FortiOS 7.0

Новые возможности

21 мая 2021

Чингис Талтаев, SE

Содержание

- Введение
- Fortinet Secure Access Service Edge (**FortiSASE**)
- Fortinet Zero Trust Network Access (**ZTNA**)
- Обзор улучшений в FortiOS 7.0
- Новые сервисы FortiGuard (Video Filtering)
- Новые сервисы FortiCloud (FortiCloud SOCaaS)
- Лицензирование
- Вопросы и ответы

Введение

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**

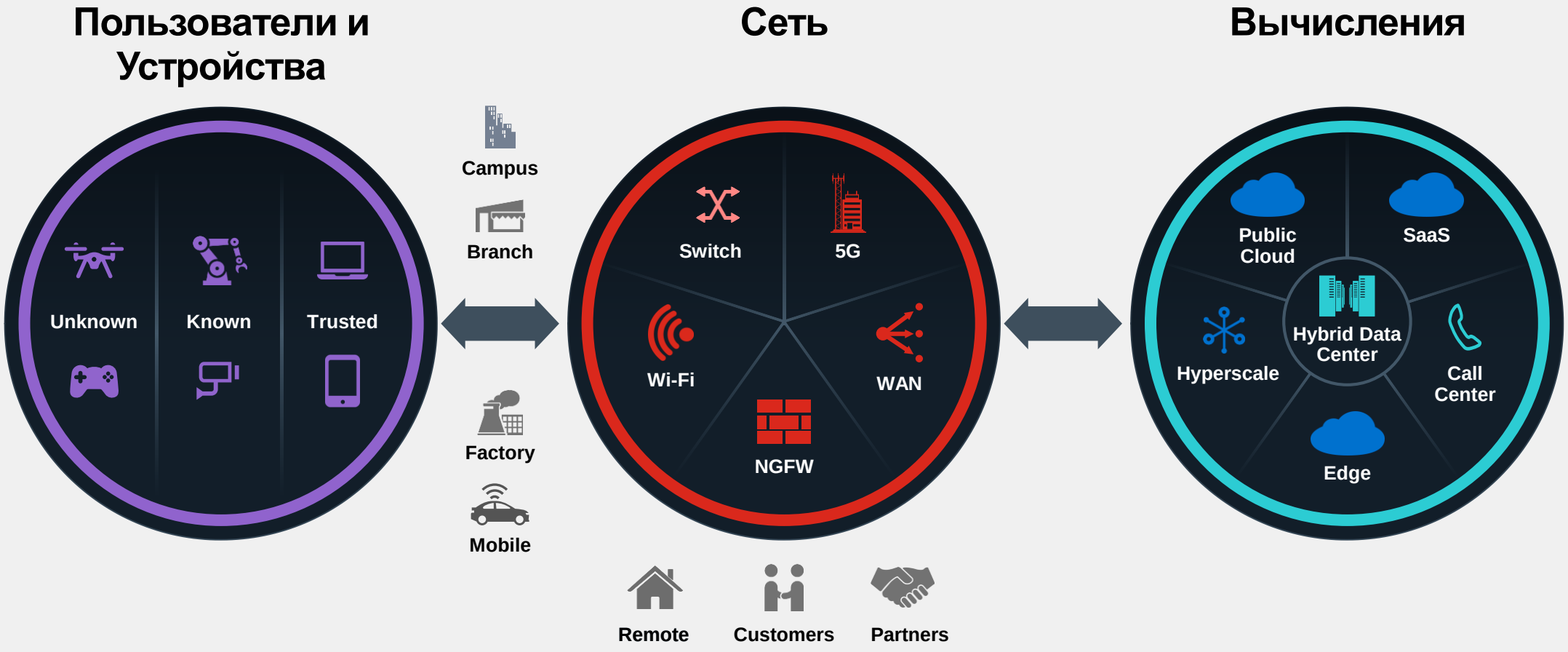
Сетевые функции и функции безопасности (например IPS, Web Filtering) на любом масштабе (Hyperscale) с использованием SPU

03 **Автоматизировать управление и реагирование на инциденты**

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

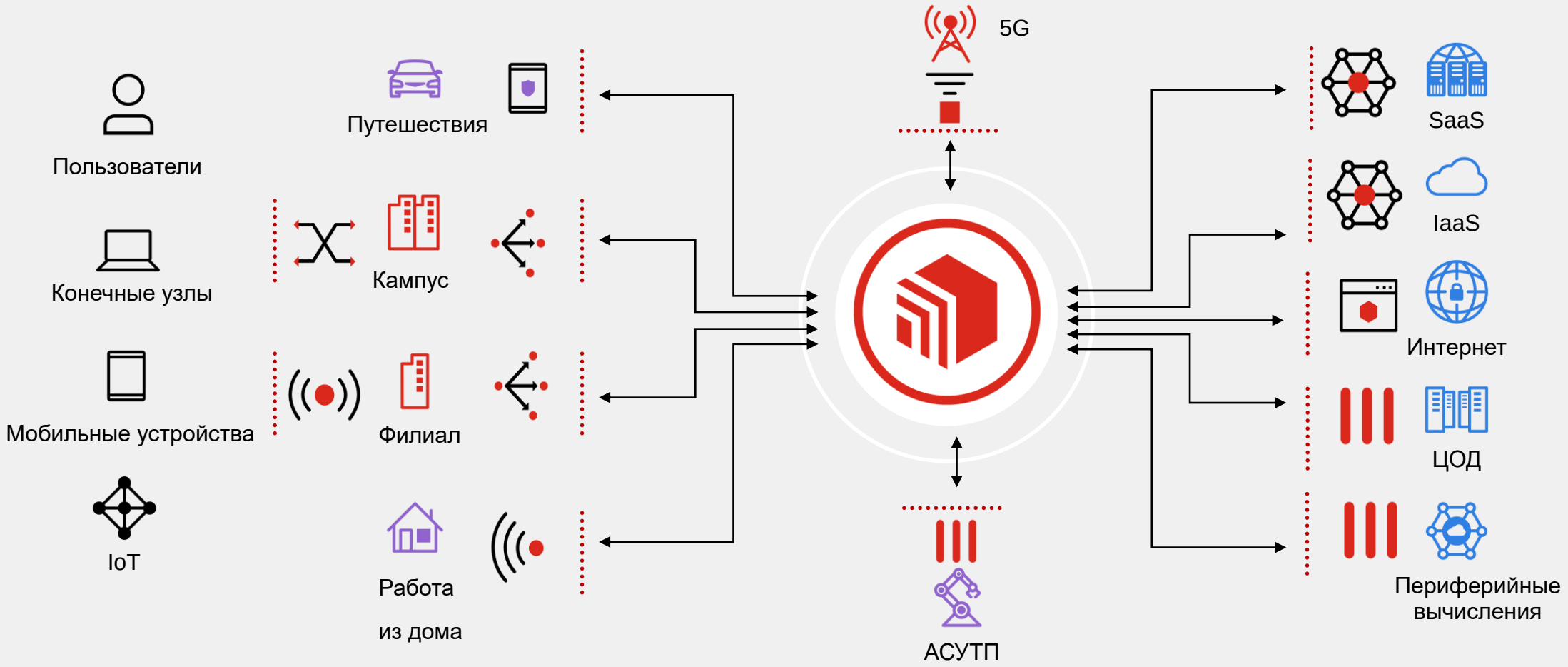
Размытие периметра безопасности

Рост количества устройств IoT, ускорение мобильности пользователей, OT внутри IT, агрессивное развитие публичных, частных облаков, SaaS, периферийных вычислений…



