DIGITAL EDITION

FORTINET®

SECURITY DAY

FortiOS 7.0 - новые функции и демонстрация особенностей обновленной ОС

Чингис Татаев, системный инженер

6 апреля 2021 | Киев | Минск

Ускоряющаяся конвергенция сети и безопасности

01 **Уменьшить площадь поверхности атаки**

Полная осведомленность, сегментация и защита от угроз с помощью Security Fabric и Enhanced FortiGuard Services

02 **Консолидировать и ускорить**

Сетевые функции и функции безопасности (например IPS, Web Filtering) на любом масштабе (Hyperscale) с использованием SPU

03 **Автоматизировать управление и реагирование на инциденты**

Защита гибридных IT с помощью расширенных функций Fabric Automation и Unified Console

Fortinet Security Fabric

Обширная

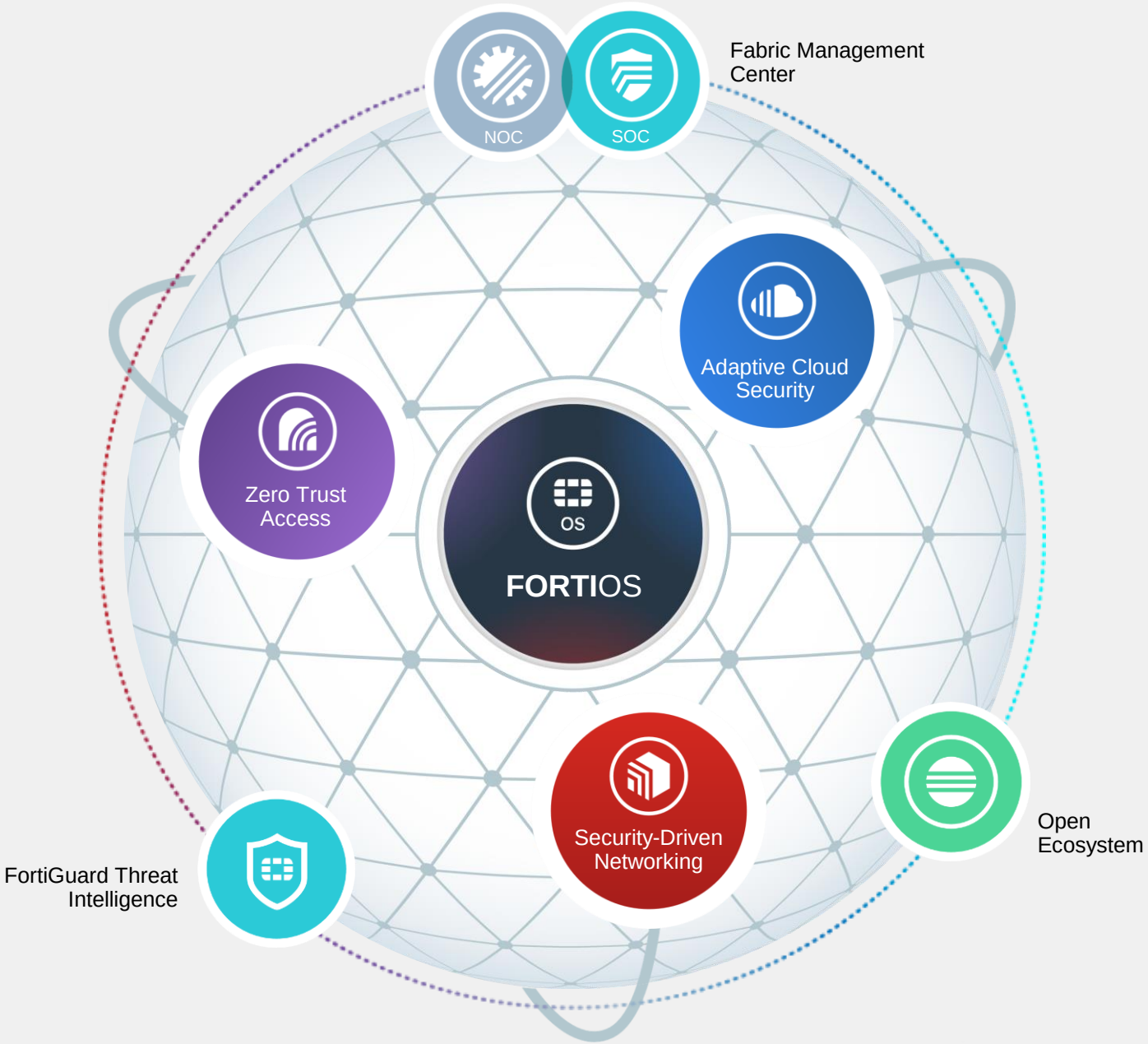
Осведомленность и защита по всей цифровой плоскости атаки для лучшего управления рисками

Интегрированная

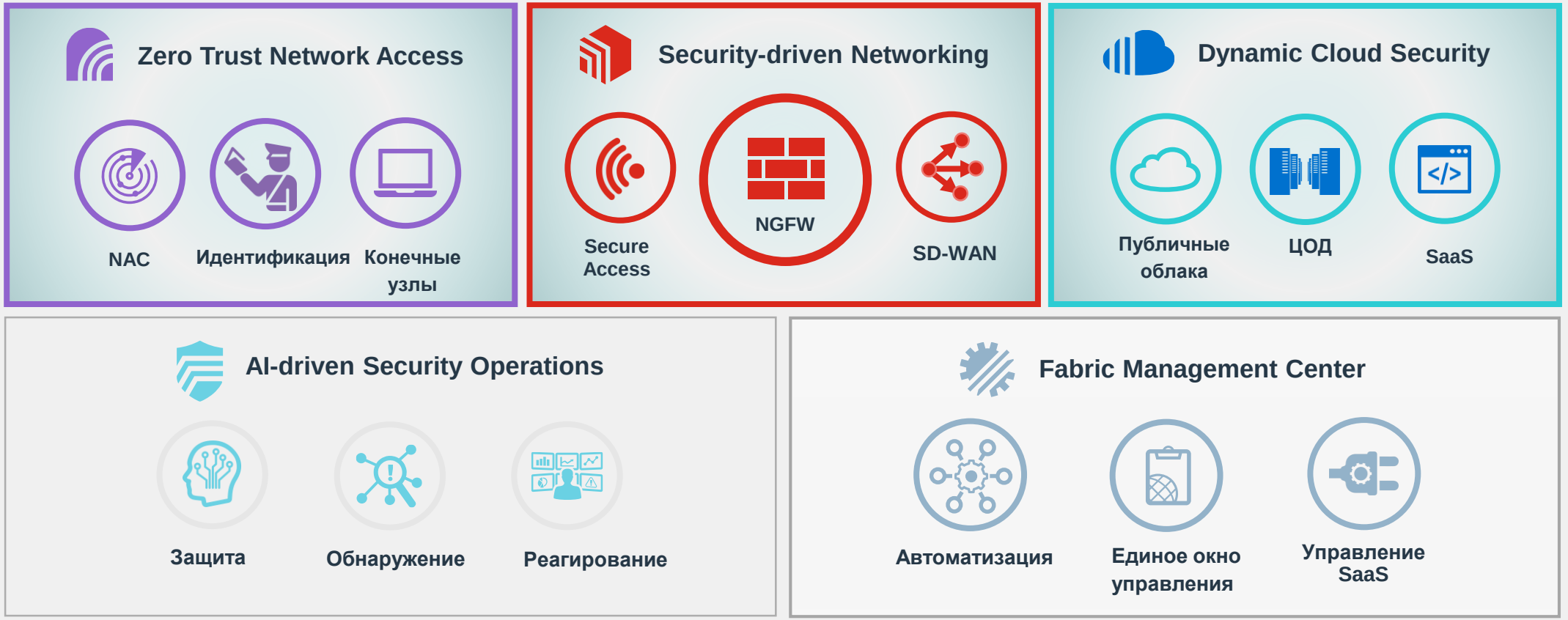
Уменьшение сложности управления и обмен данными об угрозах

Автоматизированная

Самовосстанавливающиеся сети с поддержкой безопасности на основе AI для быстрой и эффективной работы

