



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



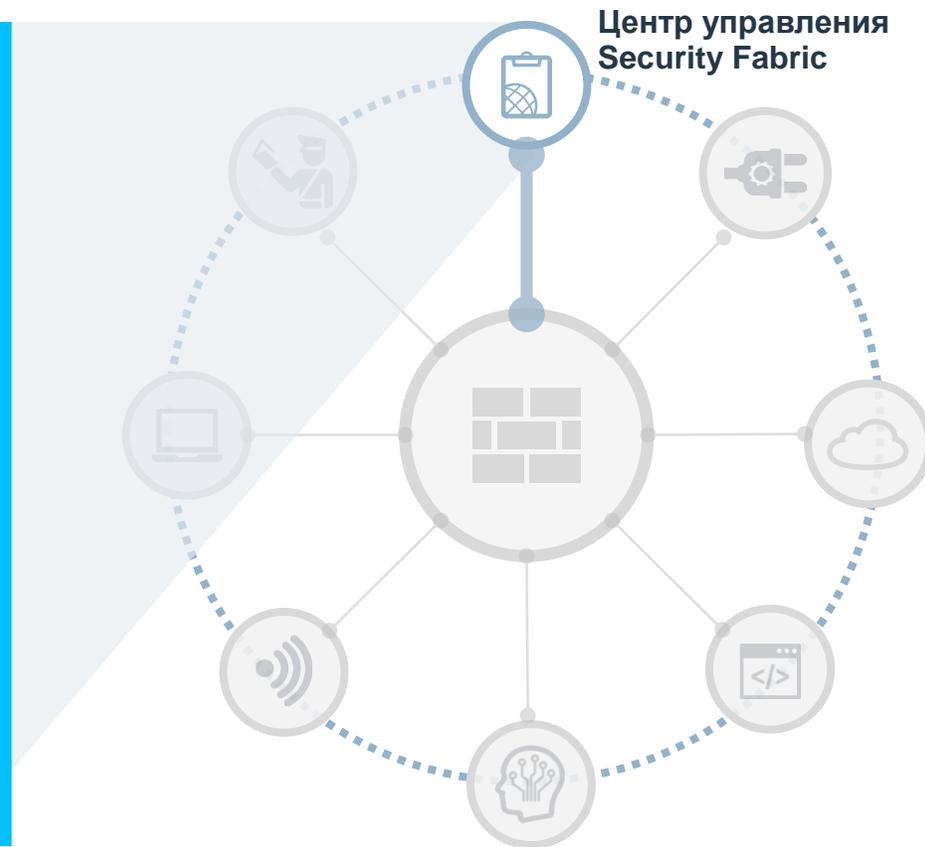
Аналитика Security Fabric

Отчетность Compliance



Автоматизация Администрирования

FortiManager & FortiAnalyzer



25K+
Пользователей



Gartner
Firewall & SD-WAN
Магические Квадранты



ПАК



Виртуальная
Машина

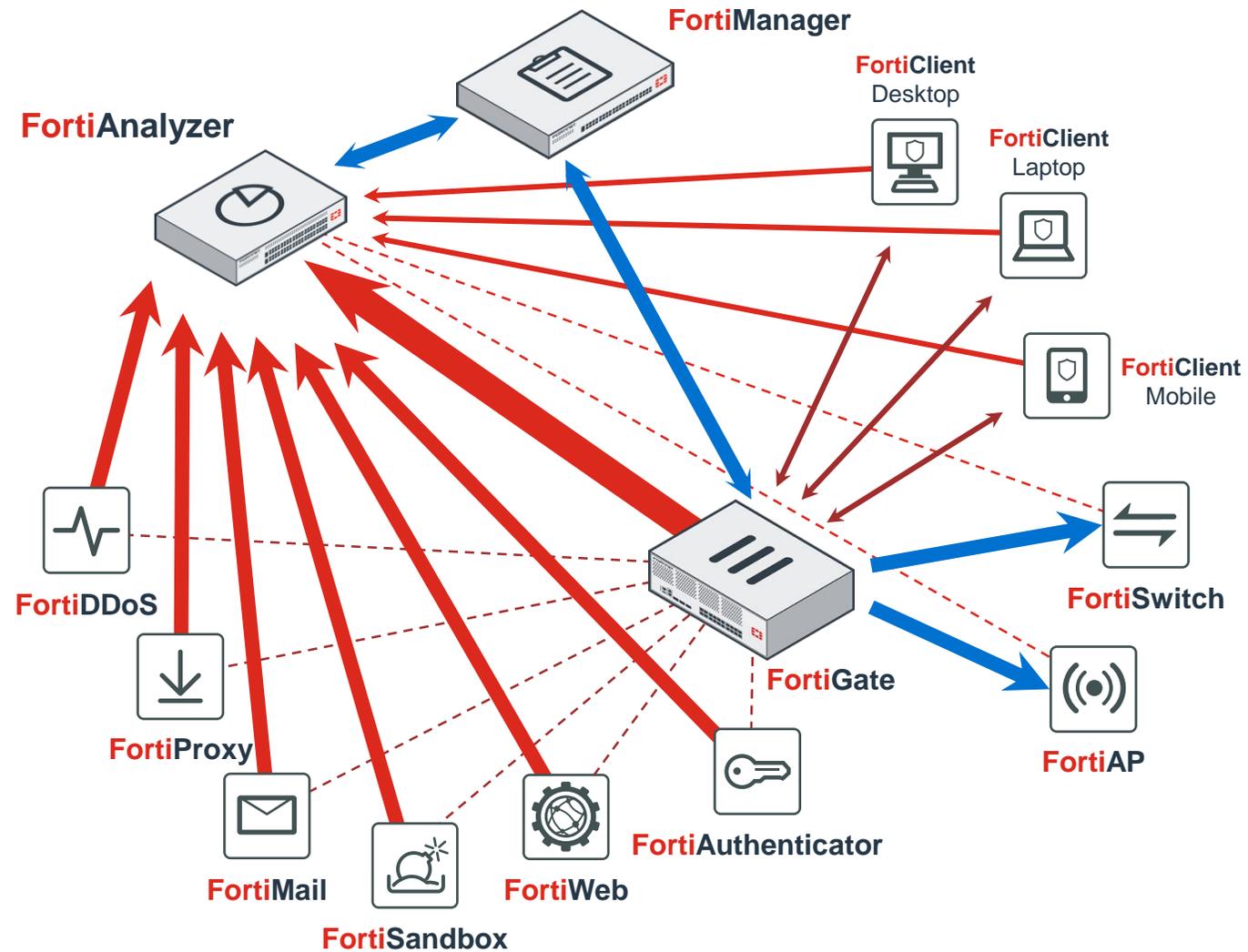


Облако

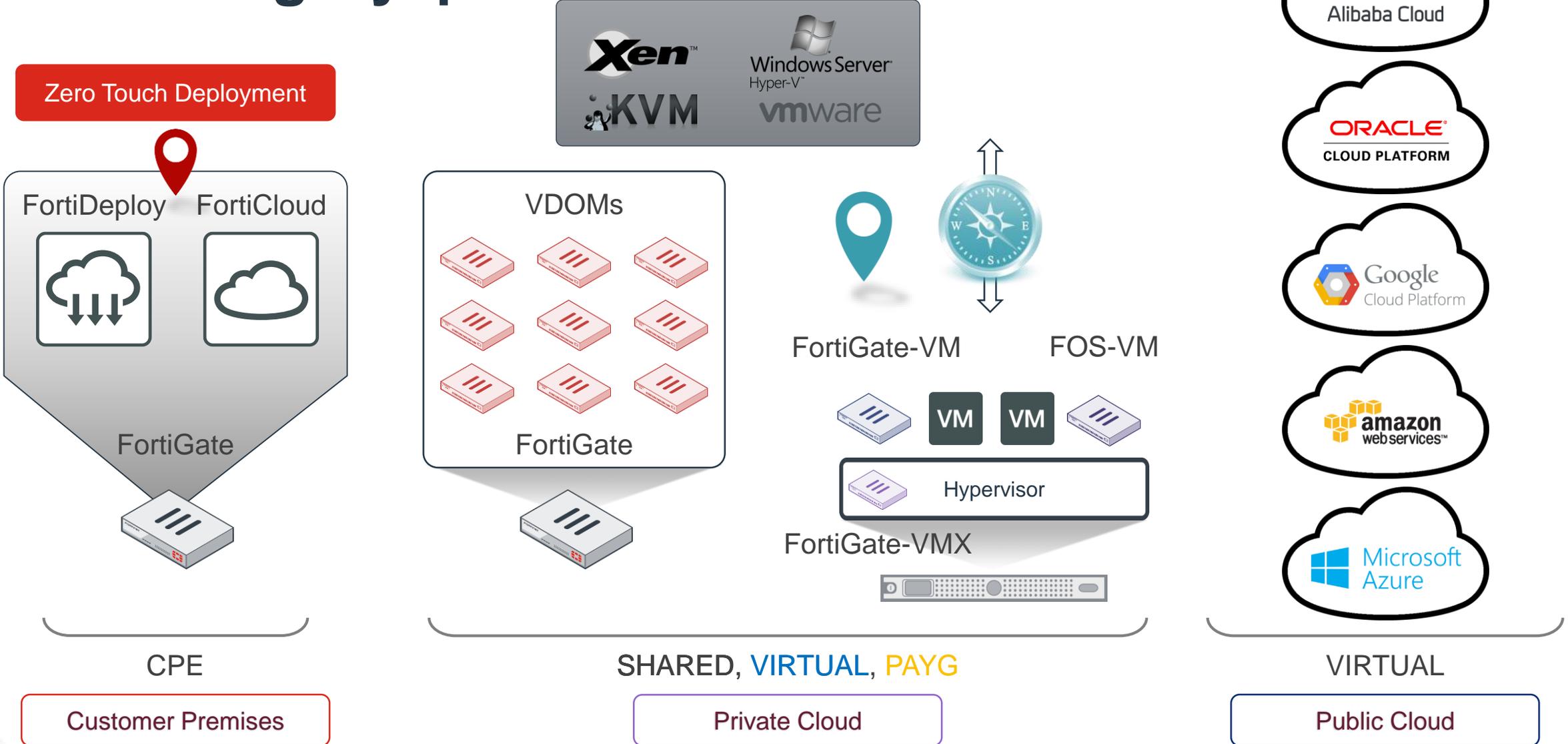


Безопасность
как Сервис

Центр управления Security Fabric – схема взаимодействий

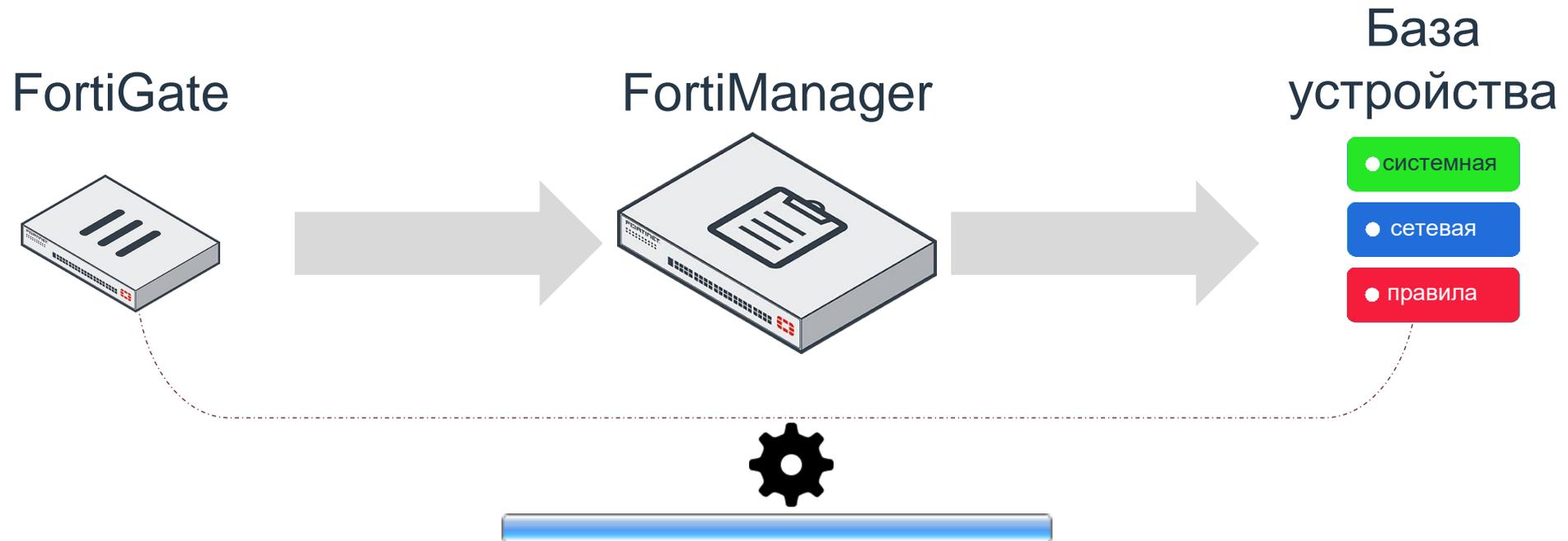


FortiManager управляет **ВСЕМИ** FortiGate



FortiManager управляет всей конфигурацией FortiGate

Конфигурация: системная, сетевая, правила доступа



1. Упрощенное Развертывание

1. Упрощенное Развертывание

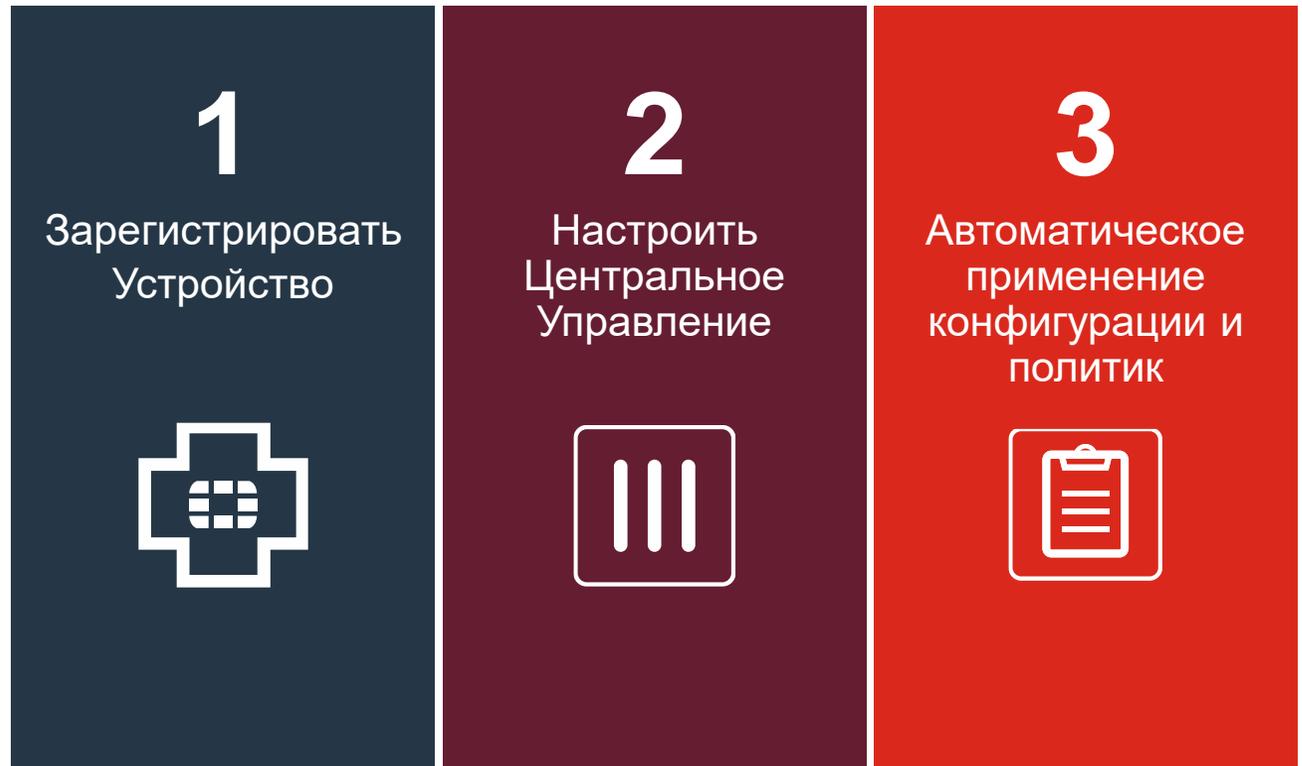
Легкий запуск в работу

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

The screenshot displays the 'Authorize Device' configuration interface in Fortinet Device Manager. The left sidebar shows a tree view with 'sd-branch' selected under 'Device Templates (2)'. The main configuration area is divided into several sections:

- DNS:** Primary DNS Server (8.8.8.8), Secondary DNS Server (208.91.112.52), Local Domain Name.
- Interface (Overridable):** A table with 7 rows, each with an 'Action' dropdown and an 'Interface' dropdown.
- Device Name:** FGVM01TM19004487, with an 'Assign New Device Name' field containing 'linglu-whistler'.
- Device Template:** sd-branch (selected).
- Firmware:** Enforce Firmware Version (checked), Firmware Version: 6.2.2.
- Policy Package:** Package Name: sd-branch-policy.

At the bottom right, there are 'Next >' and 'Cancel' buttons.

Повторно используемые объекты ZTP

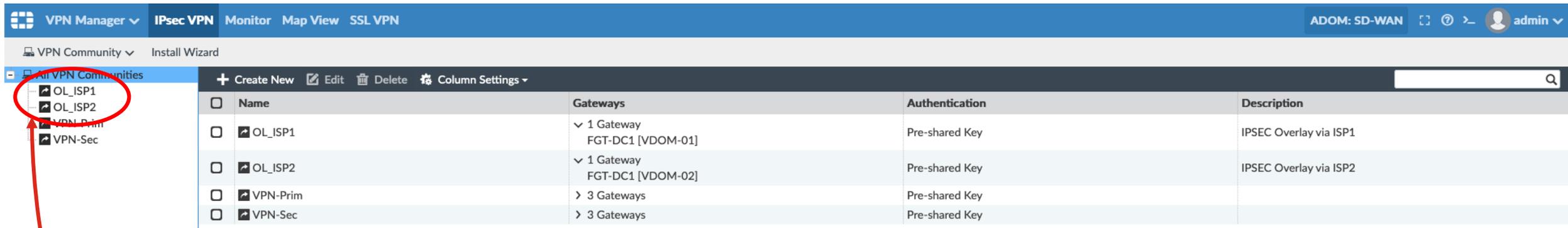
Policy Package (пакет политик и зависимые объекты)

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile	Log	NAT	Comments
▼ Production Traffic (1-2 / Total: 2)													
1	SIP Calls	any	sd-wan	LAN_BRANCHES_ZTP	FortiVoice_001	always	ALL		Accept	default	Log All Sessions	Disabled	
2	Corporate Applications	any	sd-wan	LAN_BRANCHES_ZTP	DC_NETWORKS	always	ALL		Accept	default	Log All Sessions	Disabled	
▼ Underlay Traffic (3-3 / Total: 1)													