Необходимость защиты в любой точке подключения

Security-driven Networking



Fortinet Security Fabric

Обширная

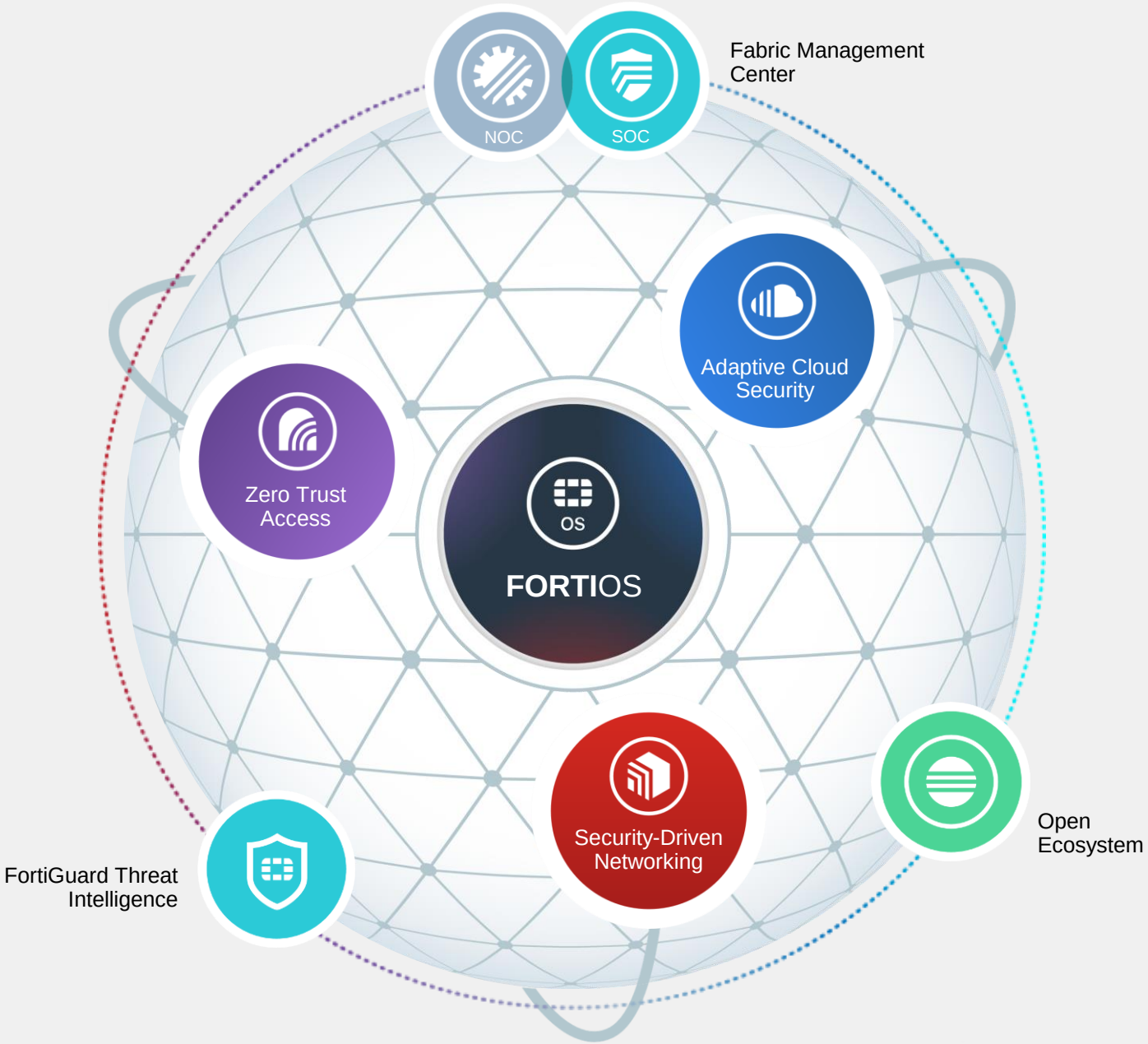
Осведомленность и защита по всей цифровой плоскости атаки для лучшего управления рисками

Интегрированная

Уменьшение сложности управления и обмен данными об угрозах

Автоматизированная

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



Платформенный подход к кибербезопасности

Гибкие модели потребления

Security-Driven Networking

Ускоренная конвергенция сети и безопасности

Zero Trust Network Access

Знание и контроль всех и всего, что находится внутри и снаружи сети

Security Fabric

Management

Ecosystem

Dynamic Cloud Security

Безопасность следует за приложениями и данными

AI-Driven Security Operations

Автоматическое предотвращение, определение и реагирование на киберугрозы

Appliance

Virtual Machine

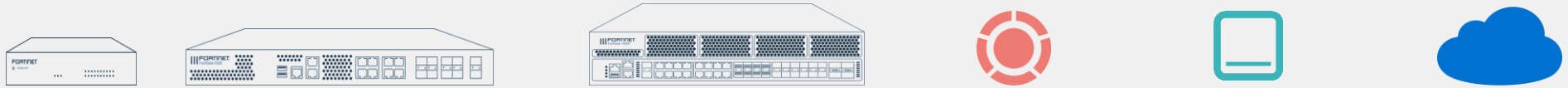
Hosted (SaaS)

Cloud

Software (Agent)

Container

Операционная система FortiOS



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

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

Fortinet Secure Access Service Edge (FortiSASE)

Мировые тренды в развитии безопасности предприятий

Multi-Cloud Adoption

93% предприятий уже имеют стратегию развития в multi-cloud

2020 State of the Cloud Report, Flexera

Work From Anywhere

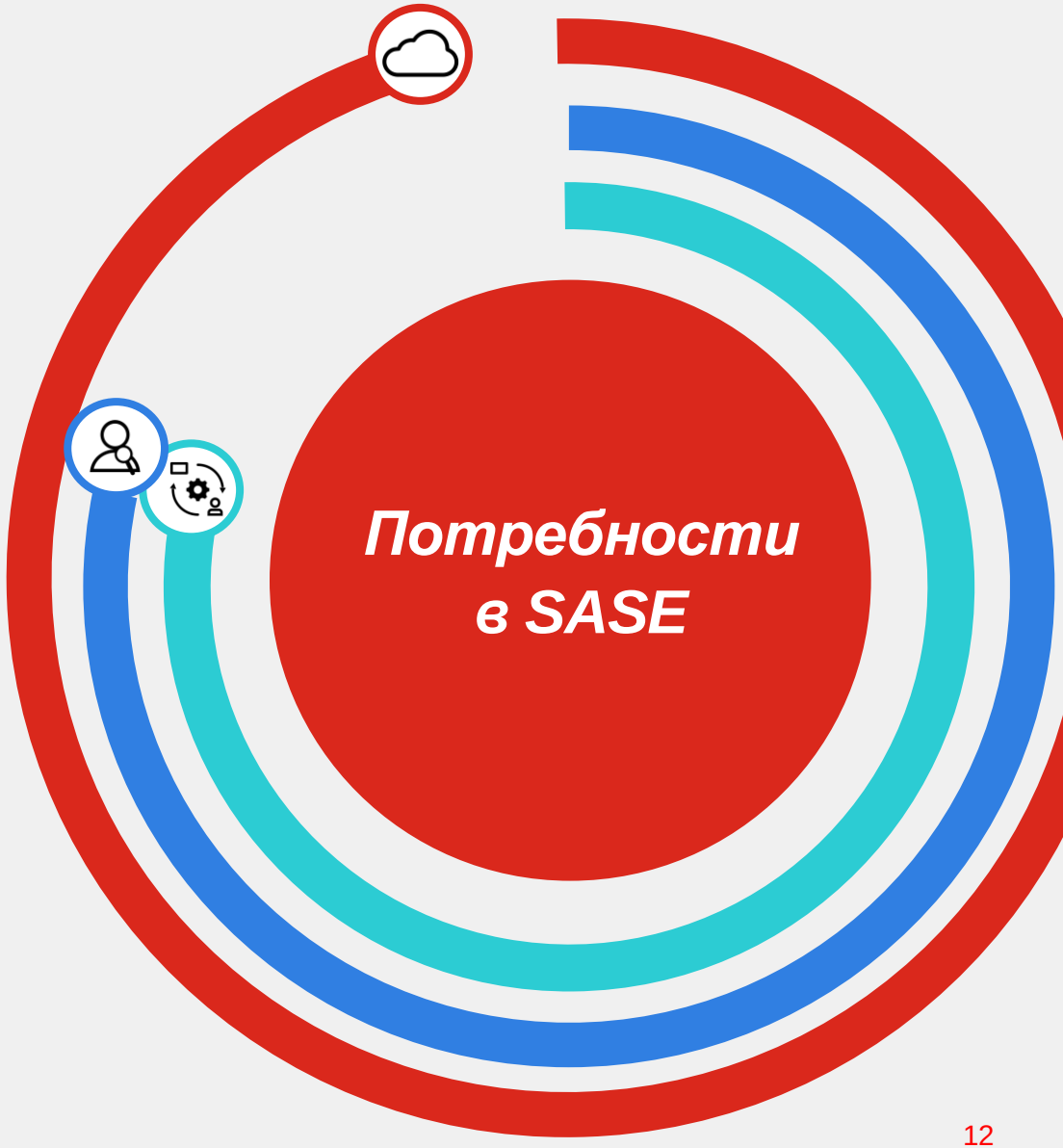
72% сотрудников работают удаленно либо в гибридном режиме (удаленно и из офиса)