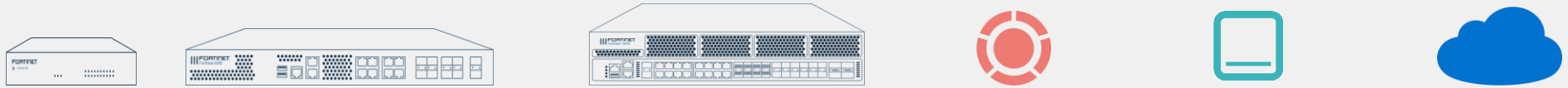


Обеспечение комплексной кибербезопасности с помощью Fortinet Security Fabric



Устройства | Виртуальные машины | SaaS | Облака | Агенты | Контейнеры

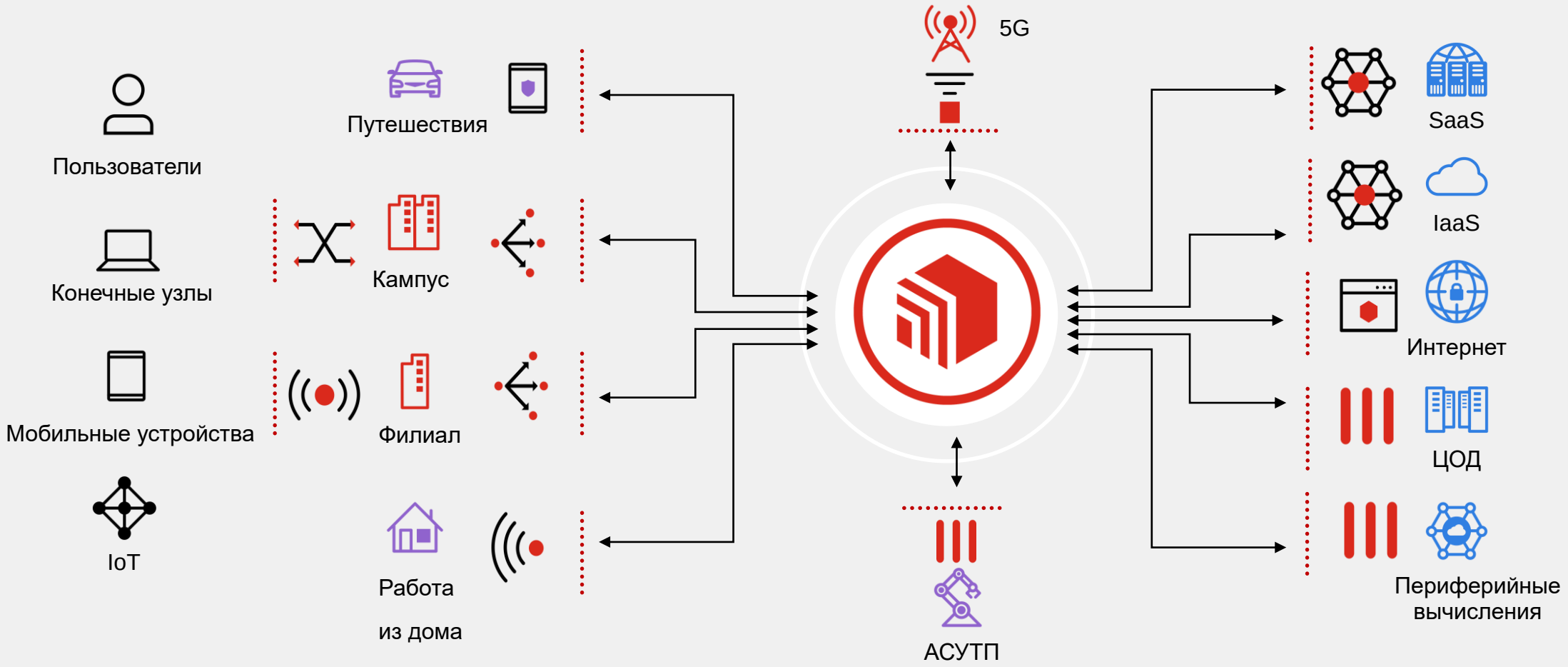
Операционная система FortiOS



Филиал | Кампус | ЦОД | Встраиваемые решения | Виртуальные машины | Облачные решения

Необходимость защиты в любой точке подключения

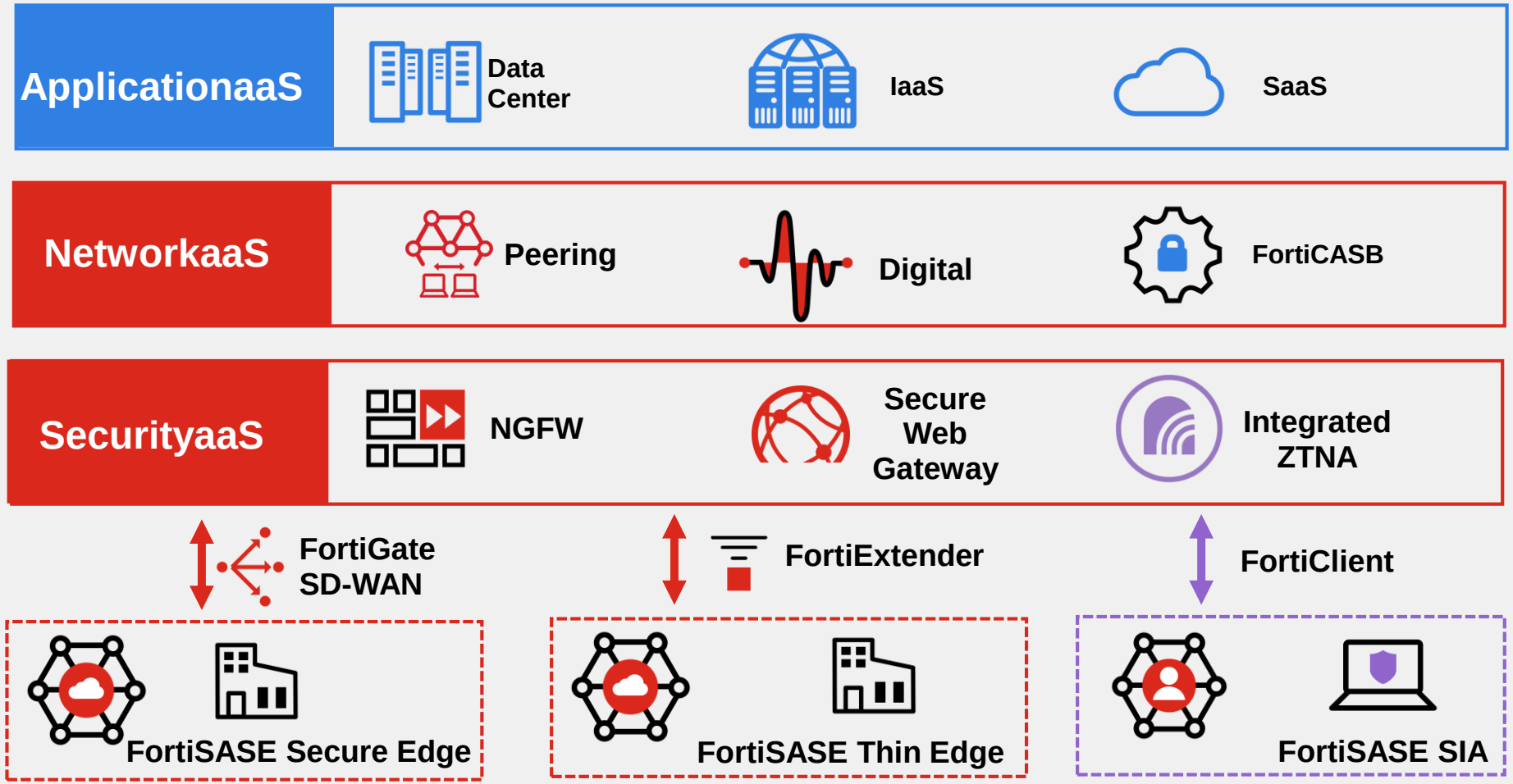
Security-driven Networking



Что такое FortiSASE ?

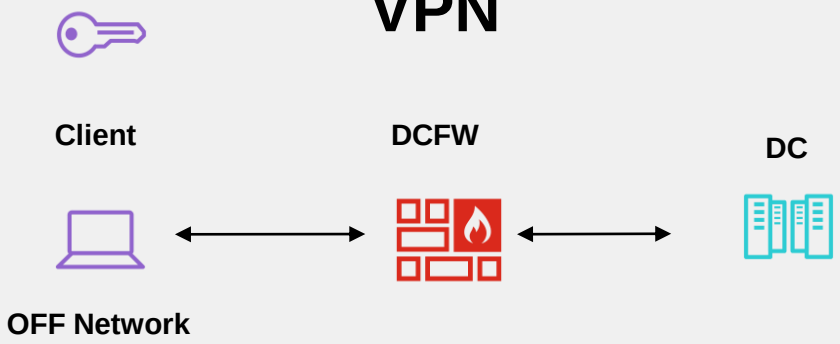
Облачный сервис обеспечения безопасного доступа к приложениям и сервисам организации для любого типа доступа (Access Edge)

- **Мониторинг эффективности работы корпоративных приложений и сервисов**
- **Сетевая безопасность с высокими независимыми оценками эффективности**
- **Наиболее гибкие возможности обеспечения доступа**



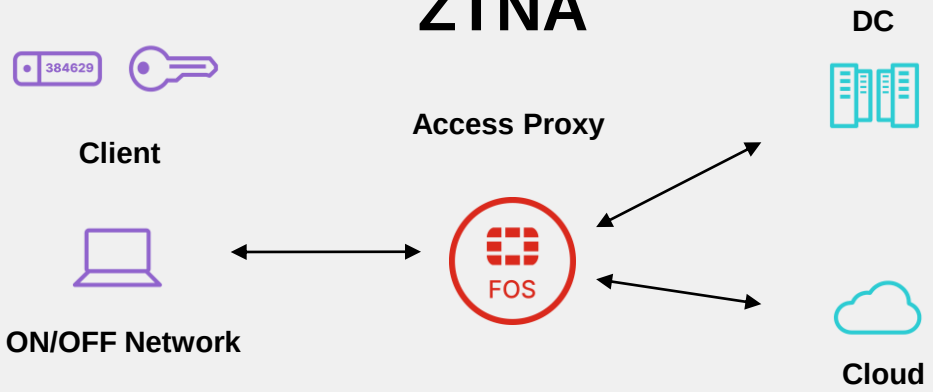
Эволюция традиционных VPN в ZTNA

VPN



- Однократная проверка доверия
- Доступ ко всей сети
- Базовый статический набор правил доступа

