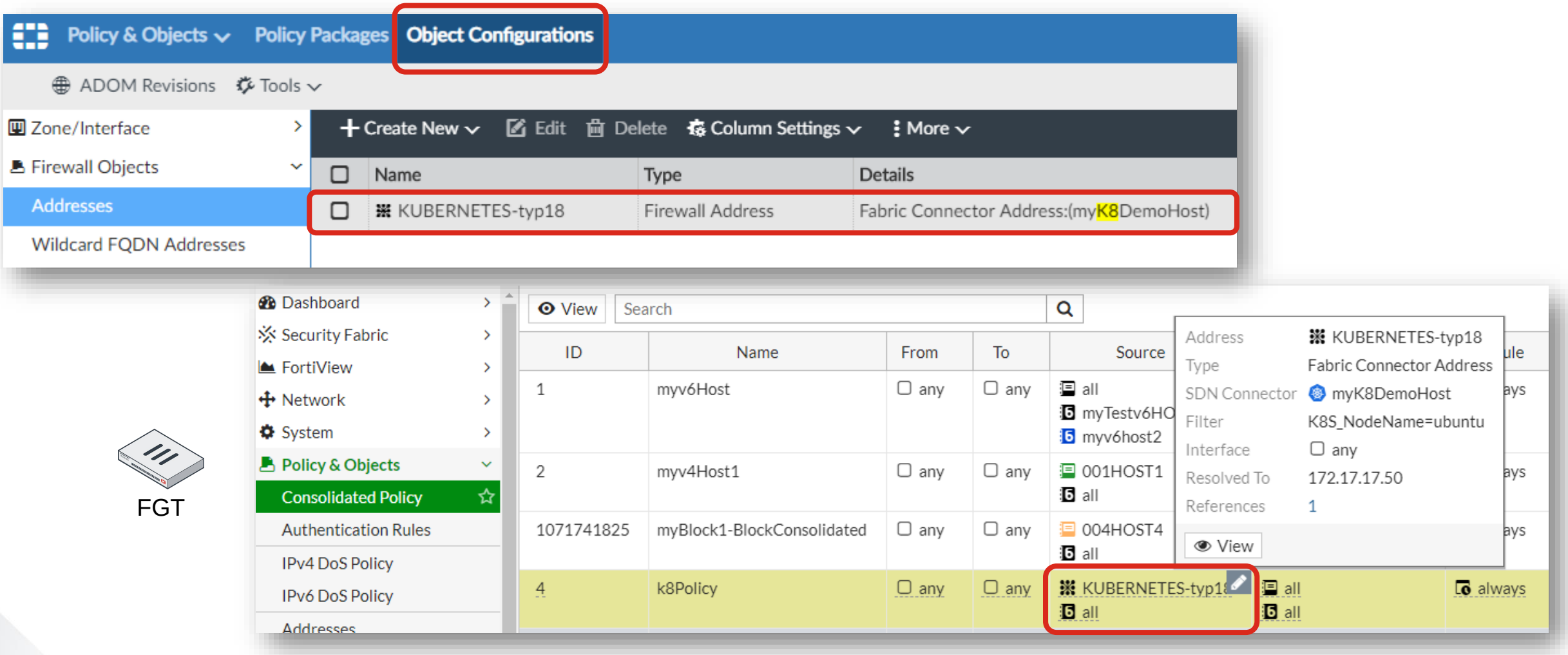


Зачем нужны Fabric Connectors – пример (1)

- Создаём фильтр для поиска контейнеров по атрибутам



Зачем нужны Fabric Connectors – пример (2)



FGT

Интеграция FortiManager и FortiAnalyzer с ServiceNow

Приложения ServiceNow Apps для FortiManager & FortiAnalyzer позволяют интегрироваться с IT Service Management и решать возникающие задачи в рамках существующих отлаженных процессов

Остались вопросы?

cis_se@fortinet.com