2021 IDC Future of Enterprise Networking

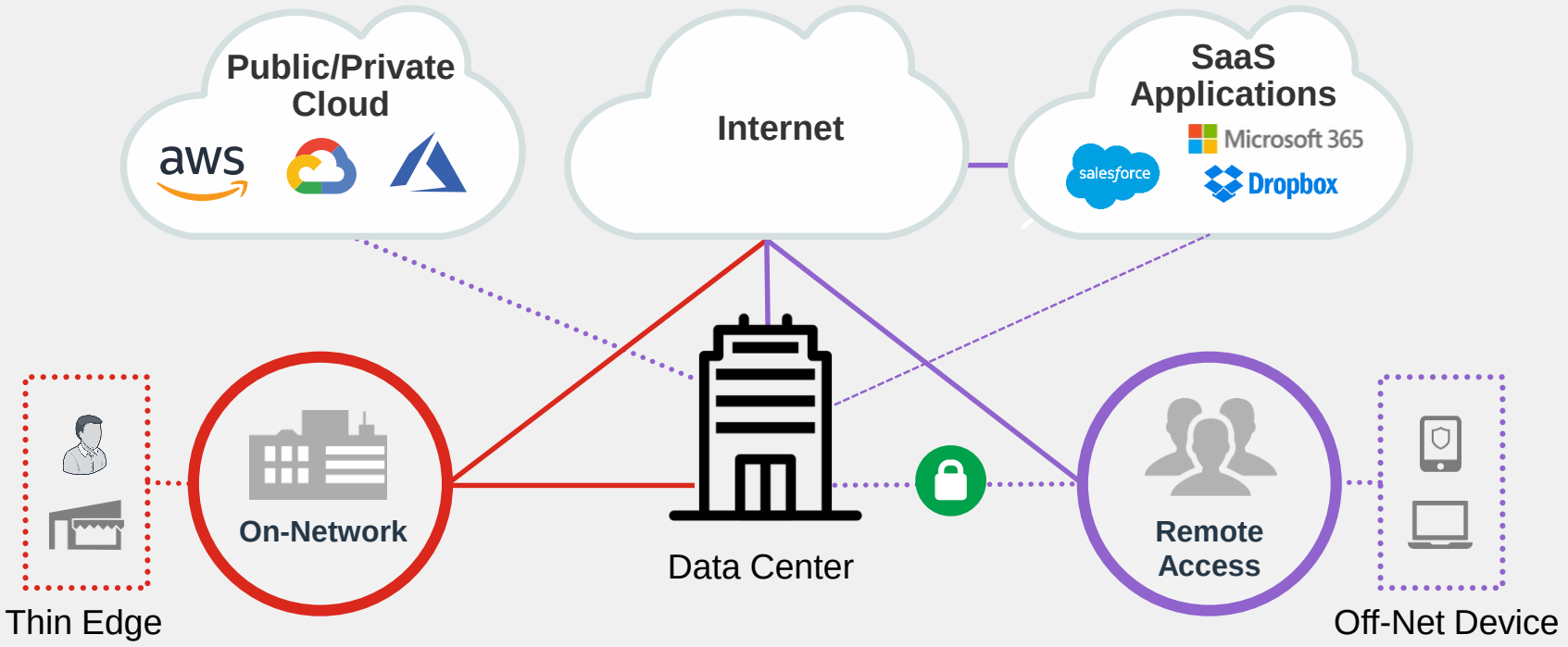
User Experience

70% пользователей предпочитают работать из дома, но жалуются на проблемы с производительностью

2021 IDC Future of Enterprise Networking



Нужна гибкость для цифровой трансформации



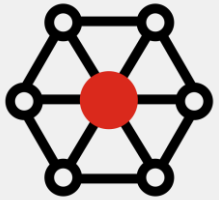
Основные вызовы

1. **Неудовлетворенность пользователей при работе с multi cloud**
2. **Проблемы безопасности для мобильных пользователей**
3. **Отсутствие внятной безопасности во всех точках подключения**

Все функции SASE от единого производителя !

Желательные компоненты SASE (по Gartner)

ZTNA as a Service	ZTNA standalone	SWG	CASB	FW(aaS)	WAF/WAAP	VPN	CDN
RBI	VDI	Sanitized DNS	Network Sandbox	Network Obfuscation	Edge Compute Protection	SD-WAN	



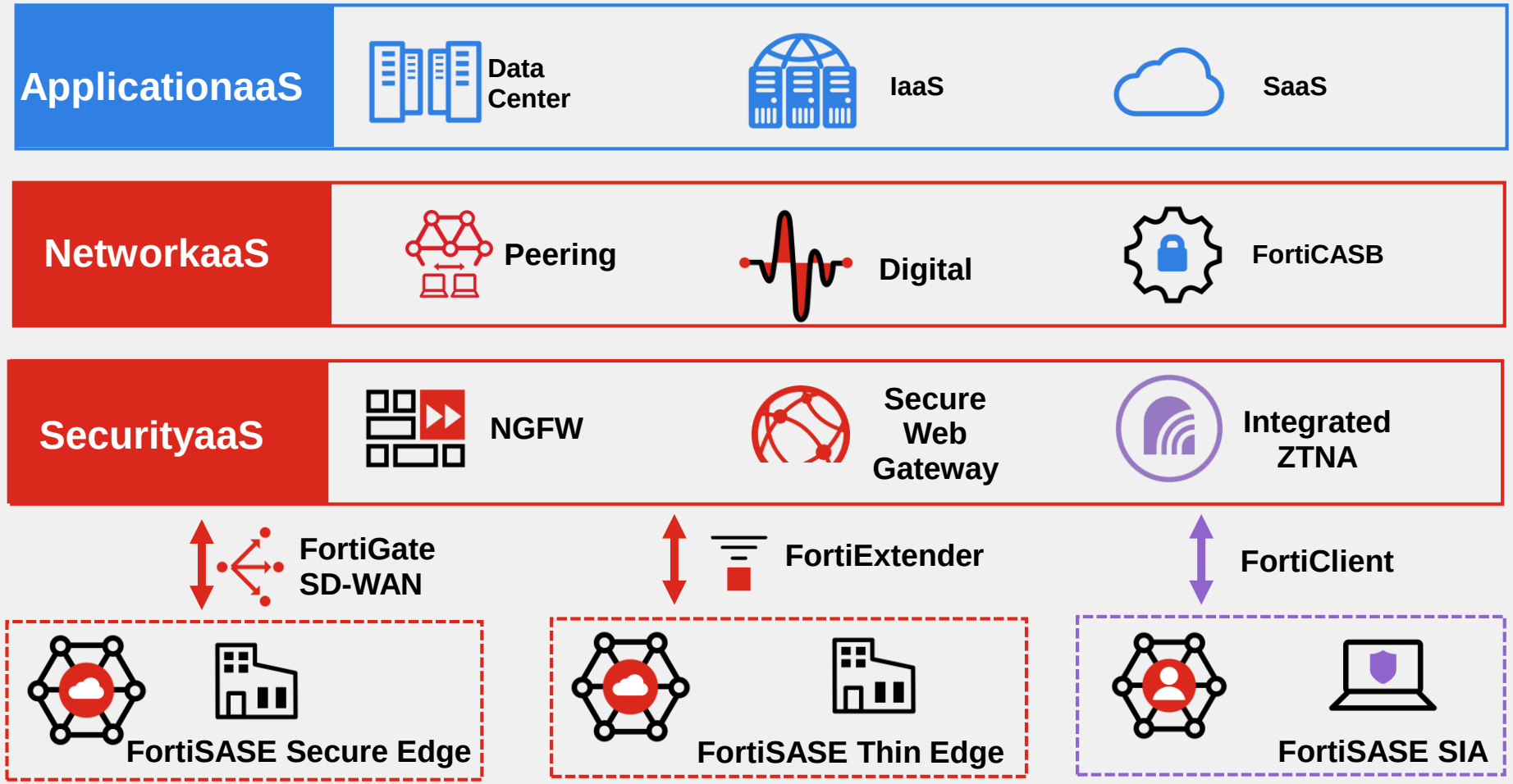
FortiSASE обеспечивает широчайший выбор встроенных функций SASE

Gartner: SASE Will Improve Your Distributed Security Everywhere - Published 8 December 2020

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**



3 принципа Fortinet Secure Access Service Edge

01 **Облачный сервис безопасности**

Уменьшение рисков и улучшение пользовательского опыта для распределенных сотрудников