3	Outgoing Traffic	LAN	ISP1 ISP2	LAN_BRANCHES_ZTP	all	always	ALL		Accept		Log Security Events	Enabled	Test #001
▼ Implicit (4-4 / Total: 1)													
4	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log		

Общий пакет Policy Package для всех ZTP шлюзов (настраиваемо)

Повторно используемые объекты ZTP

Настройки VPN



<input type="checkbox"/>	Name	Gateways	Authentication	Description
<input type="checkbox"/>	OL_ISP1	∨ 1 Gateway FGT-DC1 [VDOM-01]	Pre-shared Key	IPSEC Overlay via ISP1
<input type="checkbox"/>	OL_ISP2	∨ 1 Gateway FGT-DC1 [VDOM-02]	Pre-shared Key	IPSEC Overlay via ISP2
<input type="checkbox"/>	VPN-Prim	> 3 Gateways	Pre-shared Key	
<input type="checkbox"/>	VPN-Sec	> 3 Gateways	Pre-shared Key	

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

Device Manager Device & Groups Firmware License Provisioning Templates Scripts SD-WAN ADOM: SD-WAN admin

Install Wizard Central Management

Assigned Devices SD-WAN Templates Interface Members Health-Check Servers Monitor

Edit BRANCHES_ZTP

Name: BRANCHES_ZTP

Description: [Empty]

SD-WAN Status: ON

Interface Members

- Create New Edit Delete Move Up Move Down

#	ID	Port
1	1	OL_ISP1
2	2	OL_ISP2

Performance SLA

- Create New Edit Delete

#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold
1	HC_BRANCHES_ZTP	HC_VOICE	PING	5	5
2	HC_SCP_IPERF	HC_SCP_IPERF	PING	5	5

SD-WAN Rules

- Create New Edit Delete Move Up Move Down

#	Name	Source	Destination	Criteria	Members
1	SIP_traffic	all	SIP, SIP.Method, SIP.Via.NAT, SIP_Media.Type.A...	HC_BRANCHES_ZTP#1	OL_ISP2 OL_ISP1
2	SCP	all	DC_NETWORKS	HC_SCP_IPERF#1	OL_ISP1 OL_ISP2
3	IPERF-8801	all	DC_NETWORKS	HC_SCP_IPERF#1	OL_ISP1 OL_ISP2
4	sd-wan	ALL	ALL	Source IP Based	ALL

Общий шаблон SD-WAN для всех ZTP шлюзов (настраиваемо)

Повторно используемые объекты ZTP

Шаблон настройки управляемых коммутаторов FortiSwitch

The image shows two screenshots from the FortiSwitch Manager interface. The top screenshot displays the 'FortiSwitch Templates' table, where the 'branches_fsw_template' is highlighted with a red circle. The bottom screenshot shows the 'Managed FortiSwitch' table, where the 'Template' column for two devices is highlighted with a red circle, and a red arrow points from the template name in the top screenshot to these entries.