ZTNA

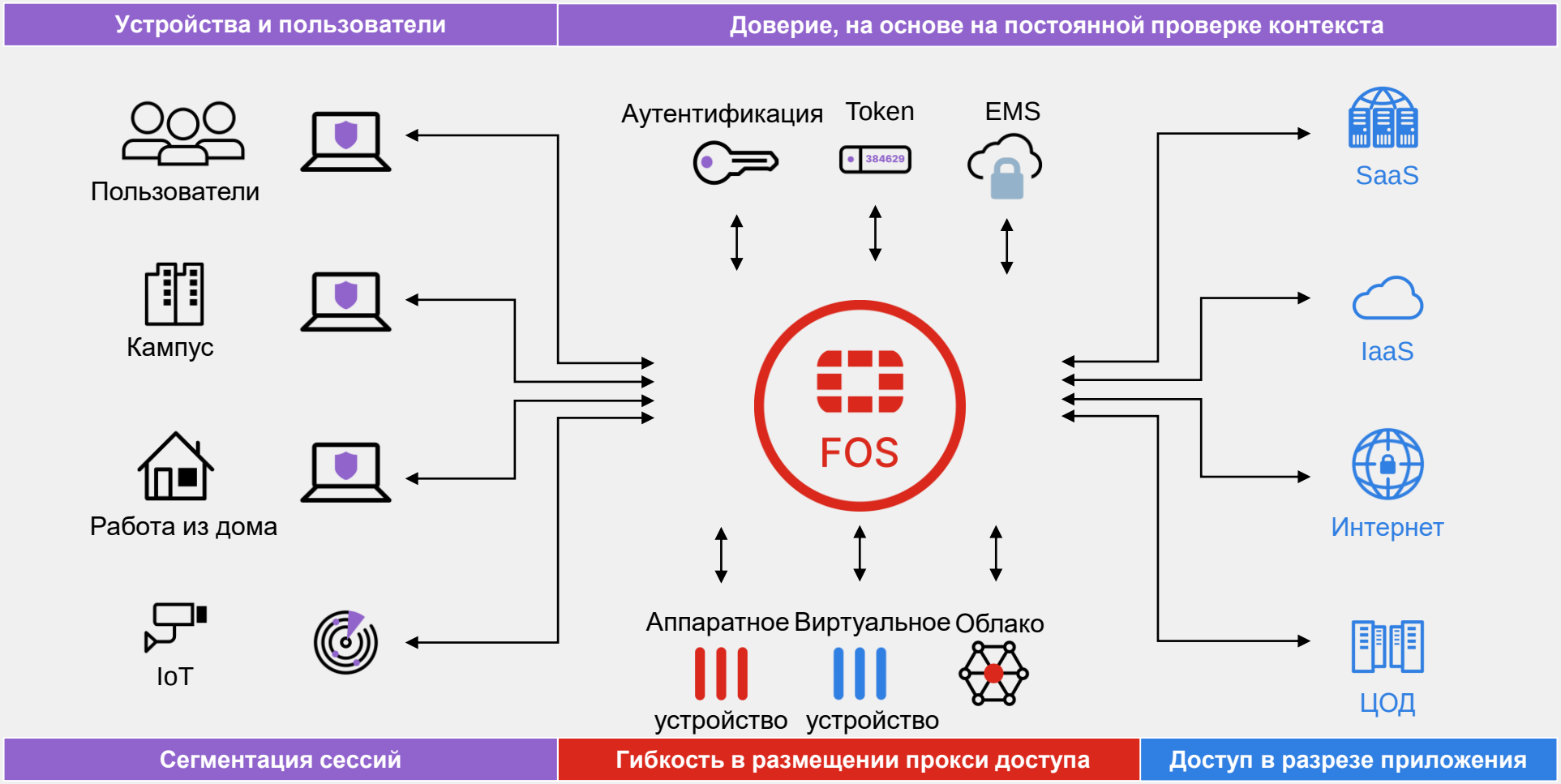


- Постоянная проверка доверия
- Доступ только к определенным приложениям
- Динамический доступ в зависимости от текущего контекста безопасности

Cloud

Видение Zero Trust Access (ZTA)

Безопасный доступ к приложениям в любое время и из любого места



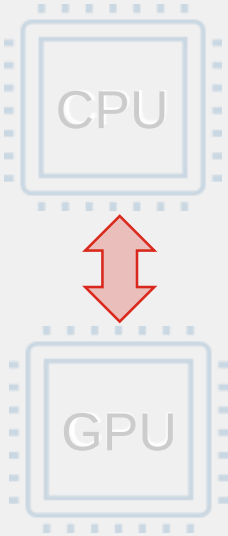
Fortinet SPU и FortiGate

Модули аппаратной обработки SPU трафика и обновление портфолио шлюзов безопасности FortiGate

Fortinet разрабатывает собственные SPU

Ускорение задач обработки сетевого трафика и задач инспекции

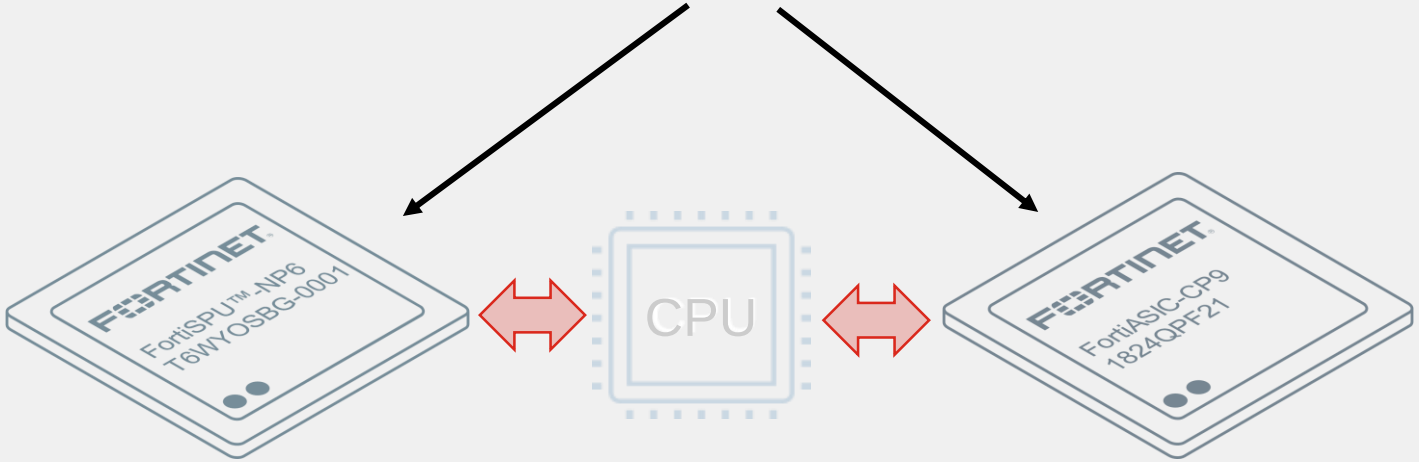
Игровые системы и задачи AI



Графический процессор (или GPU)

Ускоряют обработку и рендеринг графической информации от CPU

Security Processing Unit (SPU)



Network Processor (NP)

Занимается задачами обработки сетевого трафика

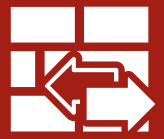
Content Processor (CP)

Занимается задачами инспекции

Вызовы масштабируемости – SPU NP7

Сложно решаются текущими решениями и технологиями

Сегментация сети

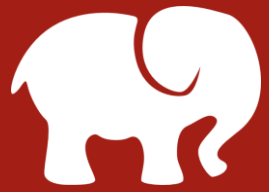


Аппаратное ускорение VXLAN

Высокопроизводительный VPN

75Gbps IPsec

Поддержка Elephant Flows



Интерфейсы 100G

Работа в динамических средах

Огромный темп установки соединений

Чувствительные к задержкам приложения

Минимальные задержки при обработке

Защита от атак

Аппаратная защита от атак DDoS

Выполнение требований 5G

Журналирование и CGNAT

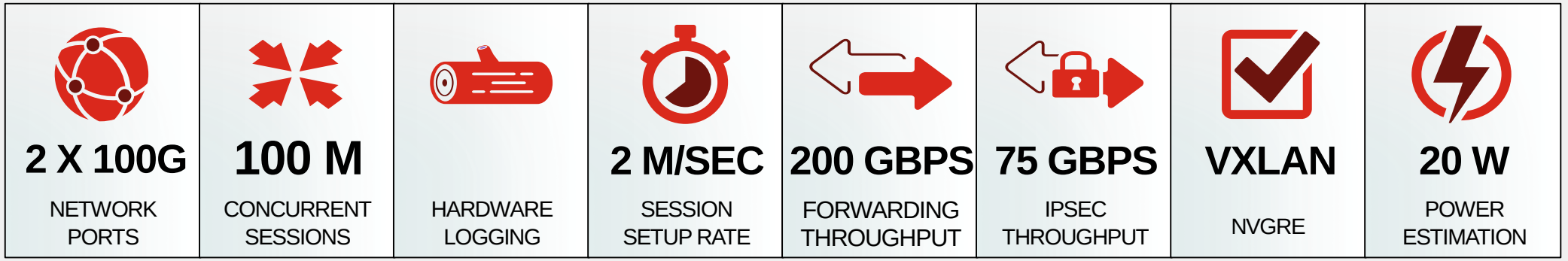
Тяжёлый трафик (UHD TV)

200Gbps пропускная способность одного SPU

SPU NP7 - новые ориентиры производительности

Улучшения NP7 в числах

Характеристика	NP6	NP7	Изменение	Возможные сценарии
Elephant Flows	10Gbps	**100Gbps**	**10x**	**Большие объёмы данных**
Connections Per Second	CPU based	**2M CPS**	**New**	**Динамические нагрузки**
IPSec Encryption	25Gbps	**75Gbps**	**3x**	**Производительный VPN**
Firewall Throughput	40Gbps	**200Gbps**	**5x**	**МСЭ (L4 Stateful Firewall)**
VXLAN Acceleration	-	**Доступно**	**New!**	**Сегментация, виртуализация сети**
Hardware Logging	-	**Доступно**	**New!**	**Все сценарии**



FortiGate 4400F

Powered by NP7 and CP9

Q3/20

Redundant PSU

Hot Swappable Fans

Производительность

1.2 Tbps
Межсетевой экран

80 Gbps
NGFW

65 Gbps
SSL инспекция

90 Gbps
IPS

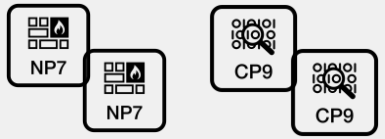
70 Gbps
Threat Protection

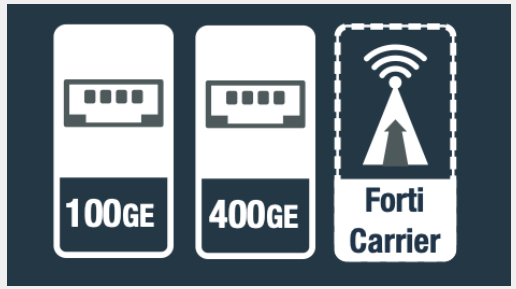
*All performance are preliminary performance targets subject to change