02 **Работа из любого местоположения**

Прямой доступ в Internet для удаленных пользователей с использованием безопасности корпоративного класса (FortiOS)

03 **От CapEx к OpEx**

Улучшение гибкости для бизнеса на основе подписочной модели Security-aaS

Из чего состоит FortiSASE

Защита удаленных пользователей

FortiClient SASE

FortiSASE Portal

Защита филиала (Thin Edge)

FEX 200F

Fortinet Fabric

Доступ по модели Zero Trust

Zero Trust Agent

Scalable ZTP

Security as a Service

Network as a Service

Zero Trust Network Access

SASE Cloud Management & Analytics

FortiSASE с интеллектом FortiGuard Labs и Services

Advanced Malware Protection

Antivirus

Advanced Threat Protection

Intrusion Prevention

Предотвращение атак в сетевом трафике

Breach Prevention

Indicators of Compromise

Vulnerability Management

Security Risk Rating

Проактивное предотвращение и определение брешей в безопасности

Content Security

Antispam

Web Filtering

Content Disarm & Reconstruct

Предотвращение атак через популярные точки входа

Application / IoT Security

Application Control

Web Application

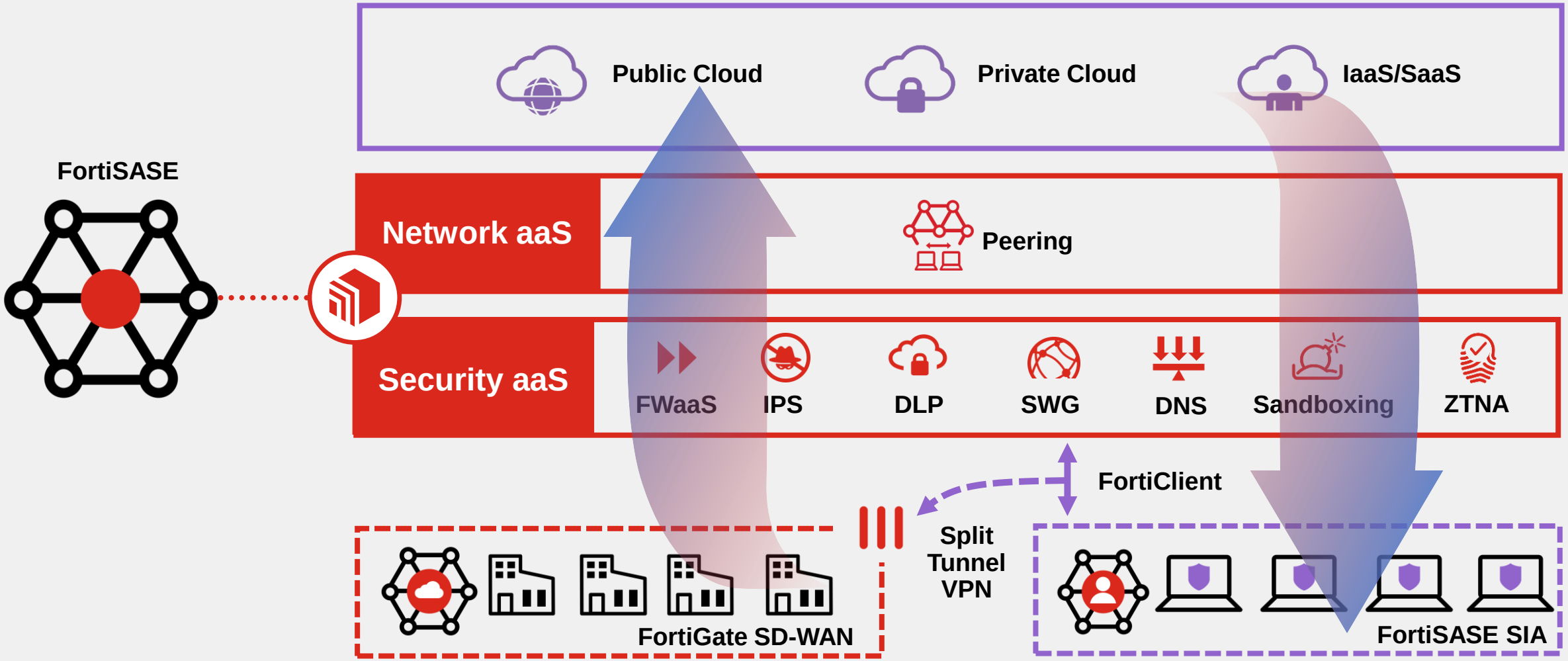
Industrial Security

Расширенная безопасность приложений

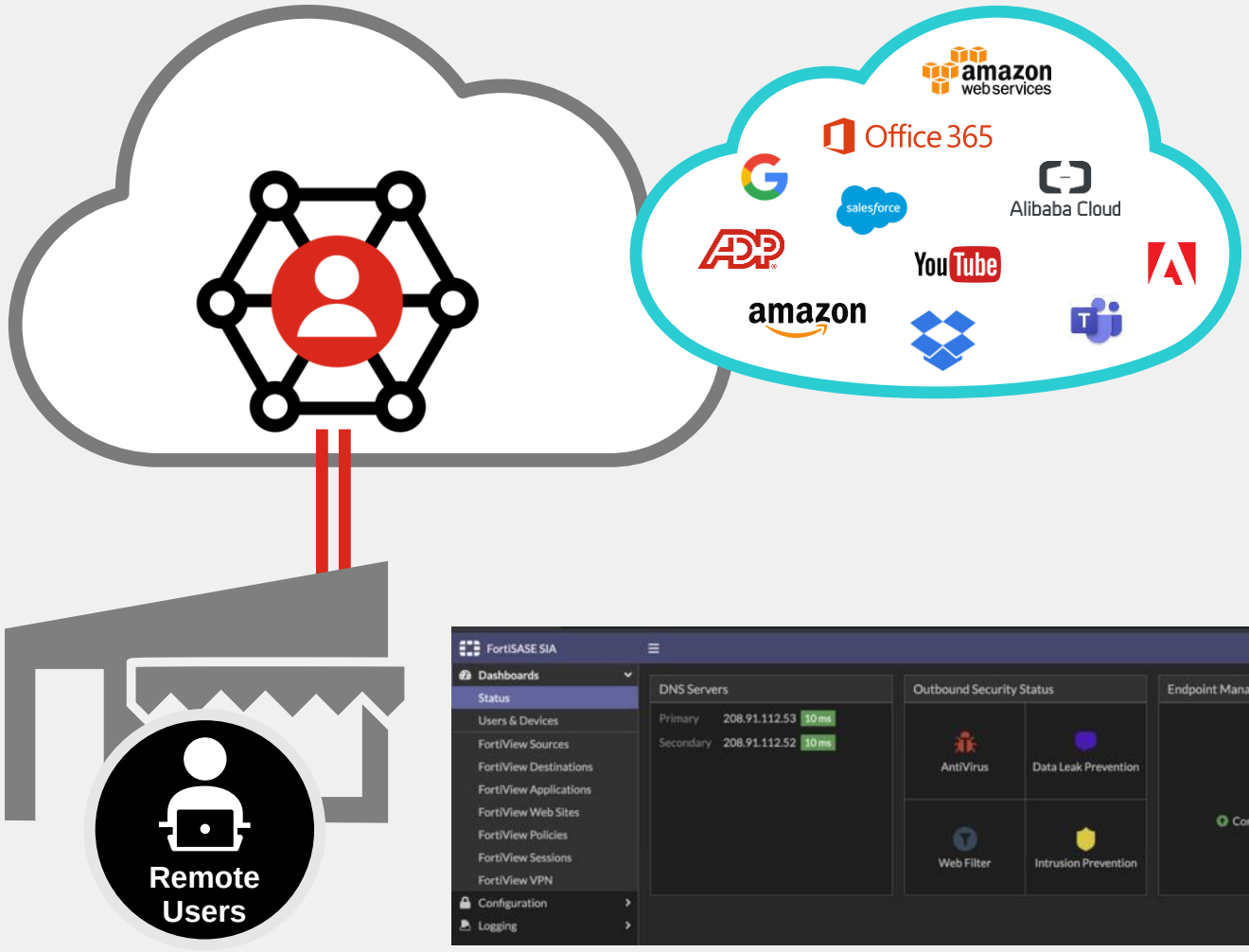
FortiSASE

FortiSASE SIA (Secure Internet Access)