FortiSwitch Templates Table:

Name	Description	Platform	Last Modified	Created Time
branches_fsw_template	FortiSwitch Template created via Ansible	FortiSwitch-124E-FPOE	admin/2019-06-25 14:32:43	2019-06-25 14:32:28

Managed FortiSwitch Table:

FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	Template	OS Version
S124EF591800	S124EF5918002109	FortiSwitch-124E-FPOE	fgt-branch2[root]	10.0.0.1	branches_fsw_template	S124EF-v6.0.4-build064,190516 (GA)
S124EF591800	S124EF5918001321	FortiSwitch-124E-FPOE	fgt-branch1[root]	10.0.0.1	branches_fsw_template	S124EF-v6.0.0-build059,190327 (Interim)

Повторно используемые объекты ZTP

Шаблон настройки управляемых точек доступа FortiAP

AP Profile	Name	Platform	Radio 1	Radio 2	Comment
	branches_fap_profile	FAP421E	2.4GHz 802.11n/g/b	5GHz 802.11ac/n/a	

4 Managed APs 4 Online 0 Offline 0 Unauthorized 0 Rogue APs 0 Client Connected

Access Point	Connected Via	AP Profile	SSIDs	Channel	Clients	OS Version
FP421E3X16000348	10.1.0.1	branches_fap_profile	Radio 1: marketing, support, Radio 2: marketing, support,	Radio 1: 10 Radio 2: 124	Radio 1: 0 Radio 2: 0	FP421E-v6.2-build0229
FP421ETF18002999	10.1.0.1	branches_fap_profile	Radio 1: marketing, support, Radio 2: marketing, support,	Radio 1: 13 Radio 2: 116	Radio 1: 0 Radio 2: 0	FP421E-v6.2-build0227
FW60DP-WIFI0	127.0.0.1		Radio 1:	Radio 1: 6	Radio 1: 0	FW60DP-v6.0-build268

Re-Usable Object Example

Шаблон (или групп) типовых повторяемых настроек - CLI Template

The screenshot displays the Fortinet FortiGate GUI. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', 'License', 'Provisioning Templates', 'Scripts', and 'SD-WAN'. The user is logged in as 'admin' on the 'ADOM: SD-BRANCH1' domain.

In the 'Scripts' section, a table lists CLI Templates. The 'branches_cli_template_group' is highlighted with a red circle. Below this, a detailed view of the 'Device & Groups' section shows a table of devices with their configuration status and applied CLI templates.

Device Name	Config Status	Policy Package Status	CLI Template Status	Firmware Version	Host Name	IP Address
fgt-branch1	Auto-update	pp_production	branches_cli_template_group	FortiGate 6.0.5,build0268 (GA)	fgt-branch1	10.210.34.238
fgt-branch2	Unknown	pp_production	branches_cli_template_group	FortiGate 6.0.5,build0268 (GA)	fgt-branch2	10.210.34.240
fgt-hub1	Unknown	pp_hub		FortiGate 6.0,build0266	fgt-hub1	

Ключевой элемент ZTP – модель устройства

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

The screenshot displays the FortiManager Device Manager interface. The left sidebar shows a tree view of managed devices, with 'FGT-Branch3' highlighted and circled in red. The main panel shows the configuration for 'FGT-Branch3' under the 'System : Interface' tab. The interface is categorized into several sections:

- Hardware Switch (1):** internal (LAN) - Hardware Switch, Manual, 10.1.3.1/255.255.255.0, Access: HTTPS, PING, SSH, HTTP, Status: Up.
- Physical (3):**
 - dmz - Physical, Manual, 10.111.3.1/255.255.255.0, Access: HTTPS, PING, HTTP, FMG-Access, CAPWAP, Status: Up.
 - wan1 (ISP1) - Physical, DHCP, 0.0.0.0/0.0.0.0, Access: PING, FMG-Access, Status: Up.
 - wan2 (ISP2) - Physical, DHCP, 0.0.0.0/0.0.0.0, Access: PING, FMG-Access, Status: Up.
- SD-WAN (3):**
 - sd-wan - SD-WAN, Status: Up.
 - OL_ISP1_0 - Tunnel, Manual, 10.10.10.4/255.255.255.255, Status: Up.
 - OL_ISP2_0 - Tunnel, Manual, 10.10.11.4/255.255.255.255, Status: Up.
- Software Switch (2):**
 - lan - Software Switch, Manual, 192.168.1.99/255.255.255.0, Access: HTTPS, PING, SSH, HTTP, FMG-Access, CAPWAP, Status: Up.
 - wqt.root - Software Switch, Manual, 10.253.255.254/255.255.240.0, Status: Up.
- Tunnel (1):** ssl.root (SSL VPN interface) - Tunnel, Manual, 0.0.0.0/0.0.0.0, Status: Up.

Ключевой элемент ZTP – атрибуты модели

Взаимосвязь с CLI Template

The screenshot shows the Fortinet Device Manager interface. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', 'License', and 'Provisioning Templates'. Below this, there are options for 'Add Device', 'Device Group', 'Install Wizard', 'Tools', and 'Table View'. The main content area is titled 'Edit Device FGT-Branch3' and shows a list of managed devices: 'branches' (2) and 'hubs' (1). Under 'Meta Fields', the following fields are listed: 'branch_number' (value: 3), 'fortilink_intf' (value: dmz), 'isp1_intf' (value: wan1), and 'isp2_intf' (value: wan2). A red box highlights the 'branch_number' field, and a red arrow points from it to the CLI code on the right.

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

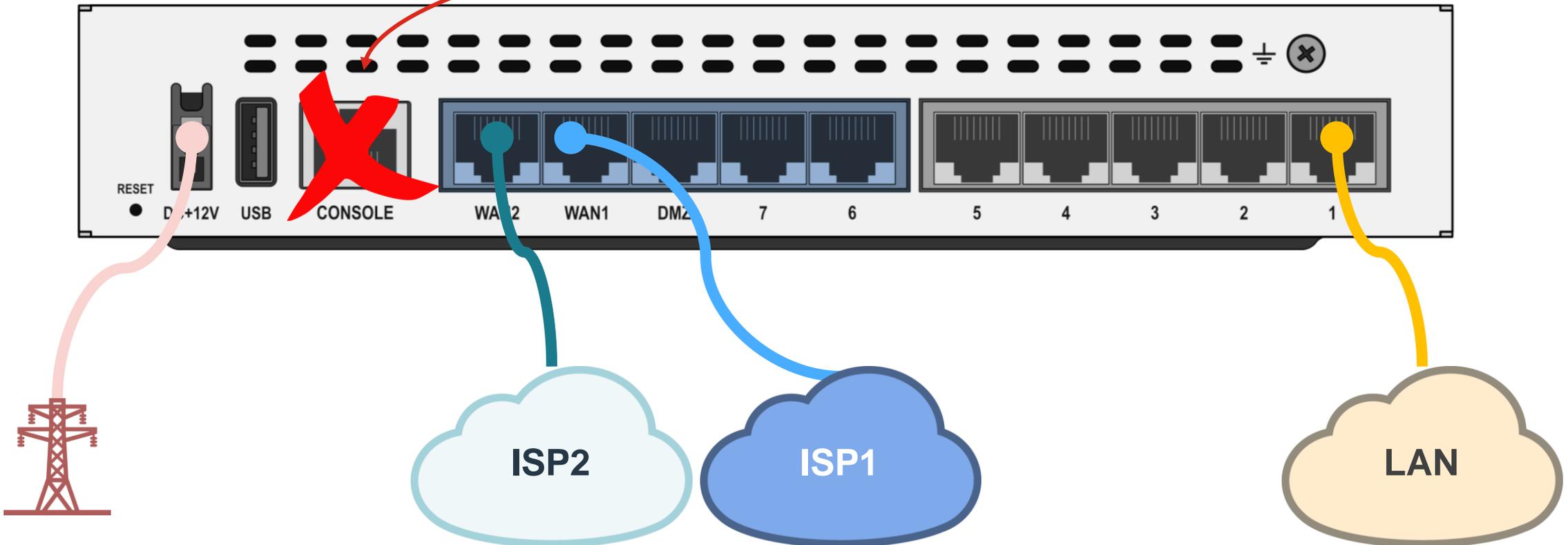
config system interface
edit $(isp1_intf)
append allowaccess https
next
edit $(fortilink_intf)
set ip 10.0.0.99 255.255.255.0
next
end

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

Процесс ZTP

Подготовка устройства – подключение интерфейсов

Не требуется подключаться к консоли



Процесс ZTP – определение адреса FortiManager

FortiCloud



DHCP



Cloud-init



FMG IP

Альтернатива
USB диск со стартовой
конфигурацией

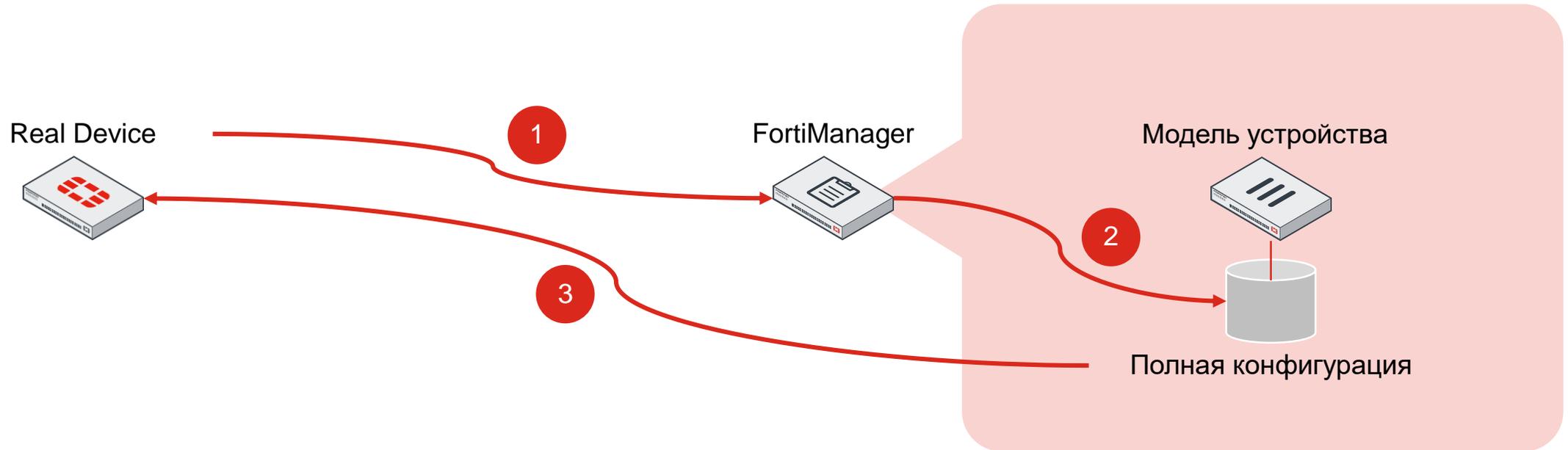


FortiGate

#	ALL (0)	Bulk Key	Device	Claimed On	Subscription	Deployed To	Deployed Time
1	<input type="checkbox"/>	6BTGMLH8EA	FGT61ETK18005042	2019-04-08 11:53		FortiManager (10.210.35.200)	2019-06-24 14:48

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

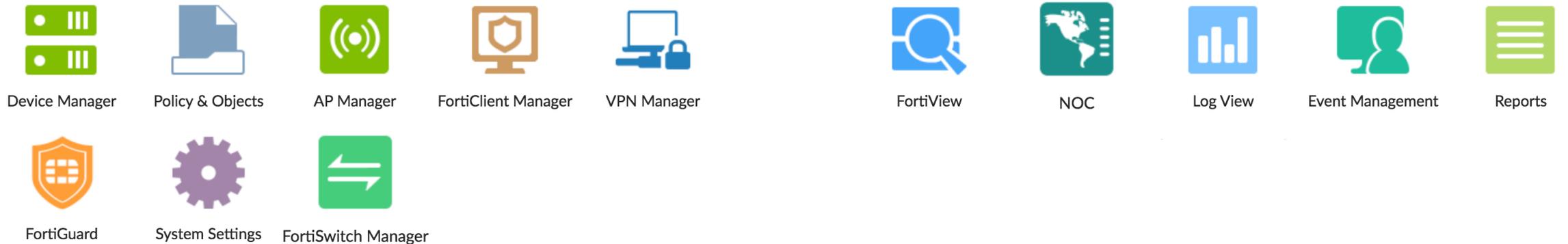
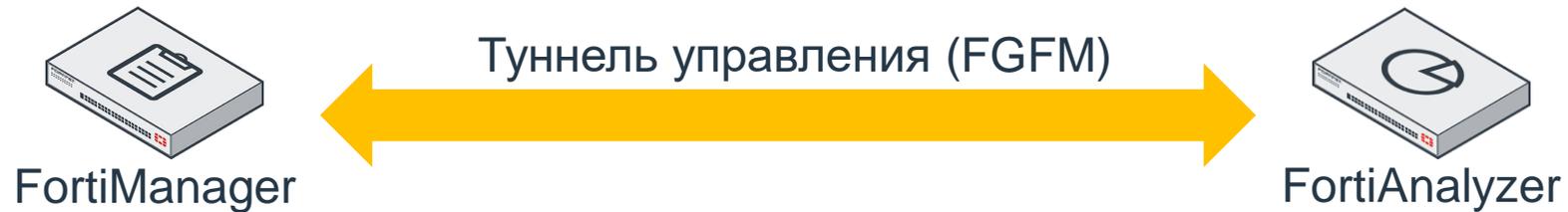
Ключевые Возможности