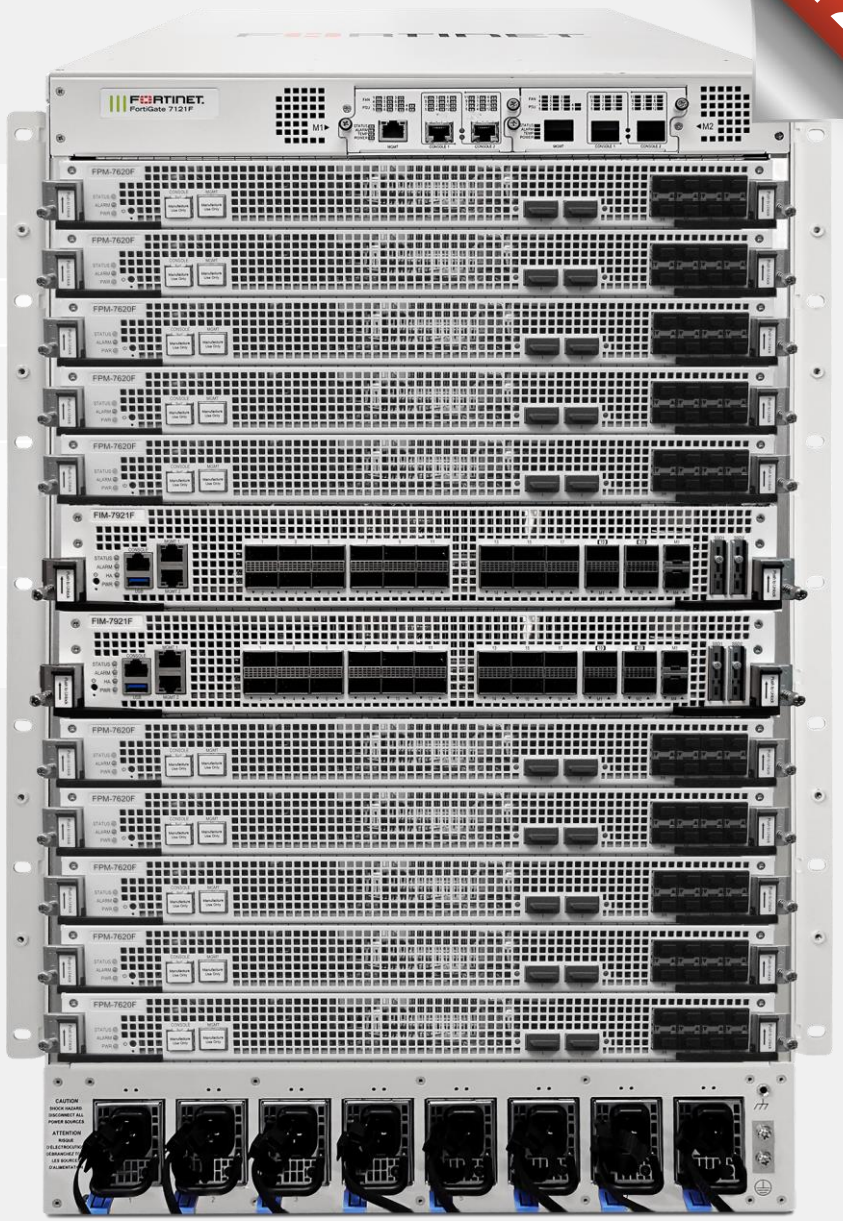
Шасси FortiGate 7121F

Powered by NP7 and CP9

Форм-фактор	16 RU
Производительность МСЭ	**1.9 Tbps***
Сетевые интерфейсы	10GE / 25GE / 40GE / 100GE / **400GE**
Производительность	**520G IPS (Intrusion Protection)* 450G Threat Protection***







1H 2021

Large Enterprise / Data Center / Service Provider

NGFW / ISFW / DCFW /CCFW

Flexible Deployment Options

*Целевые показатели производительности.

FortiOS 7.0

Более 300+ новых функциональных возможностей

Основные инновации в FortiOS 7.0

Уменьшение поверхности атаки

Video Filtering Service

Новый сервис **категоризации видео** для соответствия требованиям и контроля доступа к контенту

Expanded DNS Security

Расширение функций **безопасности DNS** для защиты пользователей, трафика и DNS-инфраструктуры

Консолидация и ускорение

Ultra-scalable Chassis

Масштабируемость по модели Pay-as-you-grow до **максимальных в индустрии** значений производитель-ности

400G I/O Support

Построение безопасных DCI с **ультравысокой** производитель-ностью

Автоматизация сети

Automated Upgrades

Автоматические **обновления ПО** (FG, FAP, FSW firmware) для выполнения соответствия требованиям

Learn Mode

Режим обучения для оптимизации политик, эффективного предотвращения работы теневого ИТ (Shadow IT).

FOS 7.0 – это 300+ новых функций

Security Driven Networking (**SASE Edge -** SASE)

- Securing remote workforce with orchestration portal for SASE capabilities
- Securing thin branch with FEX 200F + 25Mbps subscription
- New Thin Edge line us (LTE/5G)
- Journey to Zero Trust with extended risk posture checking

Security Driven Networking (**WAN Edge:** SD-WAN)

- Increased Resiliency (FEC/DUP)
- Enhanced packet duplication
- Accelerated Convergence (FWF 80F)
- Efficient Operations (scalable ZTP, Analytics, Passive WAN Measurement)
- Accelerated convergence for Thin & WAN edge

Security Driven Networking (**DC Edge:** NGFW)

- Ultra-Scalability with pay as you grow model (FGT 7121F, 400G)
- Attack surface Reduction (Video filtering , DNS)
- Efficient Operations with network automation (Policy Learn mode, automated upgrades)

Security Driven Networking (**LAN Edge:** WiFi/Switch)

- Unified code base (L3 FortiLink, NAC Visibility and Zero trust response)
- Convergence (WLM and AIOps on FMG, FortiLAN cloud)
- Simplified Operation AI/ML driven wireless easy classification and remediation)

Security Driven Networking (**LTE Edge:** 5G)

- 5G backup (+SD-WAN for WWAN with new dual modem)
- LTE portfolio expansion (+WWAN application release, 101F/201F)
- SASE bundle for Thin edge and remote workers

Zero Trust Access (ZTNA)

- single policy for on-net / off-net behavior
- Better & easier VPN with automated setup for HW/VM//SASE & cloud
- Granular access with role based application access
- Leverage existing products

Adaptive Cloud Security (VM, CWP, CASB)

- Centrally managed hybrid cloud (expended support & multi tenant policies)
- Effective usage of resources with autoscaling
- Extended application support for CASB
- Container guardian

Adaptive Cloud Security (WAF & Email)

- Email continuity switch to FortiMail cloud when service go down
- FortiWeb enhanced with ML-based API discovery, deeplearining and more.
- FortiADC/FortiGSLB user experience visibility and Auto-Scaling capabilities

FortiGuard Threa*t Intelligence* (Security Services)

- Increased Attack Surface Coverage – Video Filtering enhancement to our web filtering offering
- Security Rating expended to **Fabric Rating**
- **IoT real-time query service**

Fabric Management Center (SOC)

- MITRE attack analysis with expansion in cover and automated protection across the fabric and ecosystem
- SOAR enhanced AI/ML & out-of-the-box content packs. Intergrations. FSR cloud. mobile app.
- IR unified console, FORTISOAR container, FortiCASB connector

Fabric Management Center (NOC)

- Insider threat analysis with UEBA support
- Enhanced visibility with extended product support across the Fabric & SD-Branch
- Efficient and scalable operation with SIEM
- SaaS management with Unified GUI, easy on boarding with ZTP templet and more & efficient full branch operations

Advance Services

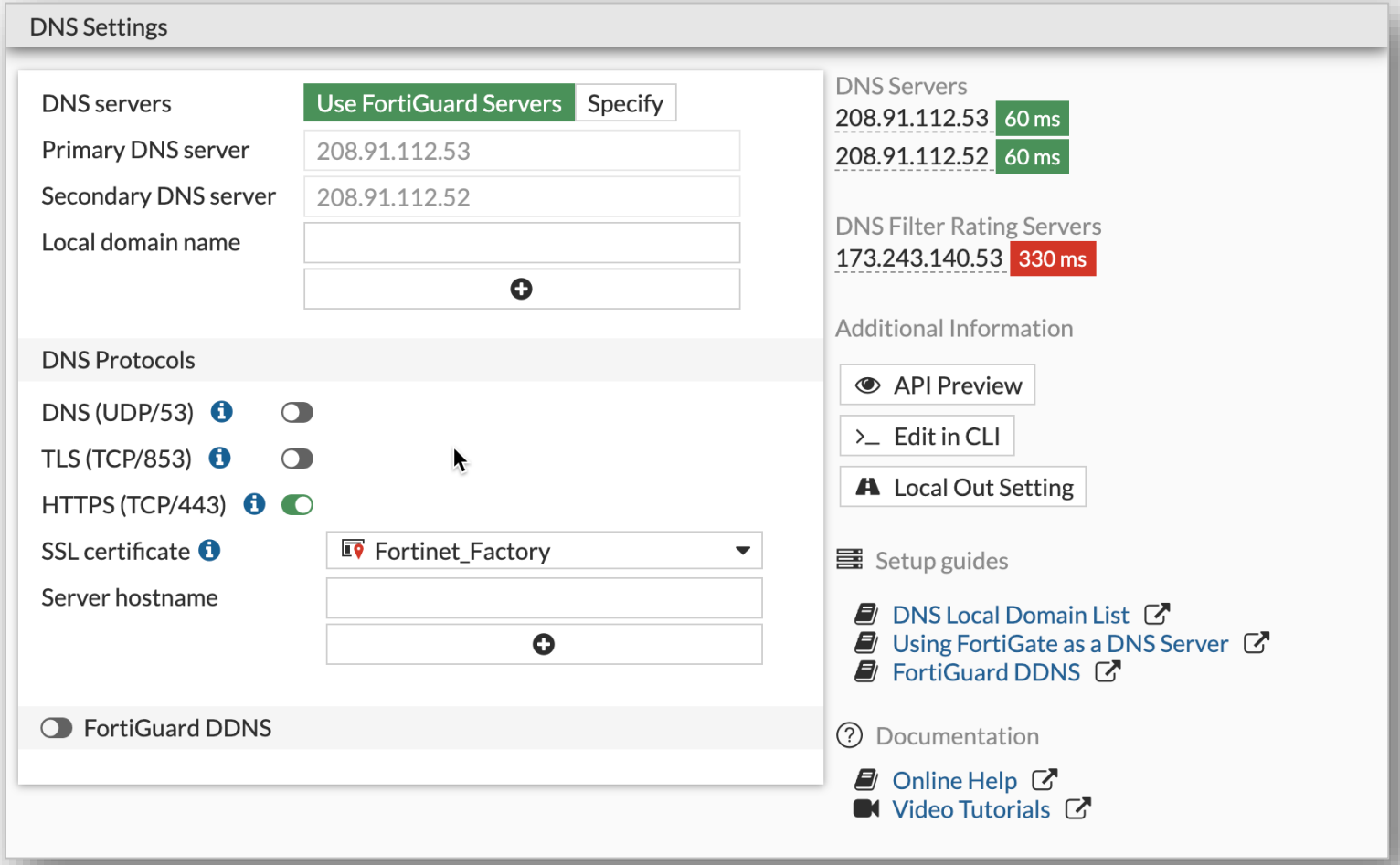
- SOC as a Service to augment organization and MSSP's SOC
- Best Practice Evaluation
- FortiGuard Consultant