Быстрая, безопасная и масштабируемая альтернатива VPN



FortiSASE - Защита удаленных пользователей

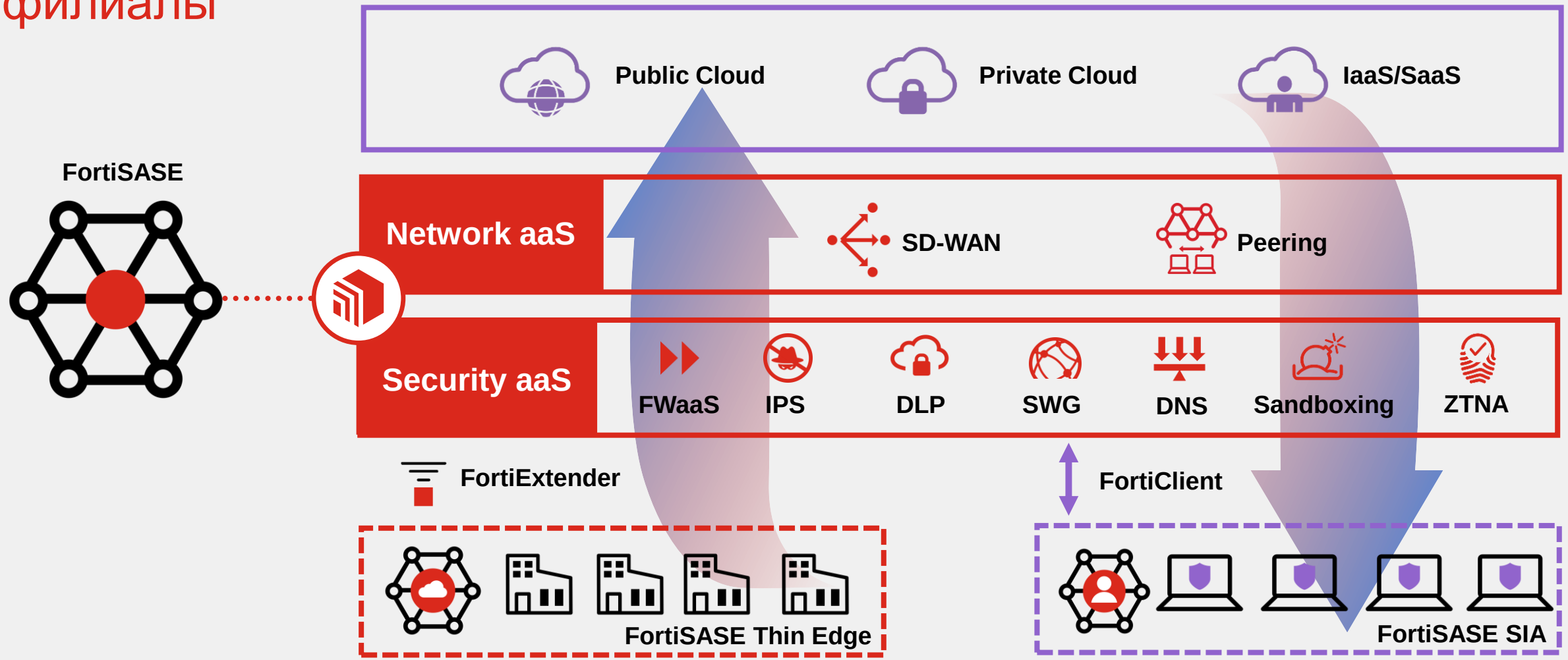


	SASE Edition
Zero Trust Security	Windows, MAC, Linux
Zero Trust Agent	•
Dynamic Security Fabric Connector	•
Vulnerability Agent & Remediation	•
SSL / IPSEC VPN with MFA	•
USB Device Control	•
Automated Endpoint Quarantine	•
Application Inventory	•
Cloud Based Endpoint Security (SASE)	
SSL Inspection	•
Inline AV & Anti-Malware	•
Intrusion Prevention (IPS)	•
FortiGuard Web Filtering	•
Application Firewall	•
Data Loss Prevention	•
Additional Services	
24 x 7 Support	Включено
SASE Cloud Management	Включено
SASE Cloud Logging	Включено
Best Practice Onboarding Service	Включено в 1-ый год

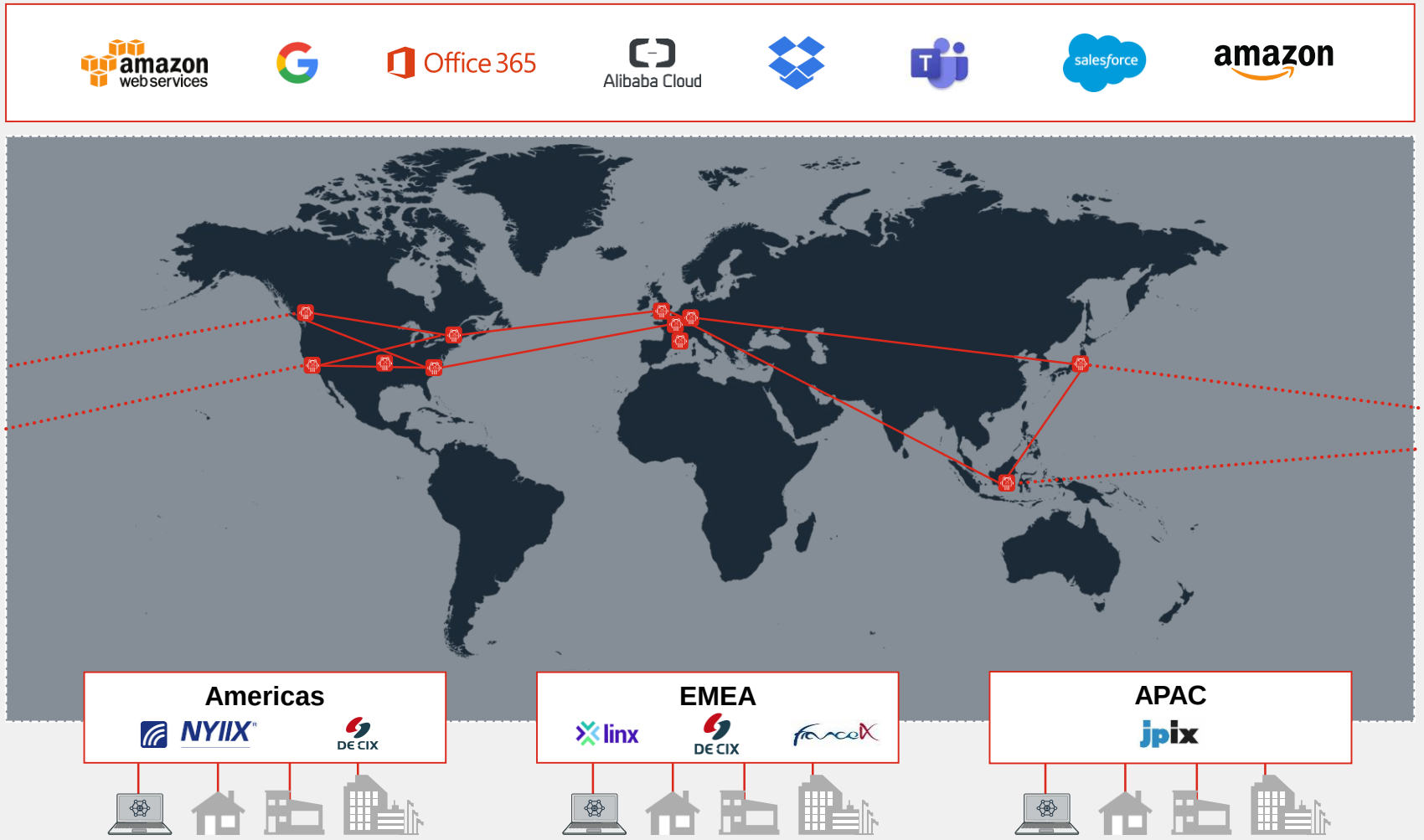
Доступны в пакетах 25, 500, 2000 and 10,000 подключений

FortiSASE Thin Edge + SIA

Расширение облачной безопасности на малые и большие филиалы



Сетевые регионы присутствия FortiSASE (Май 2021)