- 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

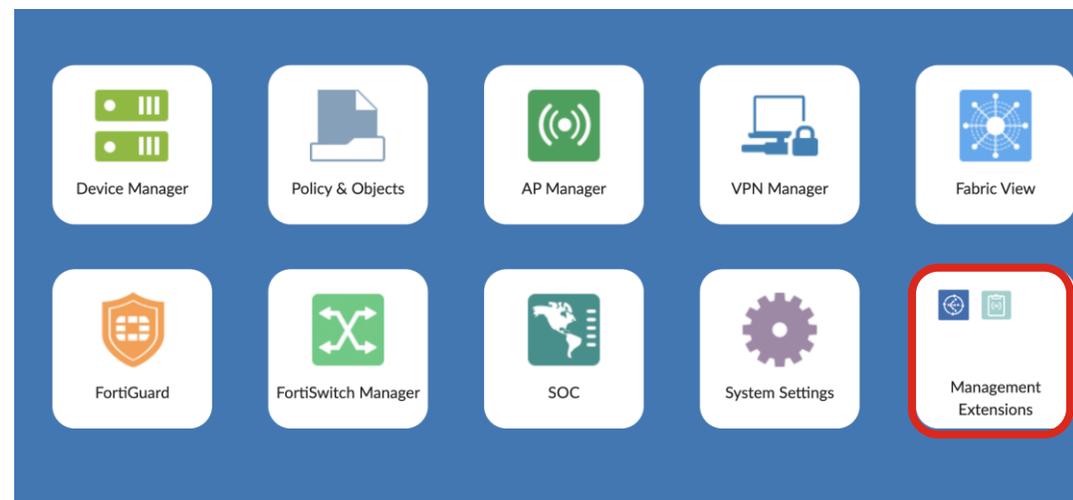
FortiManager использует FortiAnalyzer API ...



Расширенная консоль управления (6.4)

Возможность добавления расширенных возможностей управления

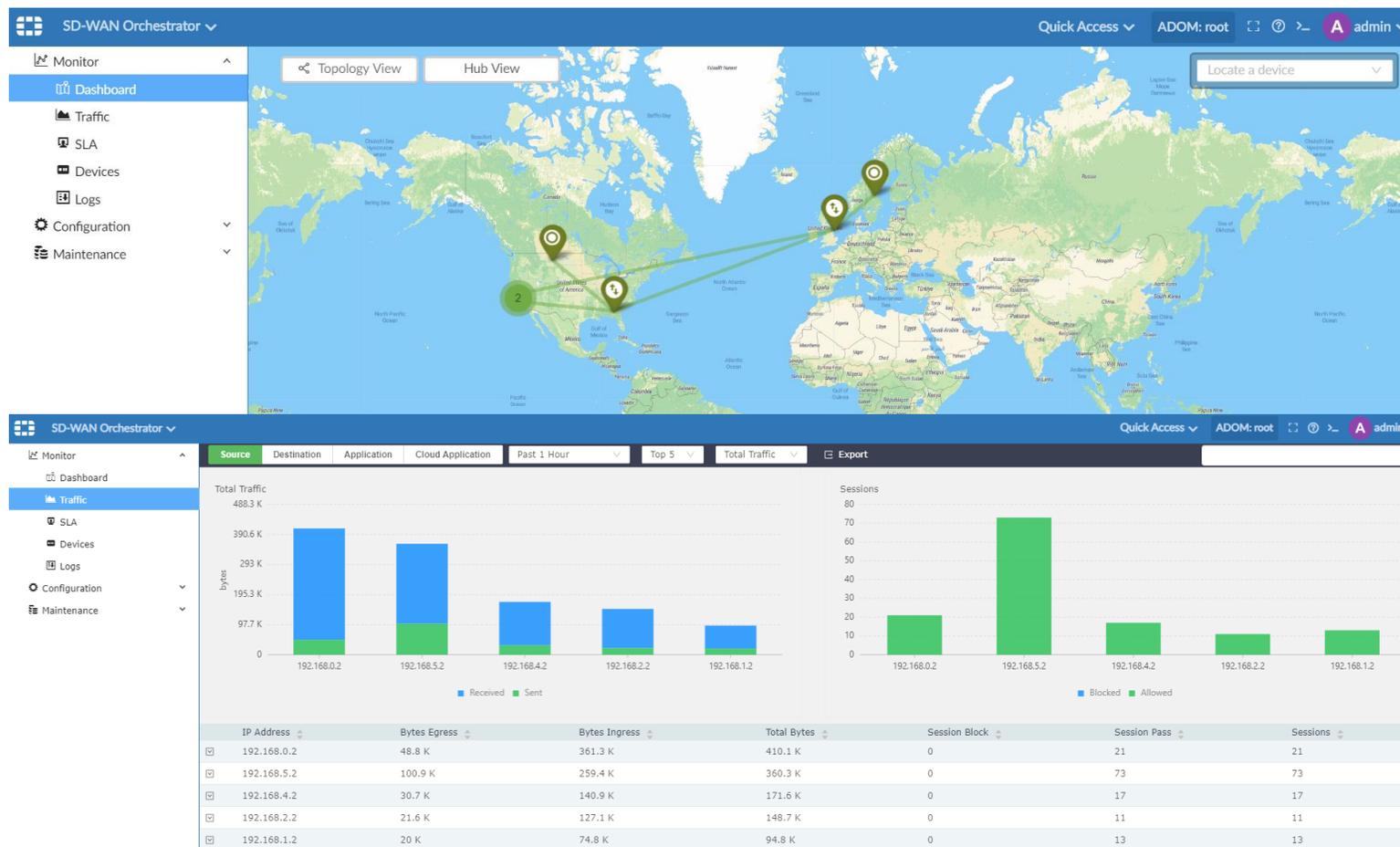
- Встроенный механизм для запуска контейнеров с расширениями возможностей управления
 - Только контейнеры от Fortinet (6.4)
 - Контейнеры загружаются в виде обновлений
 - Оповещение администраторов при возможности загрузки новых контейнеров
- Установка и удаление по запросу пользователей
- Может требоваться 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
- Требуется подписка 360 на FortiGate
- (все функции по управлению SD-WAN за пределами SD-WAN Orchestrator доступны без подписки)



Управление политиками – административные домены

Select an ADOM

Заблокировано
MSSP: *admin1*

 root FortiGate 5.4	 CUSTOMER_001 FortiGate 5.4	 CUSTOMER_002 FortiGate 5.4
 CUSTOMER_003 FortiGate 5.4	 CUSTOMER_004 FortiGate 5.4	 CUSTOMER_005 FortiGate 5.4
 CUSTOMER_006 FortiGate 5.4	 CUSTOMER_007 FortiGate 5.4	 CUSTOMER_008 FortiGate 5.4
 CUSTOMER_010 FortiGate 5.4	 CUSTOMER_011 FortiGate 5.4	 CUSTOMER_012 FortiGate 5.4
 CUSTOMER_013 FortiGate 5.4	 CUSTOMER_014 FortiGate 5.4	 CUSTOMER_015 FortiGate 5.4
 CUSTOMER_016 FortiGate 5.4	 CUSTOMER_017 FortiGate 5.4	 CUSTOMER_018 FortiGate 5.4
 CUSTOMER_019 FortiGate 5.4	 CUSTOMER_020 FortiGate 5.4	 FortiCarrier FortiCarrier 5.4
 FortiSandbox FortiSandbox	 Syslog Syslog	 Chassis -
 Global Database Global 5.4		



Заблокировано
API: *user2*

Заблокировано
MSSP: *admin2*

Заблокировано
CUSTOMER: *user1*

Заблокировано
API: *user3*

Close

Управление политиками – глобальная политика

Глобальные политики

Header Global Policies – глобальная политика

ADOM #1
Обычная Политика

ADOM #2
Обычная Политика

Footer Global Policies – глобальная политика

Управление политиками – общие фрагменты политики

Блоки политик

Header Global Policies – глобальная политика

ADOM #1
Обычная Политика #1

ADOM #1
Обычная Политика #2

Footer Global Policies – глобальная политика

Управление политиками – общие фрагменты политики

Блоки политик

Header Global Policies – глобальная политика

ADOM #1 Обычная Политика #1

ADOM #1 Блок политик А

ADOM #1 Обычная Политика #1

ADOM #1 Блок политик В

ADOM #1 Обычная Политика #1

ADOM #1 Обычная Политика #2

ADOM #1 Обычная Политика #2

ADOM #1 Блок политик В

ADOM #1 Обычная Политика #2

ADOM #1 Обычная Политика #2

Footer Global Policies – глобальная политика

Управление политиками – общие объекты

Policy & Objects Policy Packages Object Configurations

Policy Package Install ADOM Revisions Tools Collapse All Object Selector

Search...