Security-driven Networking

Улучшения в DNS Inspection (включая DNS over TLS, DNS over HTTPS)

Расширение поддержки DNS протоколов в FortiOS

- Добавление поддержки прокси для инспектирования DNS over HTTPS и TLS с использованием DNS inspection profile
- Настройки GUI для включения поддержки DNS протоколов – DNS (UDP), DNS over TLS и DNS over HTTPS

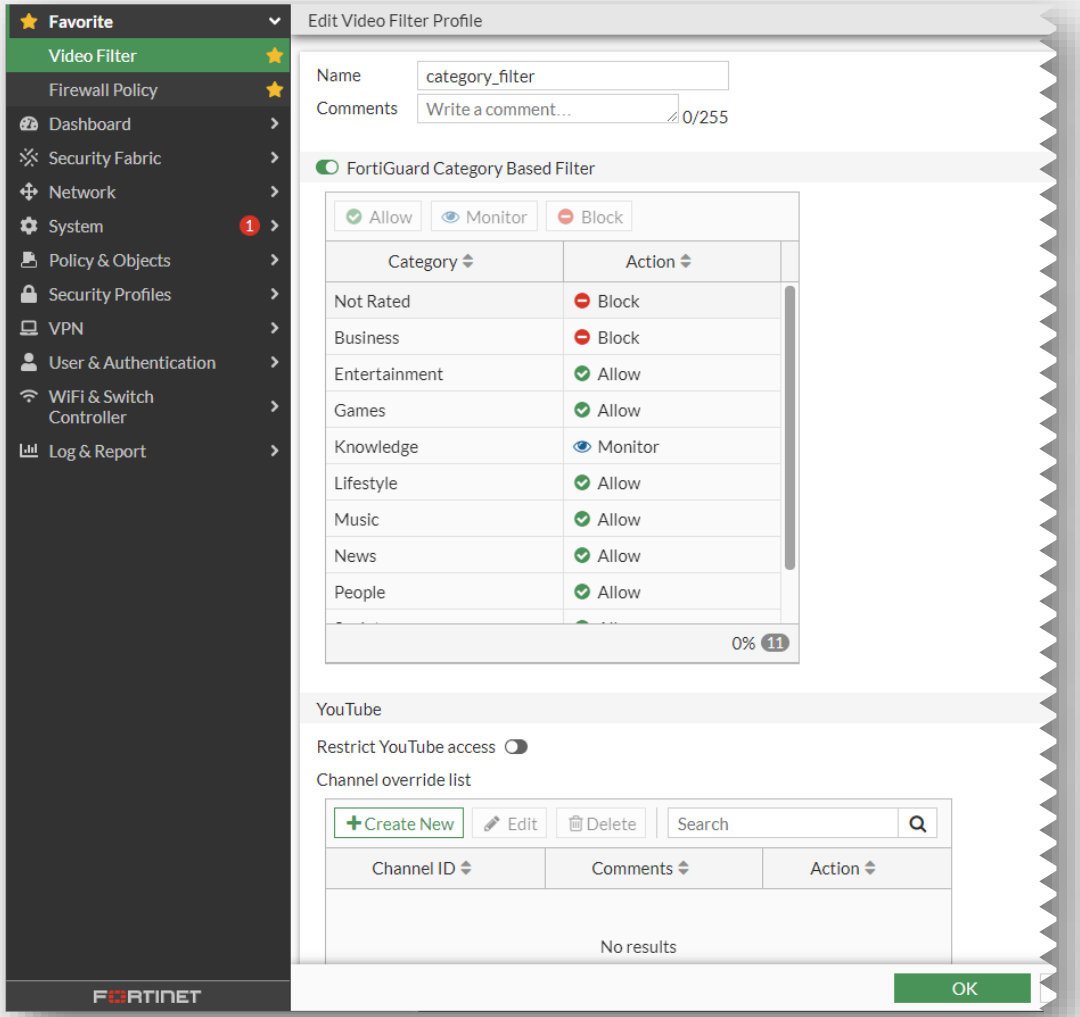


Security-driven Networking

FortiGuard Video Filtering Service

Новый сервис фильтрации FortiGuard обеспечивающий фильтрацию потокового видеоконтента по категориям

- Поддержка YouTube, Vimeo и Daily Motion
- Опция статической фильтрации для каналов YouTube

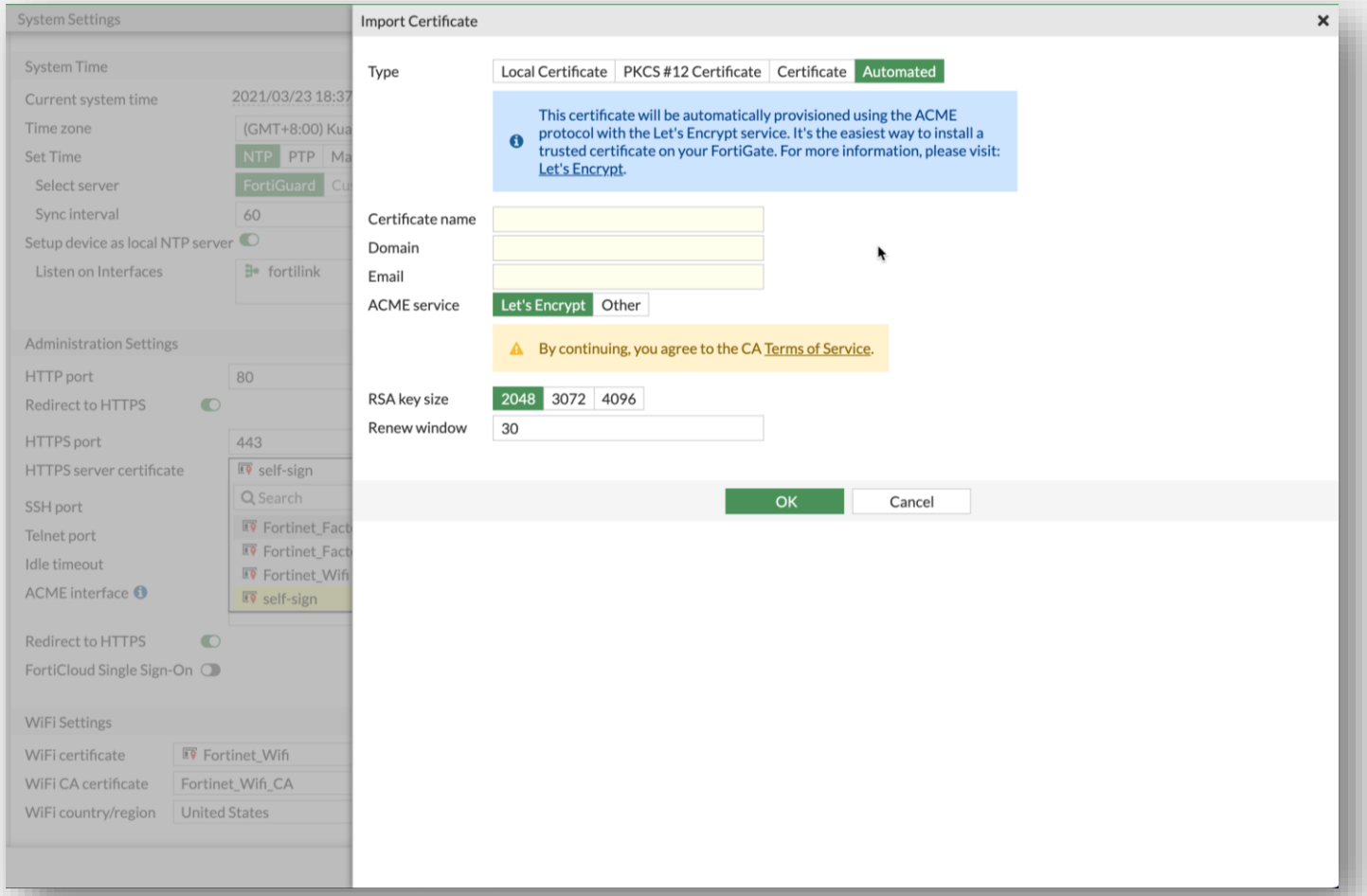


Security-driven Networking

Автоматизация управления сертификатами с помощью ACME

Автоматическое генерирование сертификата для устройства с использованием протокола ACME (Automated Certificate Management Environment)

- Для доступа HTTPS / SSL-VPN GUI
- Простой в использовании инструмент для назначения сертификатов на устройство без сложностей с ручным управлением сертификатами



Security-driven Networking

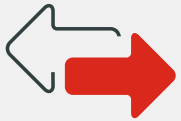
NGFW

HA Failover в зависимости от загрузки RAM

- Allow user to define a base line and threshold of RAM usage for failover
- Threshold may be referencing conserve mode
- A flip timeout may be implemented

Поддержка 4-х узлового кластера FGSP

- Resolving challenges supporting 4 FGs in a FGSP cluster
- By supporting FGSP sync when session TTL is set to 300 seconds



Улучшенная поддержка мониторинга линков и Heartbeat

- If certain network is not accessible and failure detected with link monitor, only the route to this network will be removed from routing table.
- New option for 10ms heartbeat interval, compared to default 100ms

Security-driven Networking

NGFW

Поддержка NetFlow для интерфейсов FortiExtender и туннелей VPN

- Add NetFlow visibility for 2 types of logical interfaces - FortiExtender and VPN tunnel interfaces

Security-driven Networking

SD-WAN

Пассивное измерение производительности приложений

- Uses probe-free network monitoring specific to the application by various methodologies
- Reduced load on the network and simplified configurations

Улучшения в механизме Packet Duplication

- New IPsec Interface to handle packet duplication, supports static and dialup VPNs