Пиринг с облачными платформами SaaS

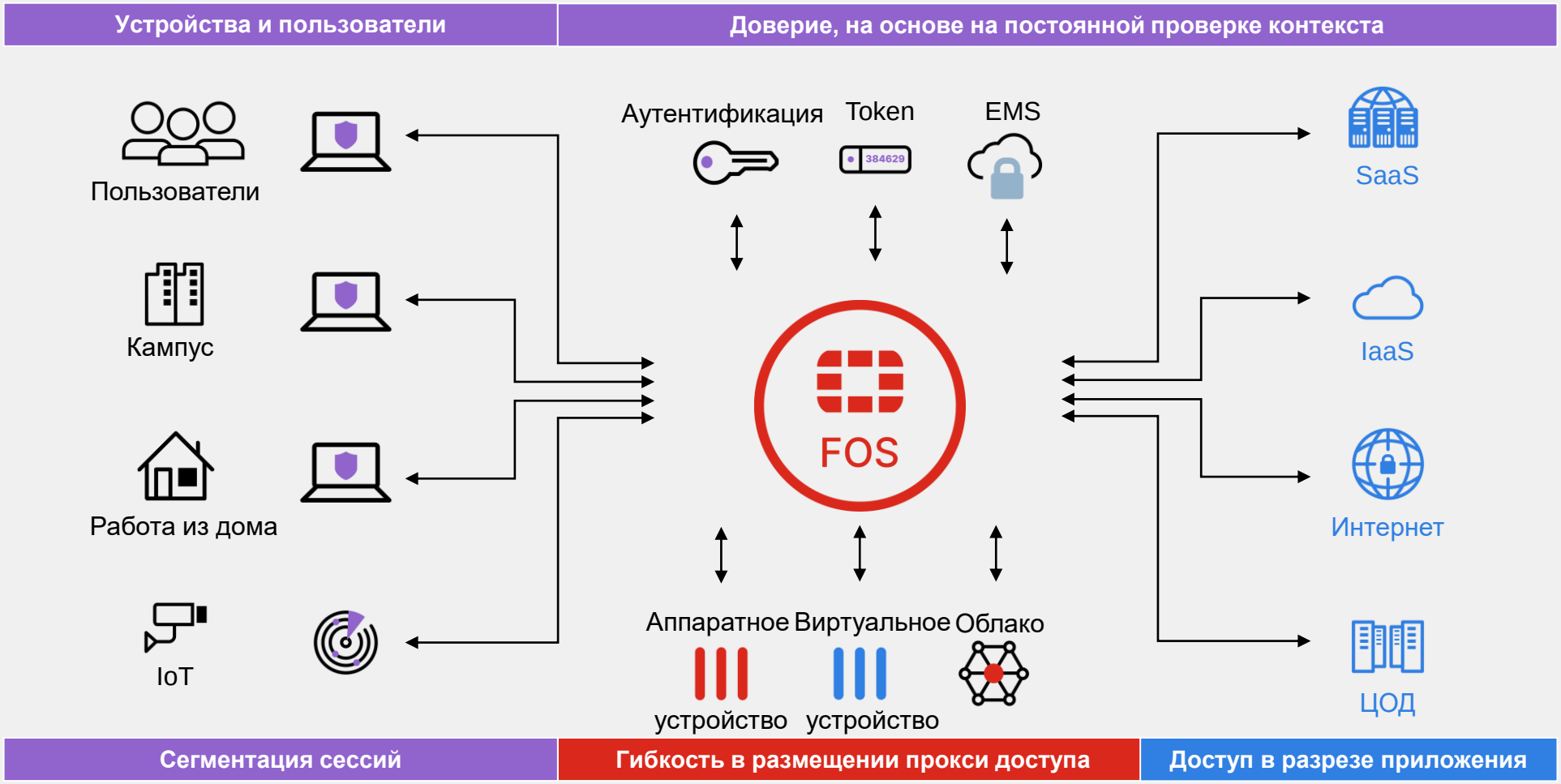
FortiSASE Cloud Hosted Security

Региональный пиринг с сервис провайдерами через IXP

Fortinet
Zero Trust Network Access (ZTNA)

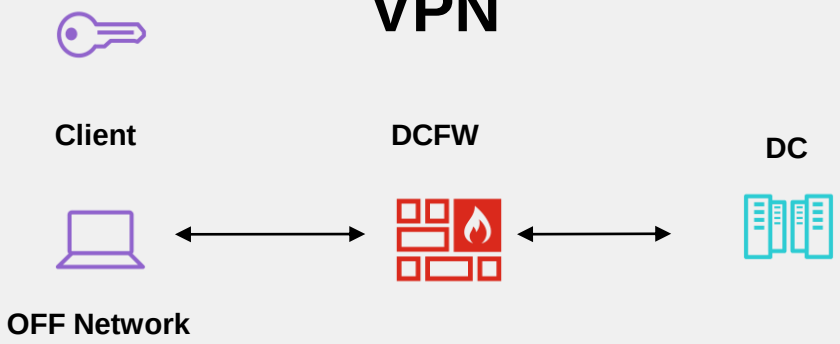
Видение Zero Trust Access (ZTA)

Безопасный доступ к приложениям в любое время и из любого места



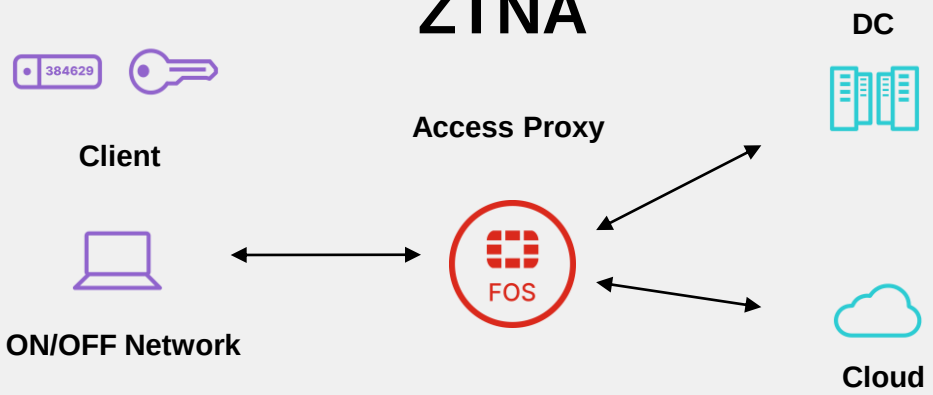
Эволюция традиционных VPN в ZTNA

VPN



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

ZTNA

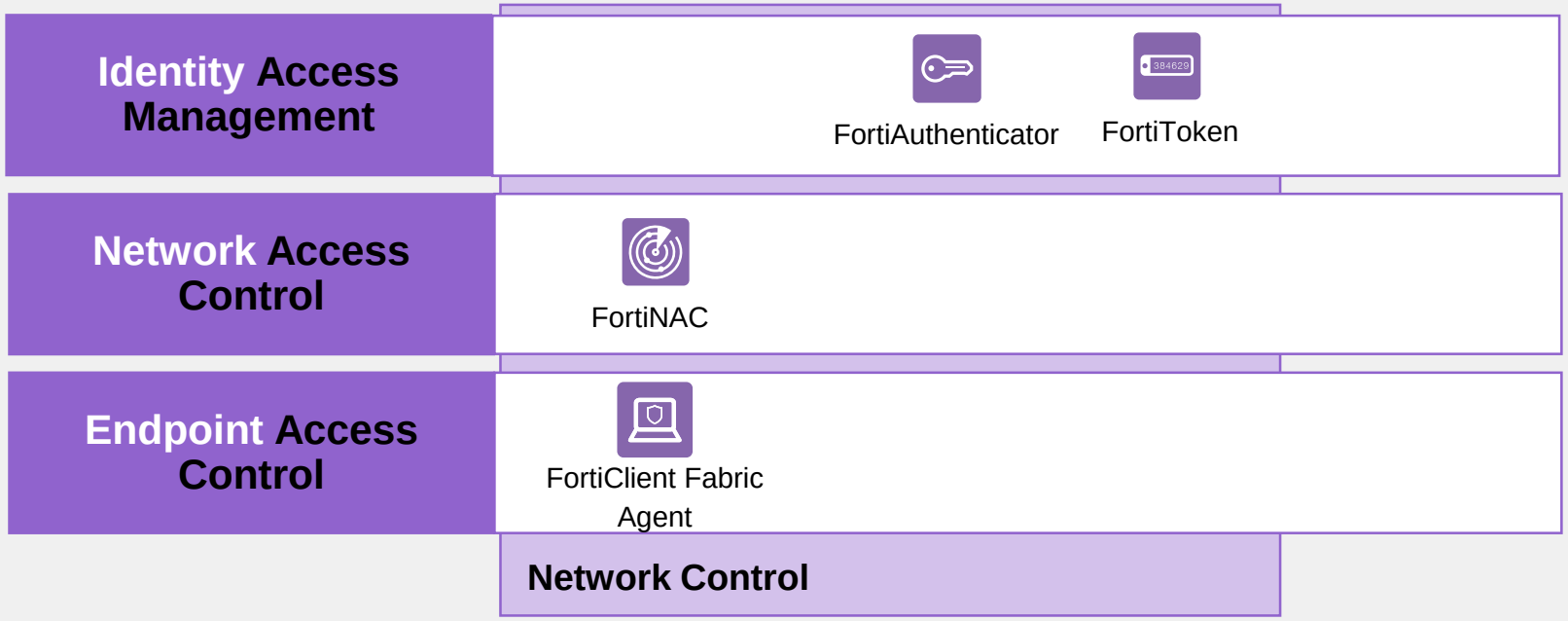


- Постоянная проверка доверия
- Доступ только к определенным приложениям
- Динамический доступ в зависимости от текущего контекста безопасности

Cloud

Zero Trust Access (вчера)

Что включает ?