- PP_BRANCHES
 - IPv4 Policy
 - Central SNAT
 - Installation Targets
 - PP_HUBS
 - default
 - Policy Blocks (0)

#	Name	Source	Destination	Sch
	iLAN -> iWAN (1-1 / Total: 1)			
	Outgoing Traffic (1-1 / Total: 1)			
1	Google Corporate	nLAN	all	
	Implicit (2-2 / Total: 1)			

Edit Address

Address Name: nLAN

Color:

Type: Subnet

IP/Netmask: 0.0.0.0/255.255.255.255

Per-Device Mapping: ON

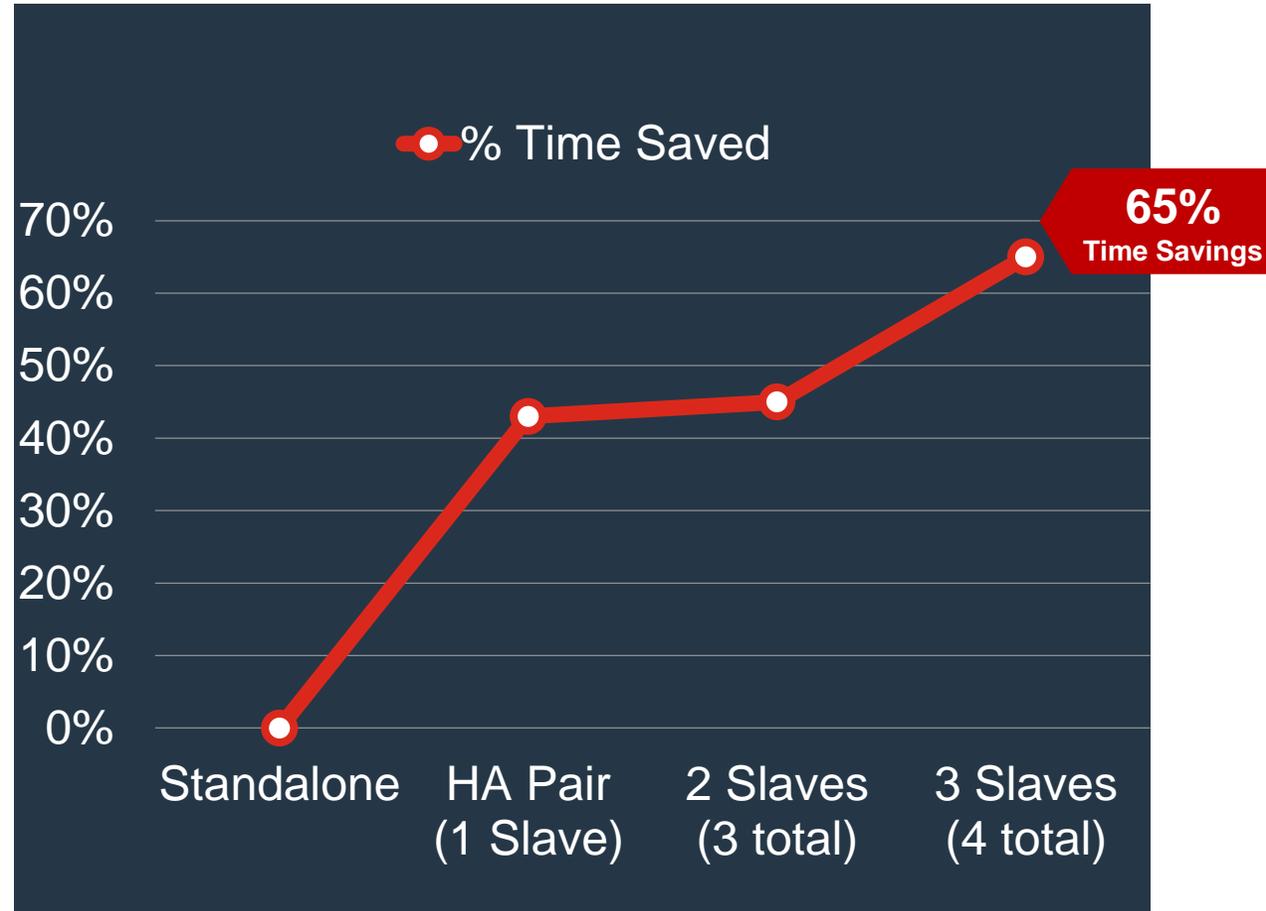
+ Create New Edit Delete Column Settings

Name	VDOM	Details
peer11	root	IP/Netmask:10.11.0.0/255.255.255.0
peer12	root	IP/Netmask:10.12.0.0/255.255.255.0
peer13	root	IP/Netmask:10.13.0.0/255.255.255.0
peer14	root	IP/Netmask:10.14.0.0/255.255.255.0
peer21	root	IP/Netmask:10.21.0.0/255.255.255.0
peer22	root	IP/Netmask:10.22.0.0/255.255.255.0
peer23	root	IP/Netmask:10.23.0.0/255.255.255.0
peer24	root	IP/Netmask:10.24.0.0/255.255.255.0
peer31	root	IP/Netmask:10.31.0.0/255.255.255.0
peer32	root	IP/Netmask:10.32.0.0/255.255.255.0
peer33	root	IP/Netmask:10.33.0.0/255.255.255.0
peer34	root	IP/Netmask:10.34.0.0/255.255.255.0

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

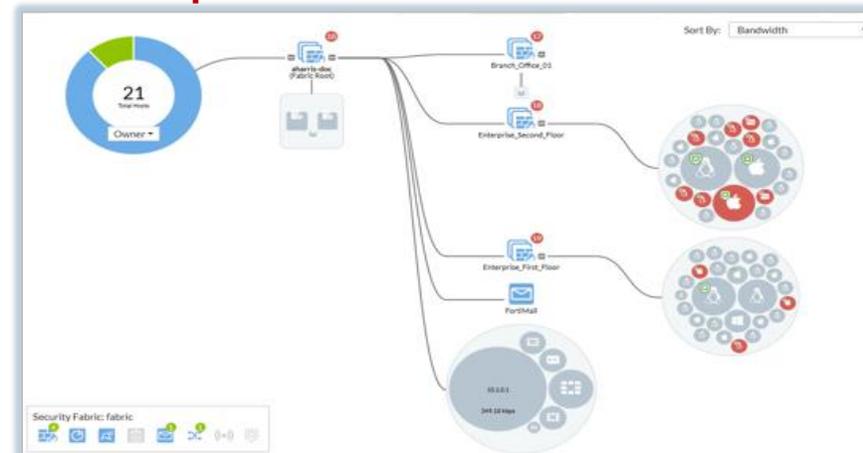
Информация о сети и защите в реальном времени

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



Forti View	Log View	Fabric View	SOC	Incidents & Events	Reports
Журналы трафика	Журналы событий	Журналы DNS	Журналы безопасности		

Мониторинг VPN

VPN Manager | IPsec VPN | Monitor | Map View | SSL VPN

ADOM: CM-LAB-001 | Unlock | admin

VPN Community | Save | Install Wizard

All VPN Communities | MESH_001

Topology View | Traffic View | Show Table | Show Tunnel Down Only

Google | South Pacific Ocean | North Atlantic Ocean | South Atlantic Ocean

Map data ©2017 Google, INEGI | Terms of Use

Bring Tunnel Up | Bring Tunnel Down | Column Settings

Status	Device	Name	Type	Remote Gateway	Incoming Data	Phase 2 Proposal	Uptime
Down	FG200D-tiger-dut-194-112[root]	MESH_001_4	automatic	192.168.195.146	0.0 KB	1	20s
Down	FG200D-tiger-dut-195-146[root]	MESH_001_1	automatic	192.168.194.76	0.0 KB	1	0s
Down	FG200D-tiger-dut-195-146[root]	MESH_001_2	automatic	192.168.194.77	0.0 KB	1	0s
Down	FG200D-tiger-dut-195-146[root]	MESH_001_3	automatic	192.168.194.112	0.0 KB	1	0s
Down	FG600C-tiger-dut-194-76[root]	MESH_001_4	automatic	192.168.195.146	0.0 KB	1	20s
Down	FG600C-tiger-dut-194-77[root]	MESH_001_4	automatic	192.168.195.146	0.0 KB	1	20s

Bring Tunnel Up
Bring Tunnel Down

Мониторинг SD-WAN

Представление в виде карты

The screenshot displays the Fortinet SD-WAN monitoring interface. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', 'License', 'Provisioning Templates', 'Scripts', and 'SD-WAN'. The user is logged in as 'admin' with the role 'ADOM: SDWAN'. The interface shows a map view of devices, with a table overlaying the map for 'fgt-branch1 (FortiGate-VM64-KVM)'. The table provides performance metrics for two interfaces: T-INET_0 and T-MPLS_0. A tooltip for 'ch1' on the map indicates a current latency of 109.47 ms, which is significantly higher than the configured 50 ms.

VDOM	SD-WAN Template	Interface	Performance SLA	Jitter (ms)	Latency (ms)	Packet Loss	Bandwidth		Session
							TX	RX	
root	sdwan_template_corporate	T-INET_0	✓ HC 10.0.0.111(PING)	0.19	1.17	0%	1.2 Kbps	2.5 Kbps	1
		T-MPLS_0	✗ HC 10.0.0.111(PING)	0.40	109.47	0%	1.6 Kbps	4.1 Kbps	0

Map View | Table View | All Devices | Show Unhealthy Devices Only

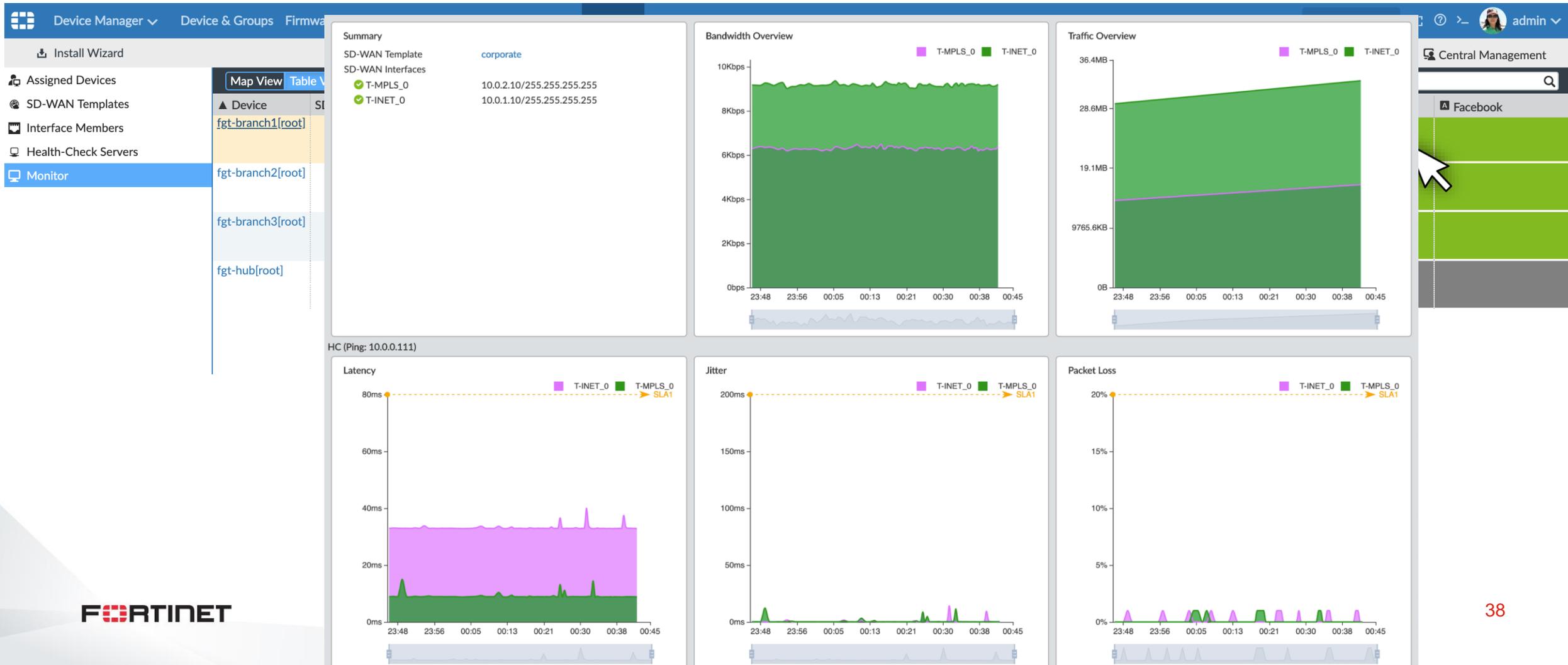
fgt-branch1 (FortiGate-VM64-KVM)