SSL VPN Client на FortiGate

- Allow site-to-site connection using SSL VPN
- Similar to IPsec dial-up client on FGT behaviour

Security-driven Networking

Secure Access - Switching

Динамические профили портов и NAC Policy Table для портов FortiSwitch

- New mode that simplifies NAC policy deployment so that admins do not have to assign NAC policy to each FortiSwitch port

Улучшения отображения топологии для FortiLink / FortiSwitch

- Show FortiLink over L3 Switches in Topology and Allow customized display of Switch GUI

Базовая поддержка мультитенантности FortiLink в GUI

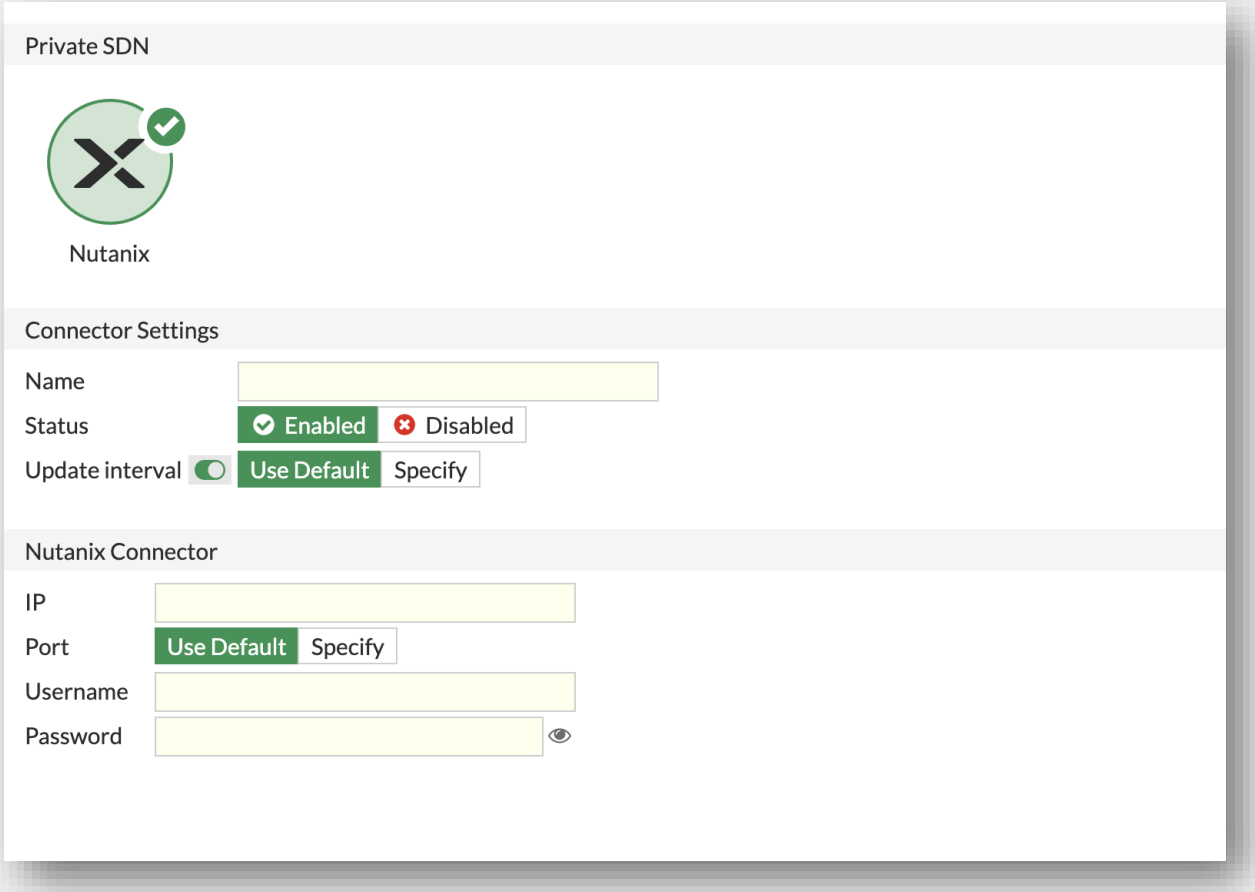
- Adjust implementation of FortiLink multi-tenancy, so that it can be presented and configured on GUI
- Need to be configured via the CLI (port exports) first

Dynamic Cloud Security

Nutanix Connector

API коннектор к Nutanix Prism Central

- Аналогичный OpenStack Connector

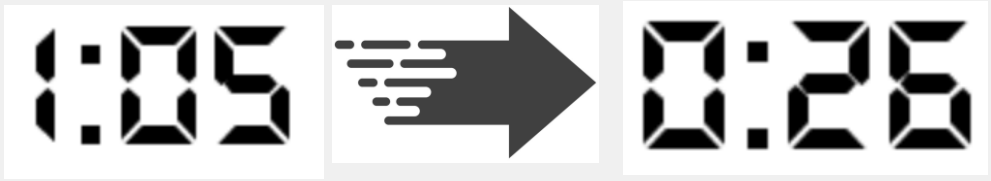


Zero-Trust Network Access

Улучшения времени реагирования NAC

Оптимизирован по времени процесс обнаружения нового устройства и назначения для него VLAN

- Вместо периодического опроса (ежеминутно) используется подход основанный на обработке события
- Новая команда настройки частоты запуска NAC engine в случае пропуска любого события



With minimum nac-periodic-interval (5 seconds), it now takes 40 sec shorter for a PC from link up to match to NAC policy

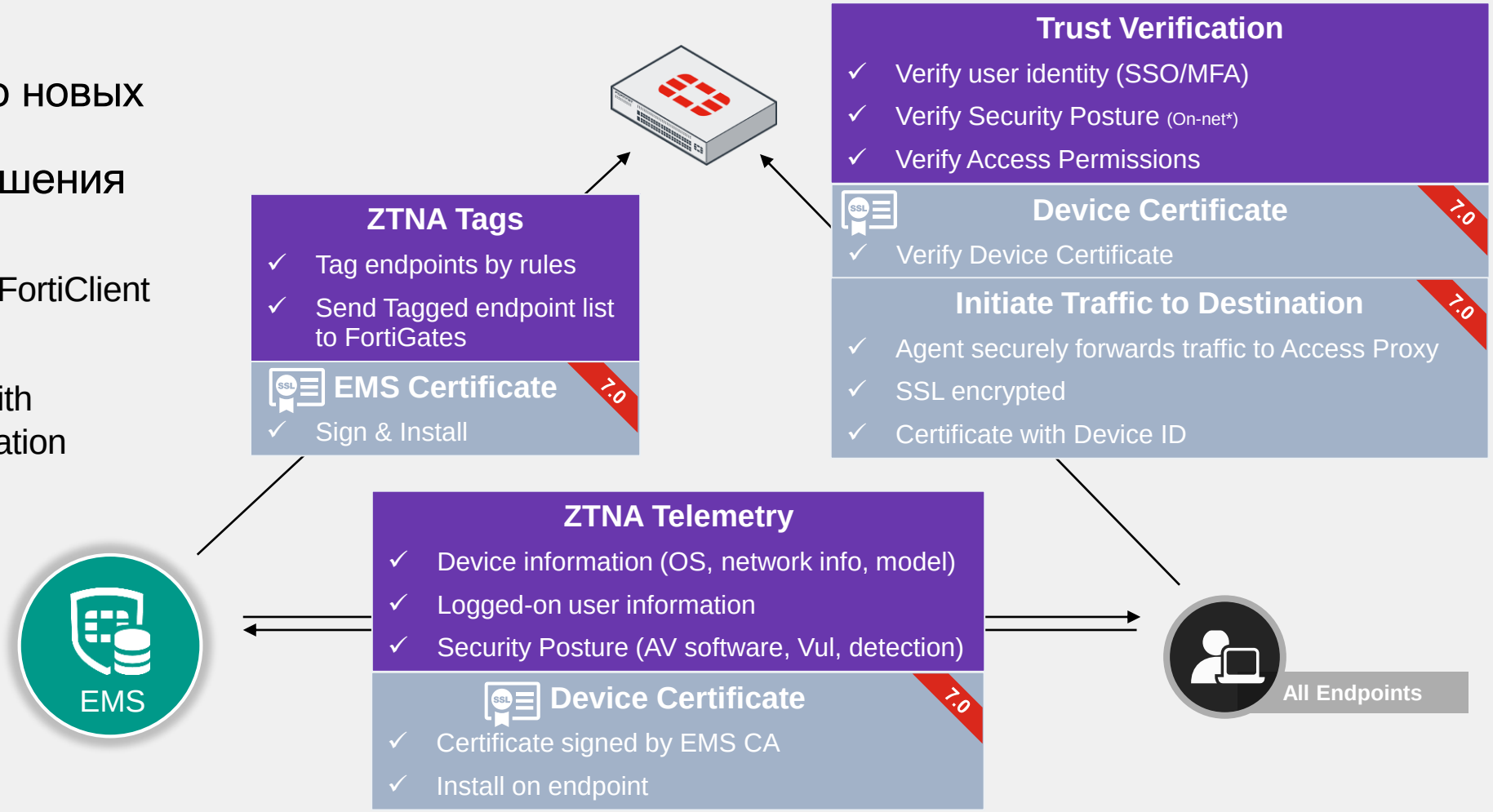
```
config switch-controller
   set nac-periodic-interval <5-60 sec>
end
```

Zero-Trust Network Access

Новое решение Zero Trust

Добавлено несколько новых возможностей для поддержки нового решения Zero Trust

- HTTPS access proxy with FortiClient as ZTNA agent
- Support trust verification with certificate-based authentication



Zero-Trust Network Access

Конечные узлы

Поддержка IPv4/IPv6 SSL-VPN

- Support dual stack where both IPv4 and IPv6 traffic can be sent over the tunnel and terminate on FortiGate
- To be supported for Web and Tunnel mode

Упрощение подключения EMS

- Allow EMS side to approve connector request for the entire fabric (of FG) with a single click, when the request comes from the root of the fabric.