<u>Контроль доступа в сеть</u>

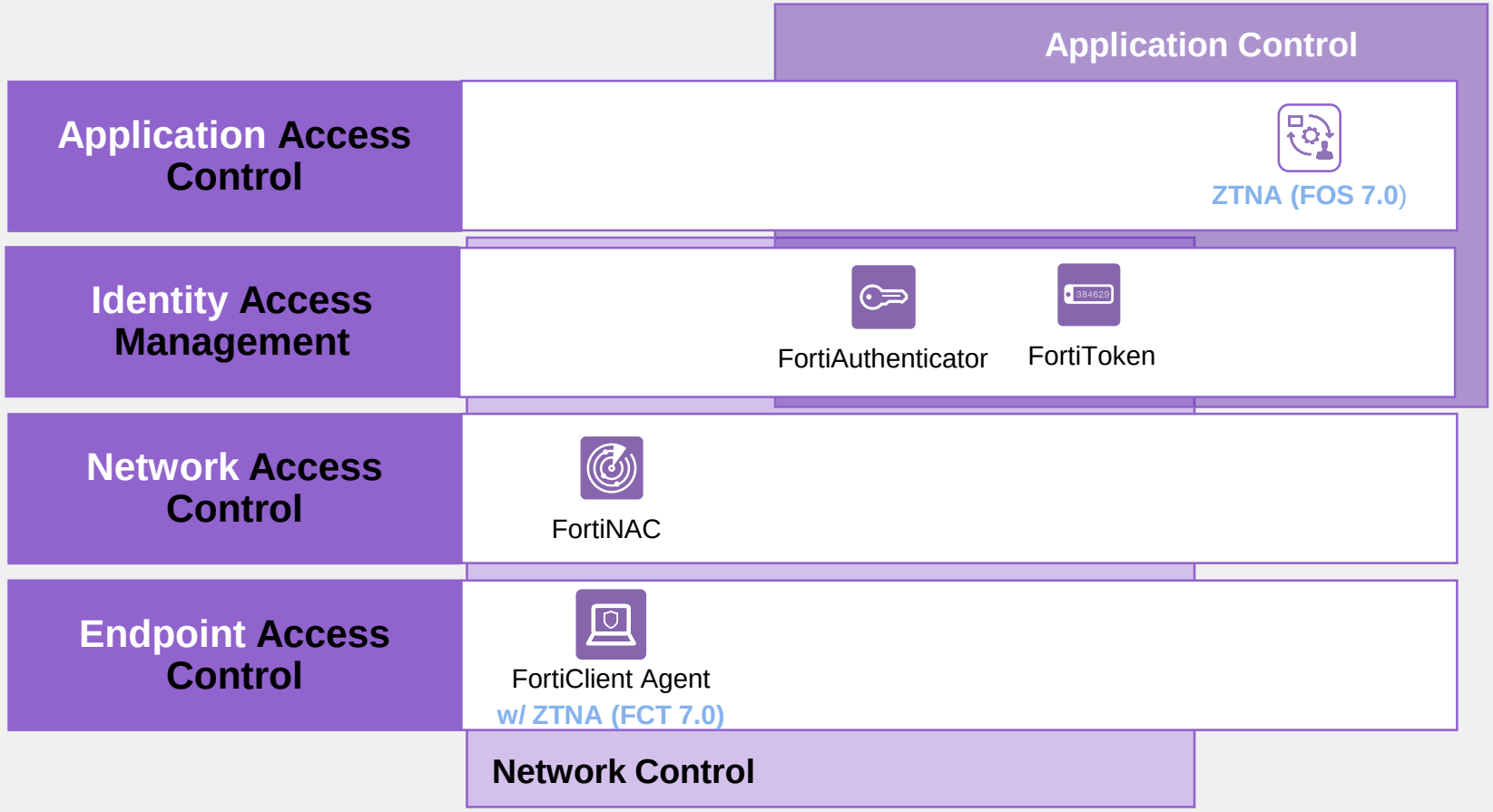
- Контроль КТО подключается и находится в сети

- Контроль ЧТО подключается и находится в сети

- Защита с помощью VPN при удаленной работе

Zero Trust Access (сегодня)

Что включает ?