Current: 109.47 ms / Config: (#1) 50 ms

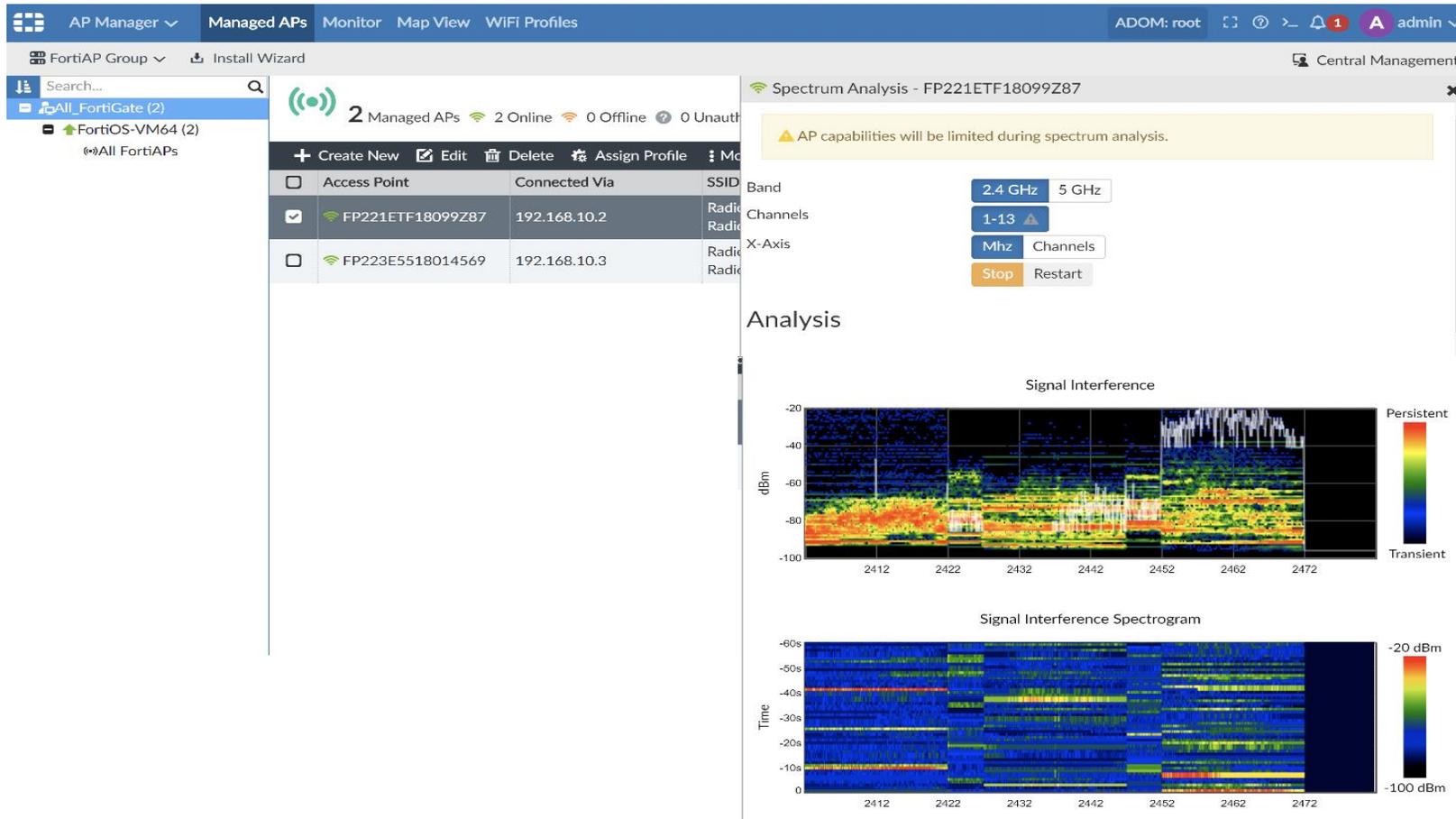
fgt-branch2

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

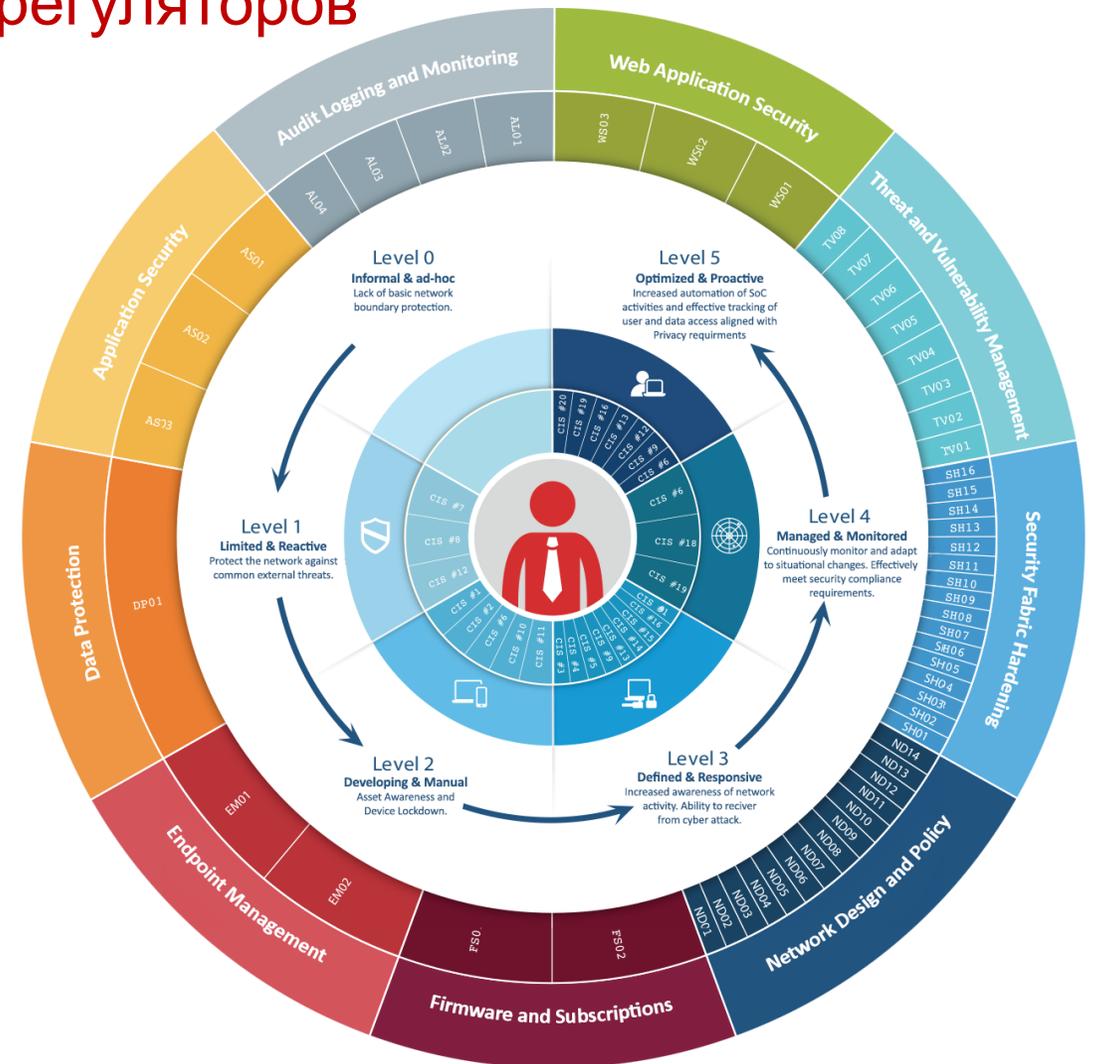
Упрощение соответствия требованиям регуляторов

Цели

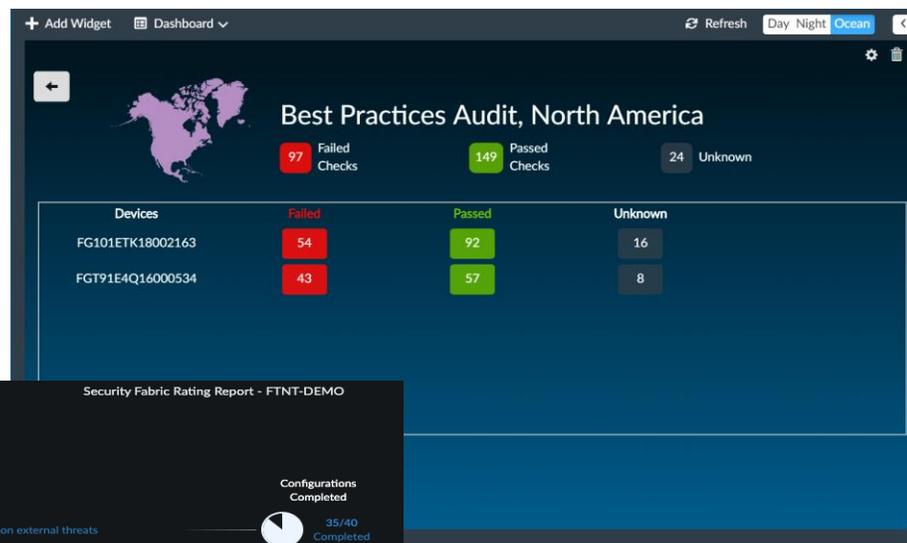
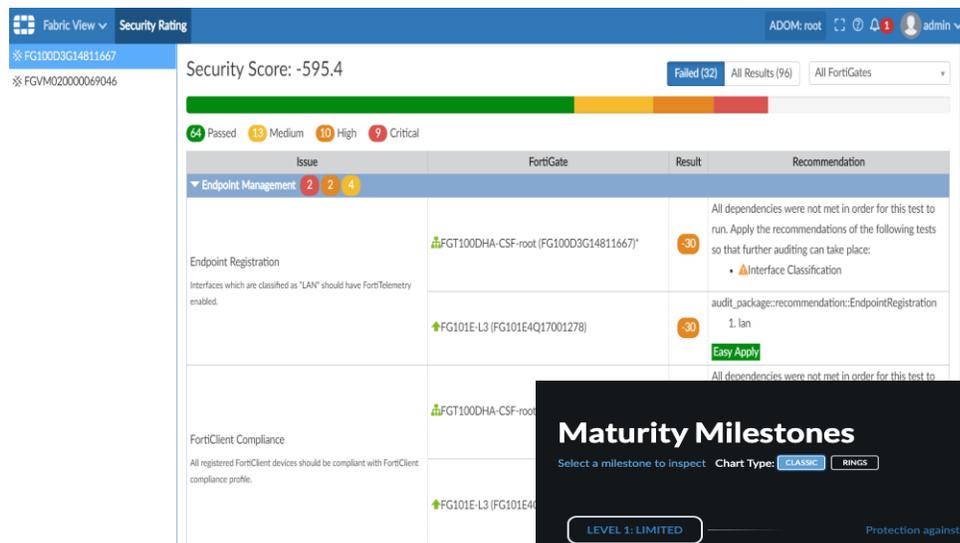
Снижение стоимости и сложности обеспечения соответствия требованиям регуляторов

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



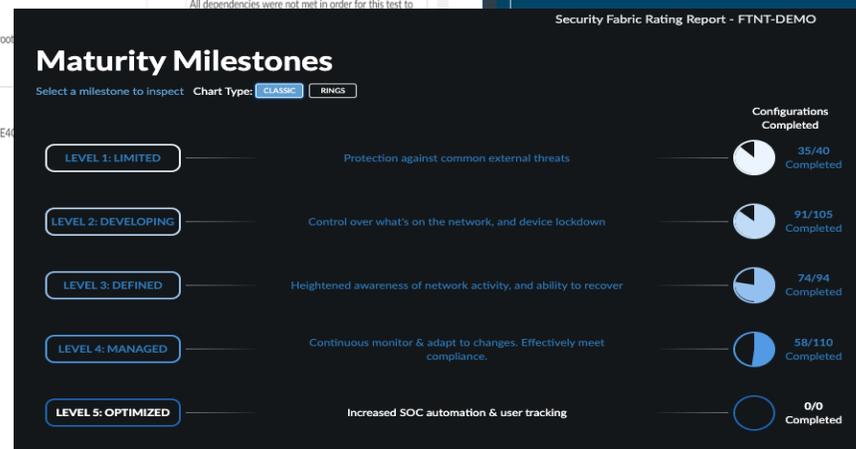
Security Rating – оценка конфигурации FortiGate