AI-driven Security Operations

Обнаружение вредоносного ПО с помощью AI

Замена старого эвристического движка на новый с поддержкой AI

- Разрабатывался командой AV/Sandbox engine в последние 4 года.
- Тот же движок используется в FortiClient 6.4

Fabric Management Center

Автоматическая установка ПО для FortiSwitch после авторизации

Добавлена опция автоматической установки firmware после добавления и авторизации новых FortiSwitch к FortiGate

Необходимо предварительно загруженное ПО для FortiSwitch на FortiGate

Поддержка 4 образов одной модели FortiSwitch для FortiGate с диском, 1 образ для FortiGate без дисков.

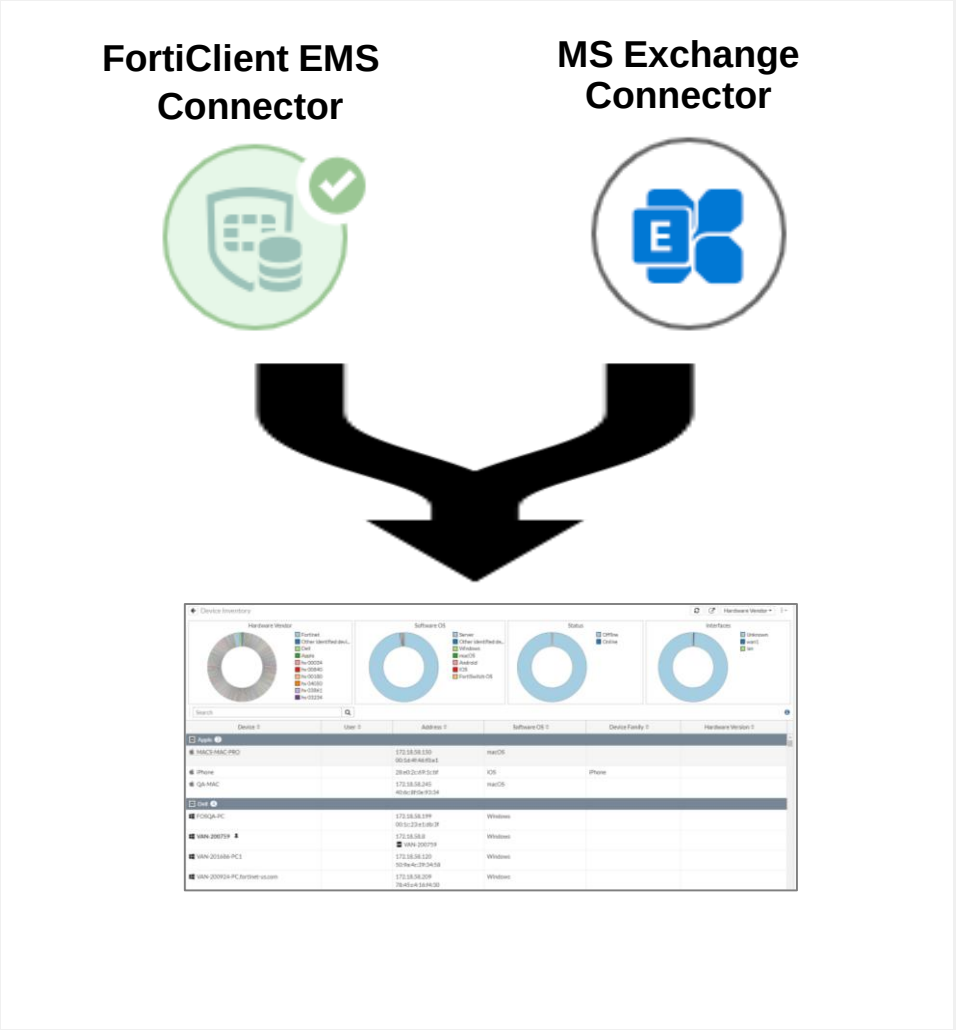
```
config switch-controller managed-switch
  edit "FSW"
        set firmware-provision [ enable |
        disable ] firmware-provision-version <
        major.minor.build >
  next
end
```

Fabric Management Center

Обогащение данных EMS с помощью Exchange Connector

Путем объединения информации из EMS и Exchange connector, FortiOS предоставляет детальную информацию о пользователях без необходимости осуществлять аутентификацию на МСЭ.

- Более полная информация о пользователе для User Store

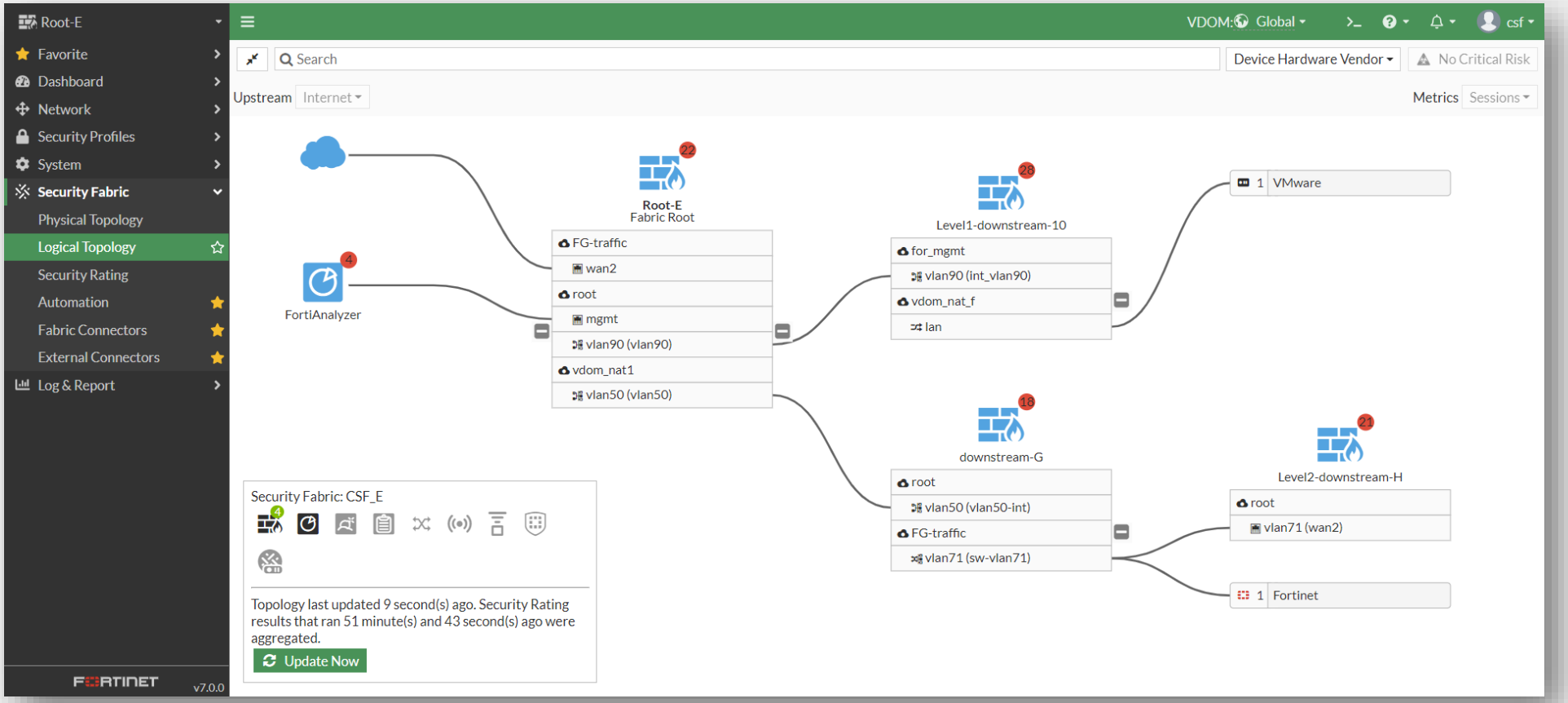


Fabric Management Center

Поддержка Security Fabric в режиме Multi-VDOM

Можно добавлять FortiGate с VDOMs в Security Fabric

- Features (as Global scope) include Fabric Topology, Security Rating and Automation



Fabric Management Center

Интеграция с FortiAI, FortiDeceptor, FortiTester, and FortiWeb

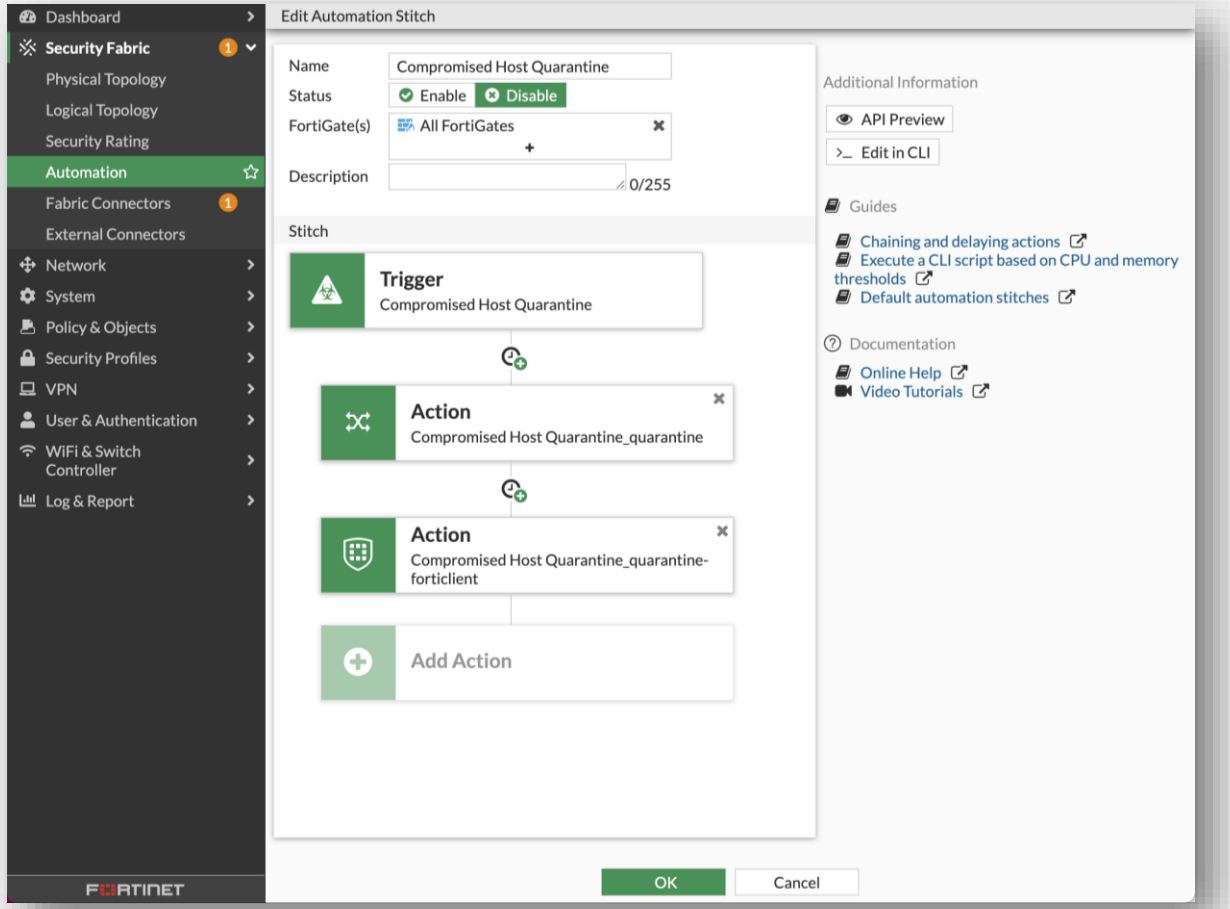
Fabric integration with more Fortinet products to yield unique solutions

Fabric Management Center

Улучшения в процессах автоматизации

Упрощение процессов автоматизации управляющих множеством связанных действий и обеспечение для пользователя прозрачного порядка их выполнения.

- Также поддержка
  - Связь множества event log ID с одним триггером
  - Кастомный HTTP body code для уведомлений через Slack
  - Фильтрация event log для более точного срабатывания триггеров

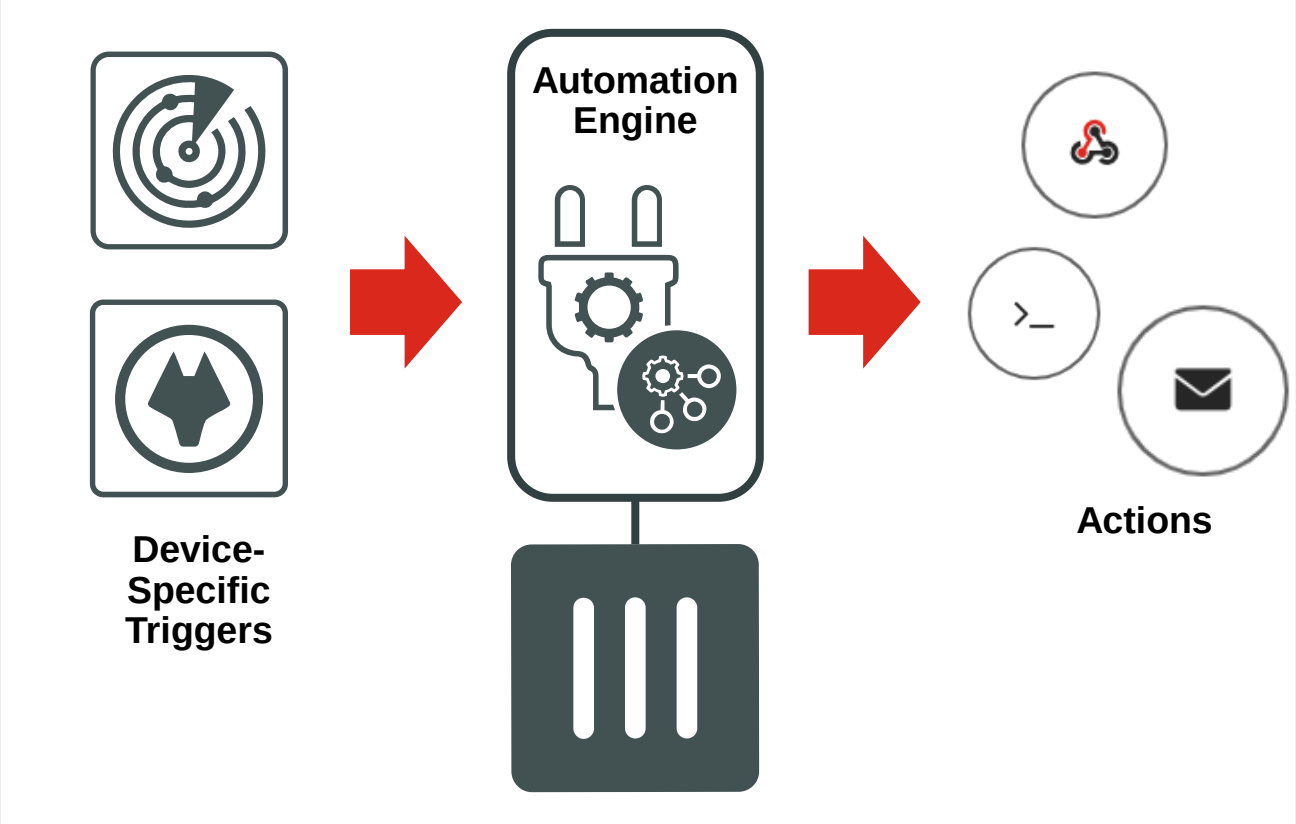


Fabric Management Center

Вызов триггеров автоматизации с помощью устройств Security Fabric

Расширение возможностей автоматизации в Security Fabric путем разрешения вызова триггеров автоматизации связанных с устройствами Security Fabric

- Расширение протокола CSF и разрешение downstream отправлять запросы на вышестоящие устройства (например root FGT)
- Обработка событий на FGT аналогична FAZ event handling

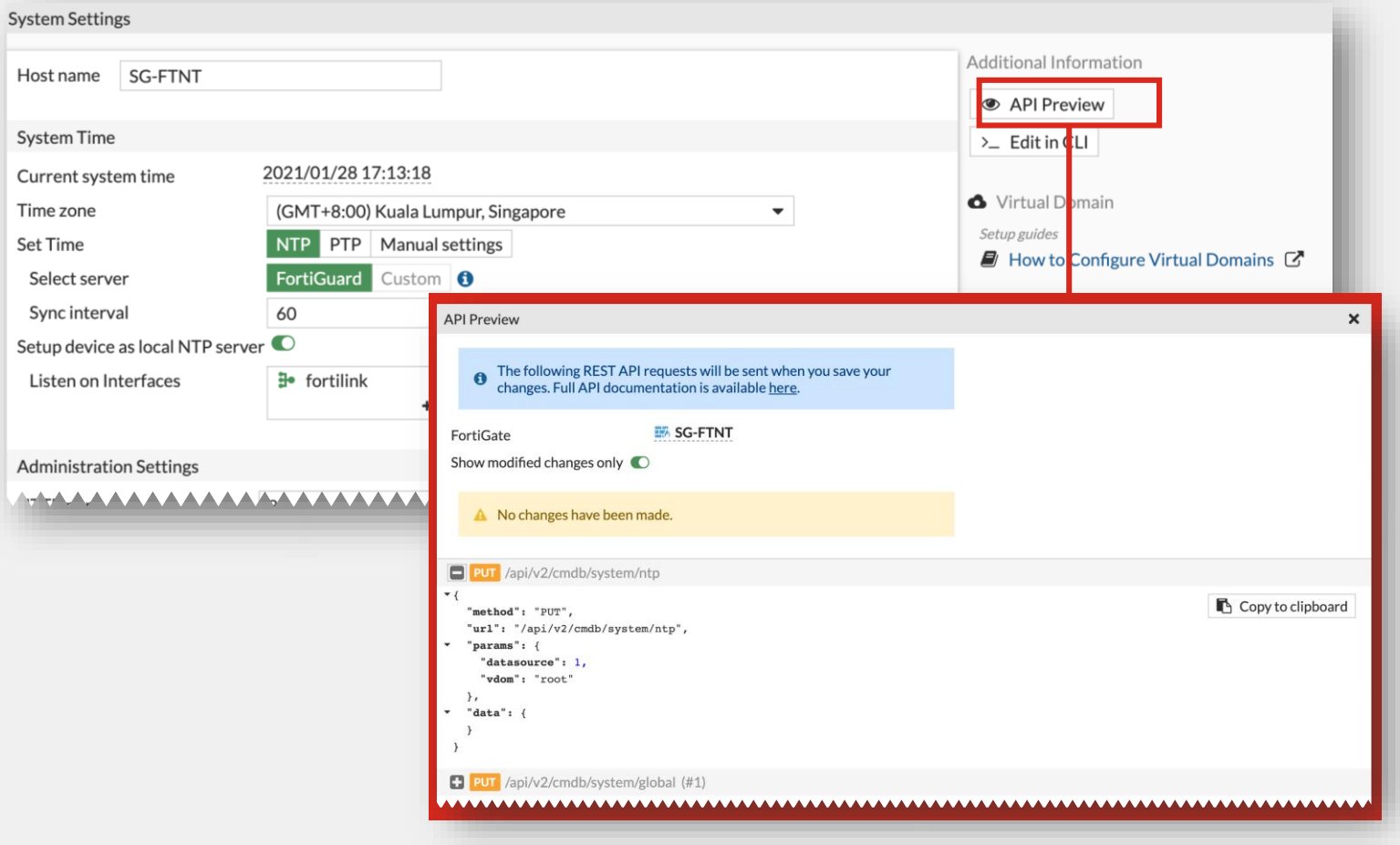


Fabric Management Center

Просмотр эквивалента команд REST API для действий GUI

Добавлена поддержка просмотра команд REST API соответствующих действиям в GUI

- API Preview is added to the right-hand side (gutter) allowing the user to see what API calls will be made when clicking "OK" or "Apply".
- If multiple requests are required, this would be broken into multiple tabs

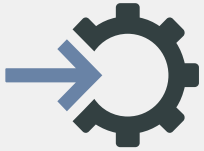


Fabric Management Center

Fabric / Automation

Упрощение подключения FOS/FMG/FAZ

- Use Oauth-like dialog to log into remote FMG/FAZ to authenticate FG request for pairing



FortiCloud Admin login

- Allow SAML SSO using FortiCloud credentials
- Disabled by default

Threat Feed Connector на каждый VDOM

- Extends Threat Feed connectors to each VDOMs


FORTINET