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

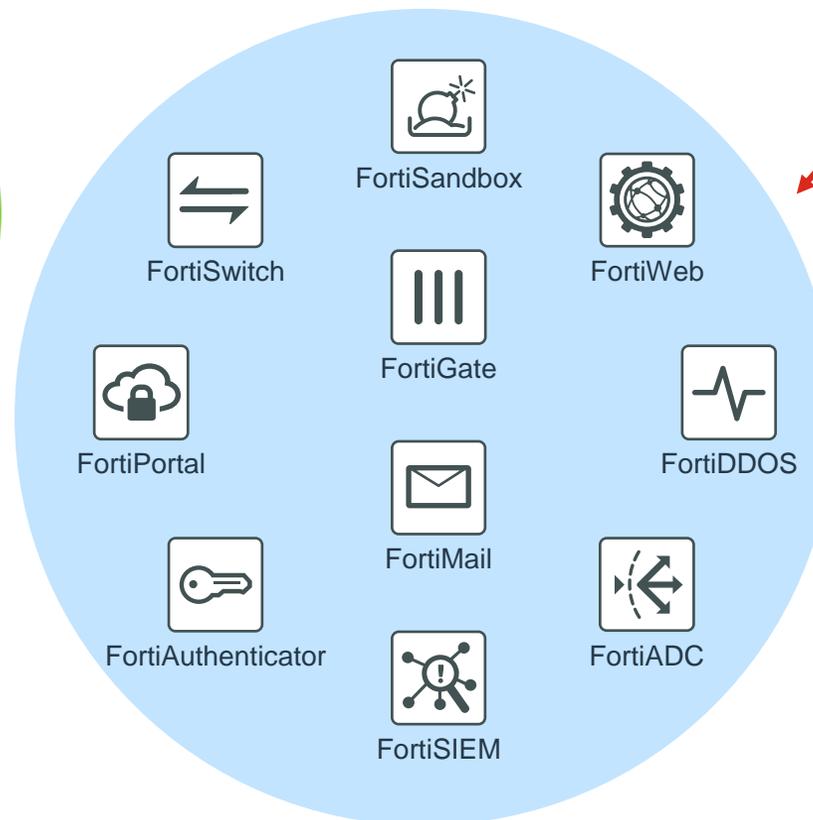
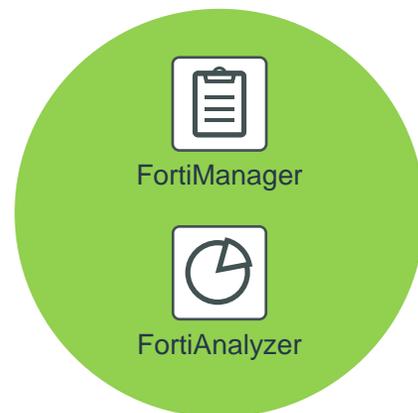
- Сопряжение (Connectors) с SDN и общими облаками (AWS/Azure/...)
- Интеграция с IT Service Management (ServiceNow)
- REST API и инструменты для автоматизации (fndn.fortinet.net)
- Возможность использования инструментов DevOps: Ansible, Teraform, и т.п.



Один продукт Fortinet = один API!

Все API работают поверх HTTP/HTTPS!

JSON RPC
XML SOAP

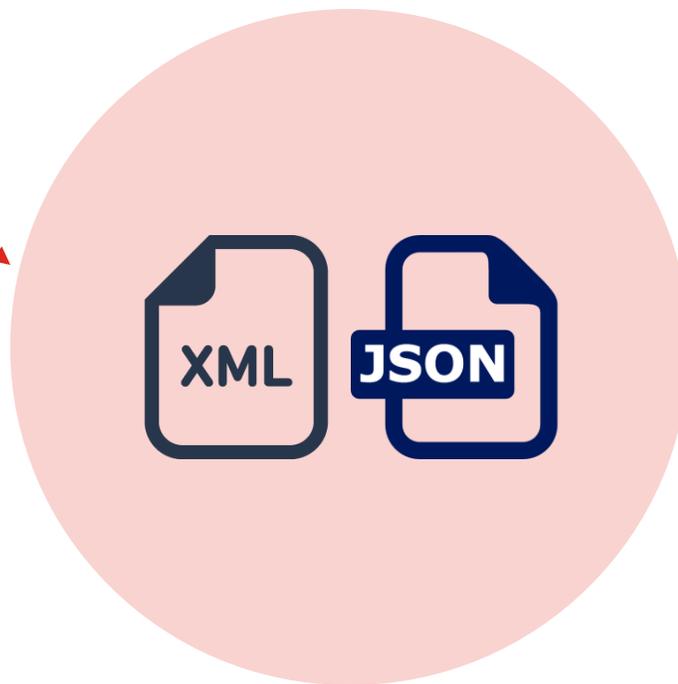


REST

Один продукт Fortinet = один API!

Все API работают поверх HTTP/HTTPS!

Формат
обмена
данными



Зачем нужен API

Настройка вручную медленная

Кликов

60

Восприятие



120_{sec}

Время

The screenshot shows the Fortinet FortiGate GUI. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', 'License', 'Provisioning Templates', and 'Scripts'. The user is logged in as 'admin' with ADOM 'CM-LAB-002'. The main content area shows the configuration for 'FGT5HD-001' under 'System Router'. A table of static routes is displayed with 10 entries. The table has columns for ID, Destination, Gateway, Interface, Distance, Priority, and Comments. The routes are all for the 'port1' interface with a distance of 10 and priority of 0.

ID	Destination	Gateway	Interface	Distance	Priority	Comments
1	10.100.0.0/255.255.255.0	10.0.0.254	port1	10	0	
2	10.101.0.0/255.255.255.0	10.0.0.254	port1	10	0	
3	10.102.0.0/255.255.255.0	10.0.0.254	port1	10	0	
4	10.103.0.0/255.255.255.0	10.0.0.254	port1	10	0	
5	10.104.0.0/255.255.255.0	10.0.0.254	port1	10	0	
6	10.105.0.0/255.255.255.0	10.0.0.254	port1	10	0	
7	10.106.0.0/255.255.255.0	10.0.0.254	port1	10	0	
8	10.107.0.0/255.255.255.0	10.0.0.254	port1	10	0	
9	10.108.0.0/255.255.255.0	10.0.0.245	port1	10	0	
10	10.109.0.0/255.255.255.0	10.0.0.254	port1	10	0	

Зачем нужен API (2)

Настройка с API гораздо быстрее

Время на добавление 10 статических маршрутов

GUI

120

сек

API

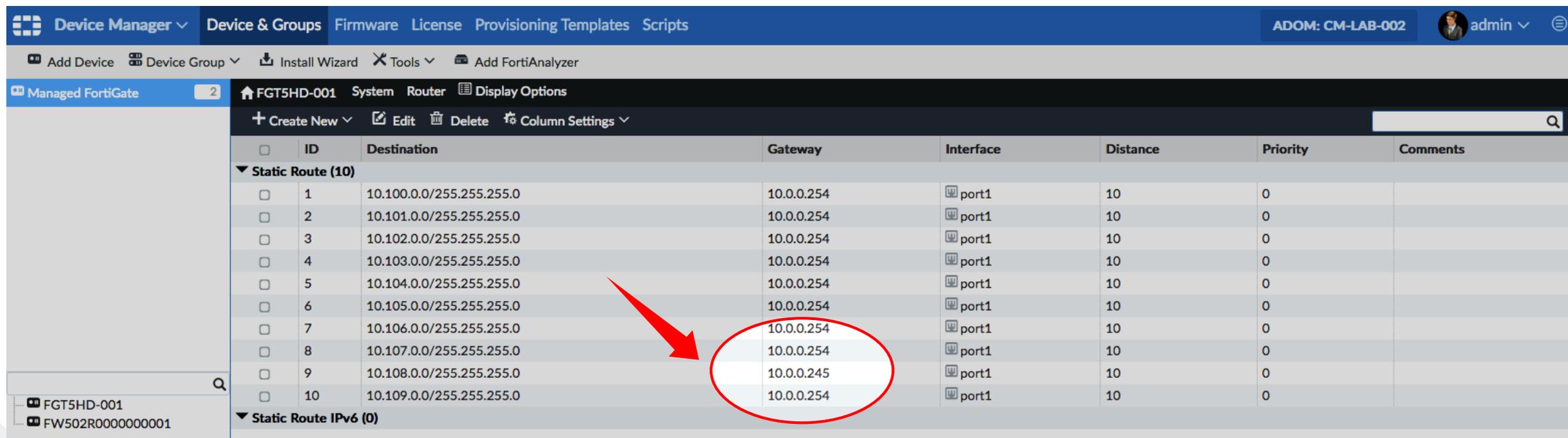
```
$ ./add-static-routes.py
```

```
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
```

Зачем нужен API (3)

Настройка с API менее подвержена ошибкам

Найдите ошибку



The screenshot shows the Fortinet Device Manager interface for a managed FortiGate. The main content area displays a table of static routes. A red arrow points to a specific row where the gateway IP address is 10.0.0.245, which is circled in red. This is an error because all other gateway IP addresses in the list are 10.0.0.254.

ID	Destination	Gateway	Interface	Distance	Priority	Comments
1	10.100.0.0/255.255.255.0	10.0.0.254	port1	10	0	
2	10.101.0.0/255.255.255.0	10.0.0.254	port1	10	0	
3	10.102.0.0/255.255.255.0	10.0.0.254	port1	10	0	
4	10.103.0.0/255.255.255.0	10.0.0.254	port1	10	0	
5	10.104.0.0/255.255.255.0	10.0.0.254	port1	10	0	
6	10.105.0.0/255.255.255.0	10.0.0.254	port1	10	0	
7	10.106.0.0/255.255.255.0	10.0.0.254	port1	10	0	
8	10.107.0.0/255.255.255.0	10.0.0.254	port1	10	0	
9	10.108.0.0/255.255.255.0	10.0.0.245	port1	10	0	
10	10.109.0.0/255.255.255.0	10.0.0.254	port1	10	0	

Описание функций API

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

The screenshot shows the FortiManager JSON API Documentation interface. On the left, there is a sidebar with a search bar and a tree view of API endpoints under 'FortiManager 6.2.0 GA'. The main content area displays the documentation for the '/dvmdb/adom' endpoint, which is described as an ADOM table. Two API methods are listed: 'POST /dvmdb/adom (add)' and 'POST /dvmdb/adom (get)'. The 'POST /dvmdb/adom (get)' method is expanded to show its parameters. A 'Try it out' button is visible. The parameters section includes a table with columns for 'Name' and 'Description'. A 'body' parameter is listed as required, with an example value shown in a dark box.

FortiManager

FortiAPI Forum

Search APIs

FORTIMANAGER - DVMDB/ADOM

FortiManager JSON API Documentation ^{6.2.0}

[Base URL: yourFMGip/jsonrpc]

/dvmdb/adom ADOM table, most attributes are read-only and can only be changed internally.

POST /dvmdb/adom (add)

POST /dvmdb/adom (get)

Parameters Try it out

Name	Description
body ^{required}	

(body)

```
{
  "method": "get",
  "params": [
    {
      "expand member": "string",
      "fields": [
        [
          "desc"
        ]
      ]
    }
  ]
}
```

Инструменты сопряжения (Fabric Connectors)

Новые Fabric Connectors

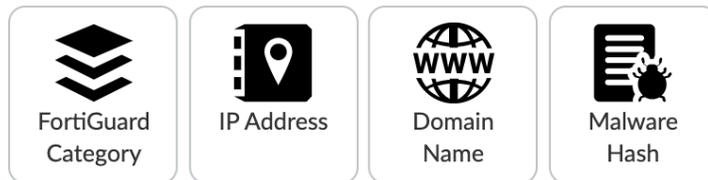
SDN (12) ▾



SSO/Identity (9) ▾



Thread Feeds (4) ▾



SOAR (3)



Зачем нужны Fabric Connectors

Лучше **осведомленность** => выше **эффективность**



SDN IP

IP Address
Public Cloud IP
User
User Group
FQDN
URL

Зачем нужны Fabric Connectors – пример (1)

- Создаём фильтр для поиска контейнеров по атрибутам

Filter Generator

Filter Logic

K8S_NodeName (1)
K8S_NodeName=ubuntu

K8S_Label.beta.kubernetes.io/arch (1)
K8S_Label.beta.kubernetes.io/arch=amd64

K8S_Label.beta.kubernetes.io/os (1)
K8S_Label.beta.kubernetes.io/os=linux

K8S_Label.kubernetes.io/arch (1)
K8S_Label.kubernetes.io/arch=amd64

K8S_Label.kubernetes.io/arch	K8S_Label.kubernetes.io/os
amd64	ubuntu

Filter Generator

Filter Logic

K8S_NodeName=ubuntu

K8S_NodeName	K8S_Label.beta.kubernetes.io/arch	K8S_Label.beta.kubernetes.io/os	K8S_Label.kubernetes.io/arch	K8S_Label.kubernetes.io/hostname	K8S_Label.kubernetes.io/os
ubuntu	amd64	linux	amd64	ubuntu	linux

Зачем нужны Fabric Connectors – пример (2)

Policy & Objects Policy Packages **Object Configurations**

ADOM Revisions Tools

Zone/Interface > + Create New Edit Delete Column Settings More

Firewall Objects

Addresses

Wildcard FQDN Addresses

Name	Type	Details
<input type="checkbox"/> KUBERNETES-typ18	Firewall Address	Fabric Connector Address:(myK8DemoHost)



Dashboard Security Fabric FortiView Network System Policy & Objects Consolidated Policy Authentication Rules IPv4 DoS Policy IPv6 DoS Policy Addresses

View Search

ID	Name	From	To	Source	Address	Type	SDN Connector	Filter	Interface	Resolved To	References
1	myv6Host	<input type="checkbox"/> any	<input type="checkbox"/> any	all myTestv6HO myv6host2	KUBERNETES-typ18	Fabric Connector Address	myK8DemoHost	K8S_NodeName=ubuntu	<input type="checkbox"/> any	172.17.17.50	1
2	myv4Host1	<input type="checkbox"/> any	<input type="checkbox"/> any	001HOST1 all							
1071741825	myBlock1-BlockConsolidated	<input type="checkbox"/> any	<input type="checkbox"/> any	004HOST4 all							
4	k8Policy	<input type="checkbox"/> any	<input type="checkbox"/> any	KUBERNETES-typ18 all							

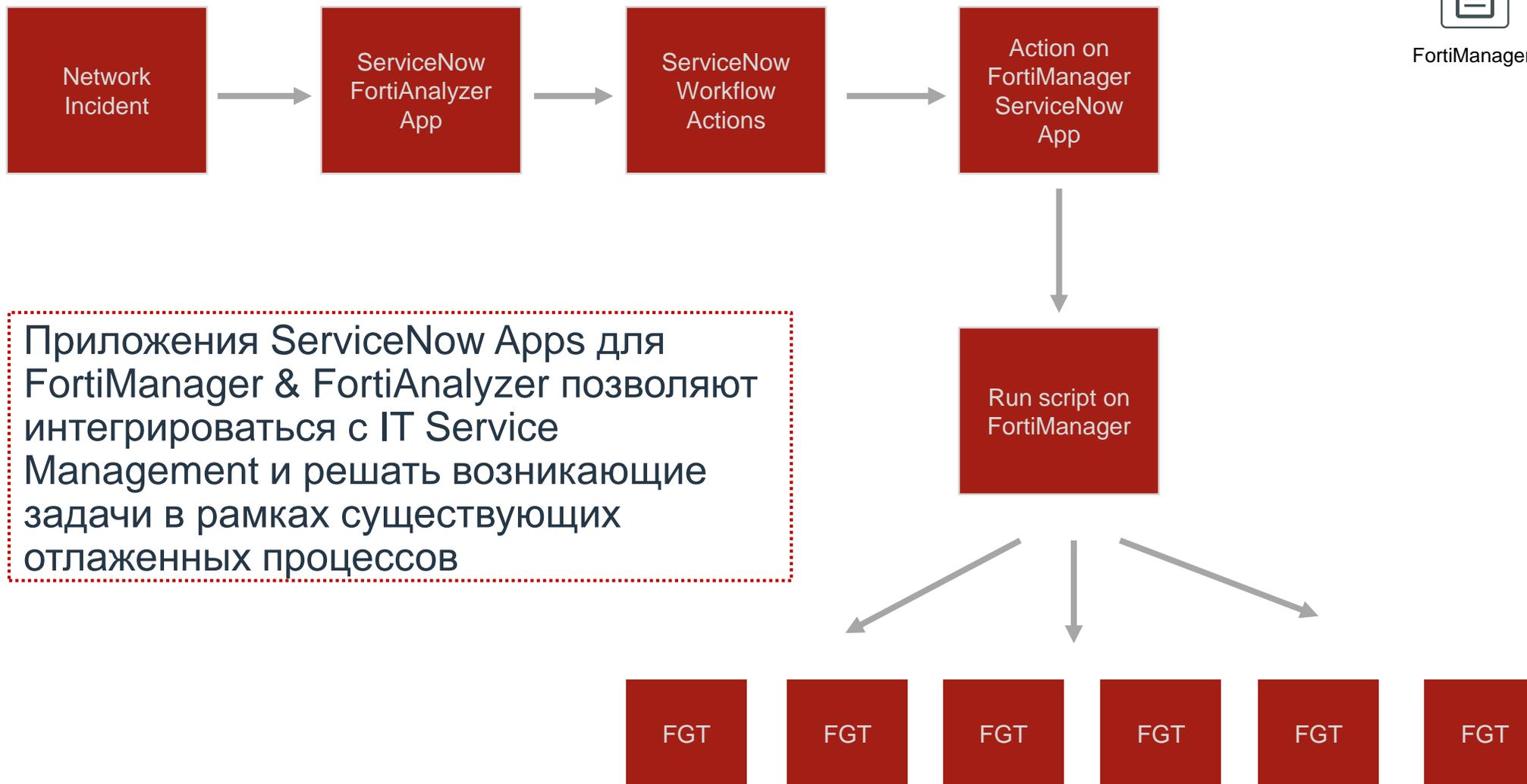
Address: KUBERNETES-typ18
Type: Fabric Connector Address
SDN Connector: myK8DemoHost
Filter: K8S_NodeName=ubuntu
Interface: any
Resolved To: 172.17.17.50
References: 1

View

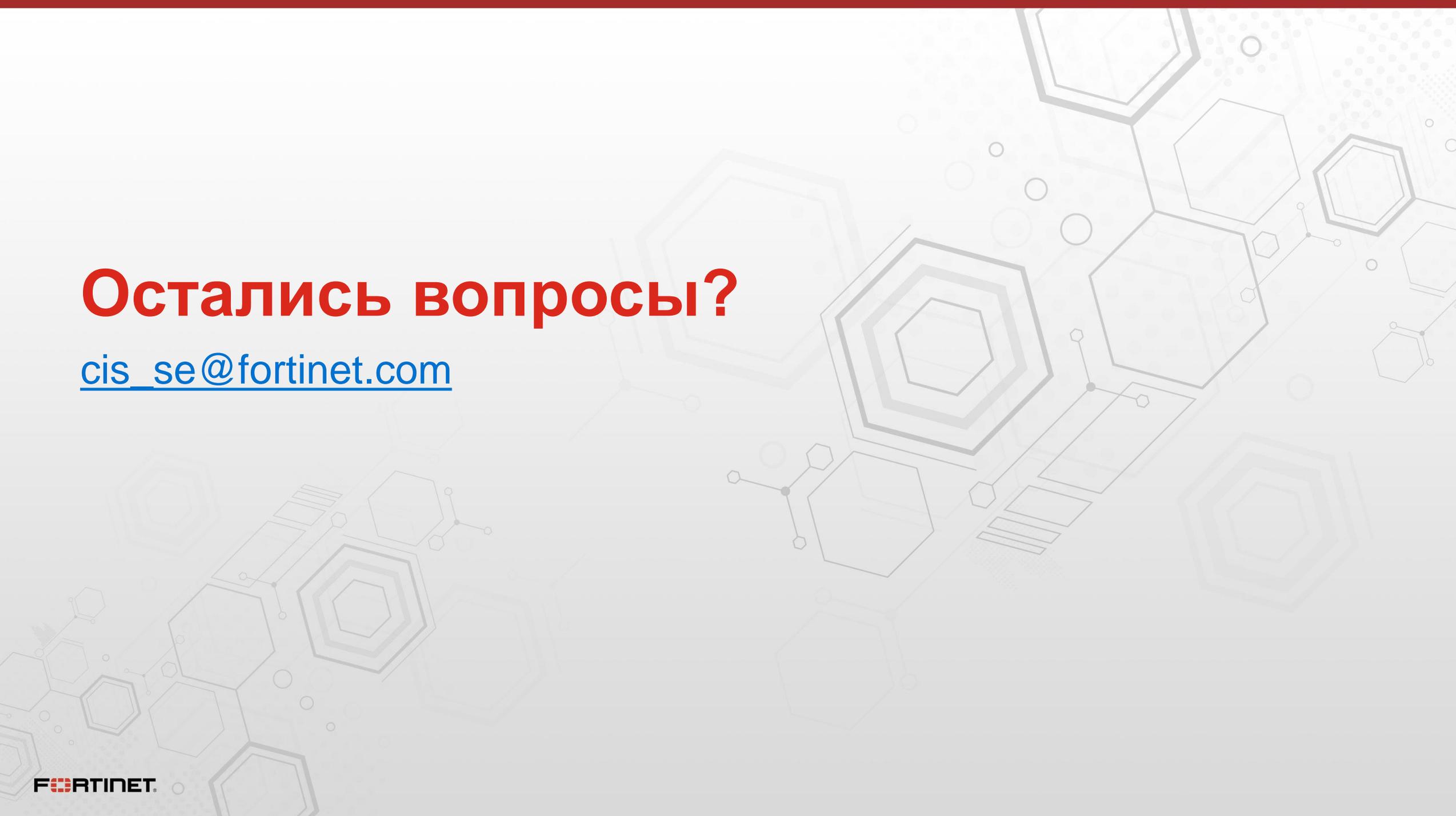
Интеграция FortiManager и FortiAnalyzer с ServiceNow



FortiManager FortiAnalyzer



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

The background features a light gray gradient with a complex pattern of overlapping hexagons and circuit-like lines. Some hexagons are solid, while others are outlines. The lines resemble a network or data flow diagram, with small circles at the nodes.

Остались вопросы?

cis_se@fortinet.com