Контроль доступа к приложениям

- Контроль КТО получает доступ к ПРИЛОЖЕНИЯМ, где бы они не находились

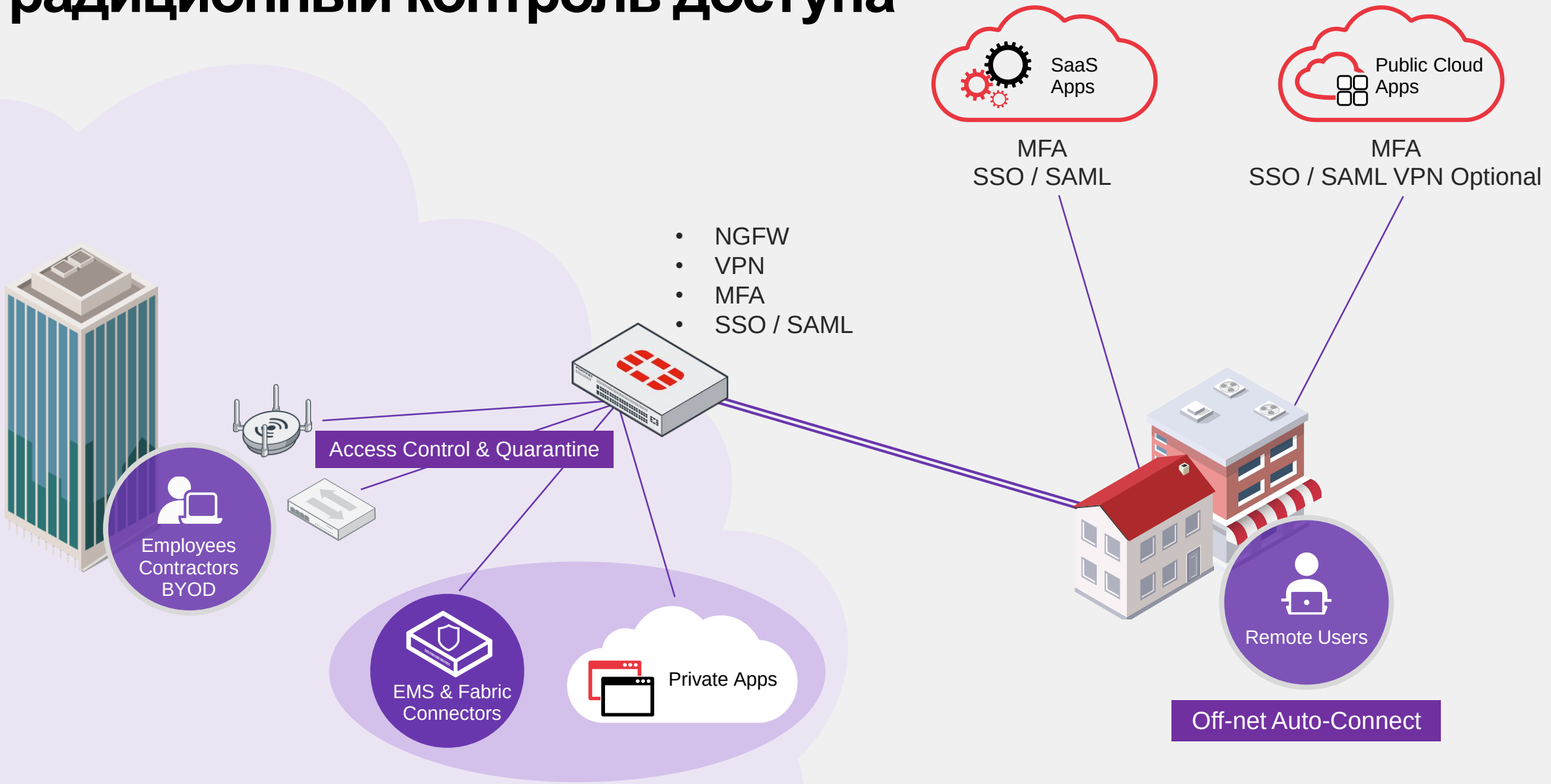
Контроль доступа

- Контроль КТО подключается и находится в сети

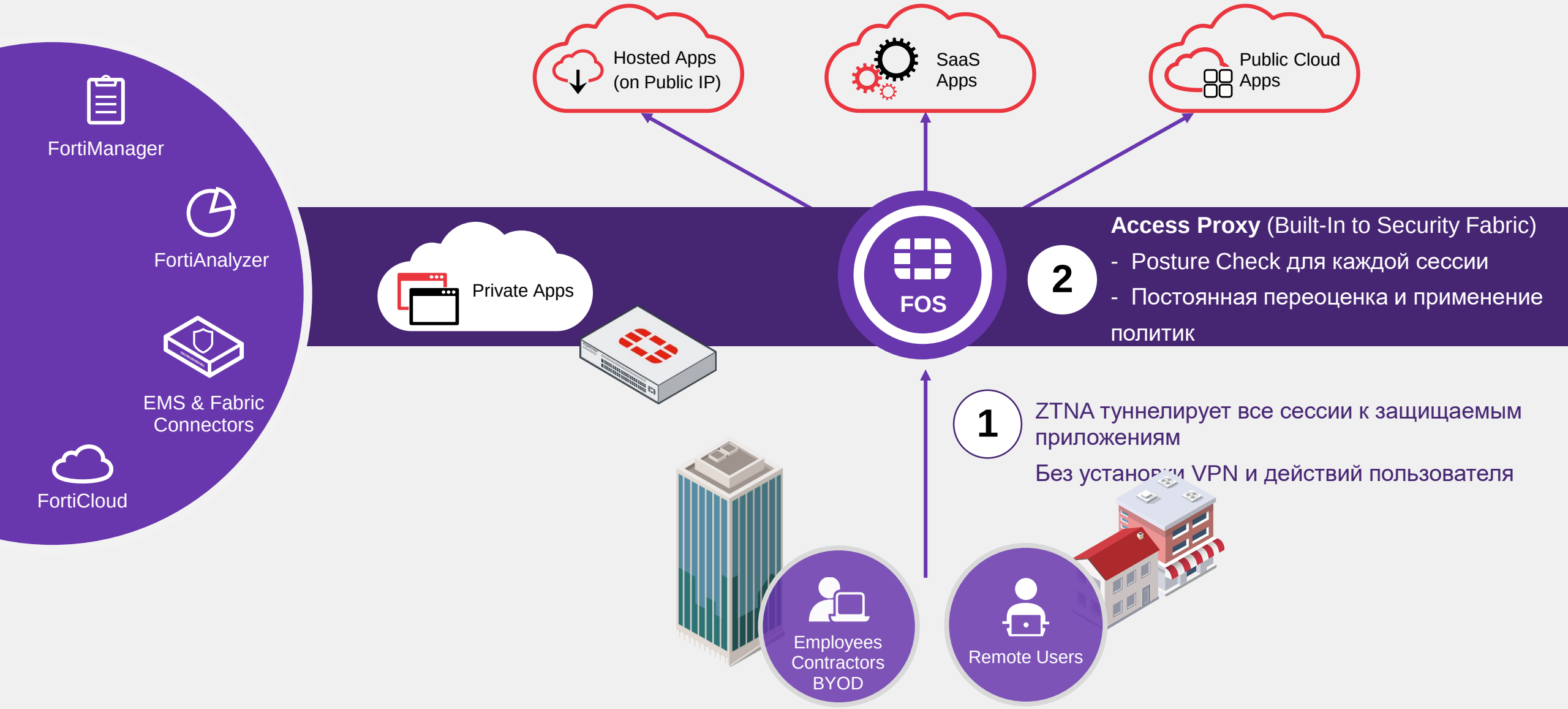
- Контроль ЧТО подключается и находится в сеть

- Secure ZTNA на удаленном доступе
- Гранулярное туннелирование VPN-like

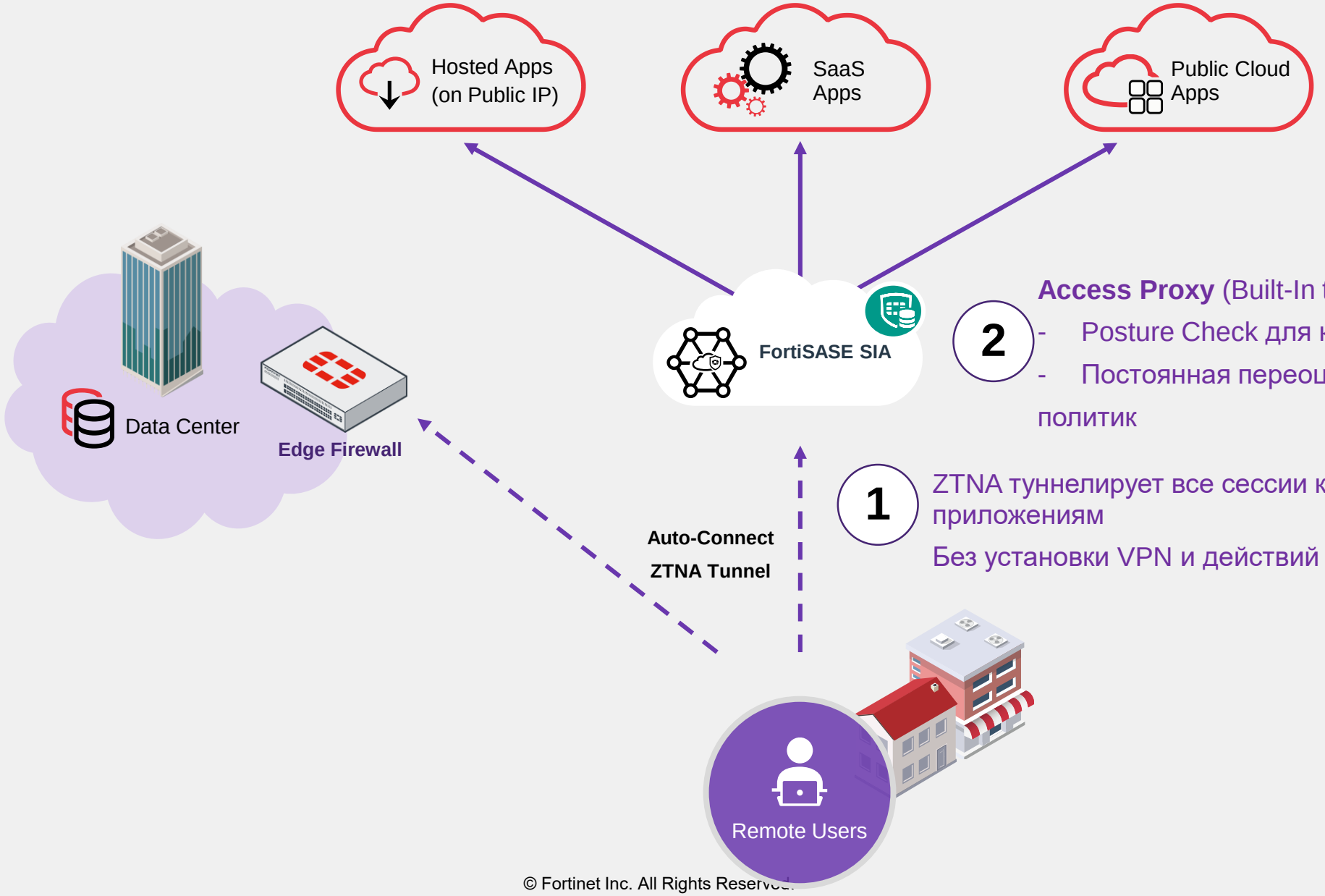
Традиционный контроль доступа



Контроль доступа с ZTNA (FortiOS Access Proxy)



Контроль доступа с ZTNA (FortiSASE SIA)



Access Proxy (Built-In to SASE SIA)

2

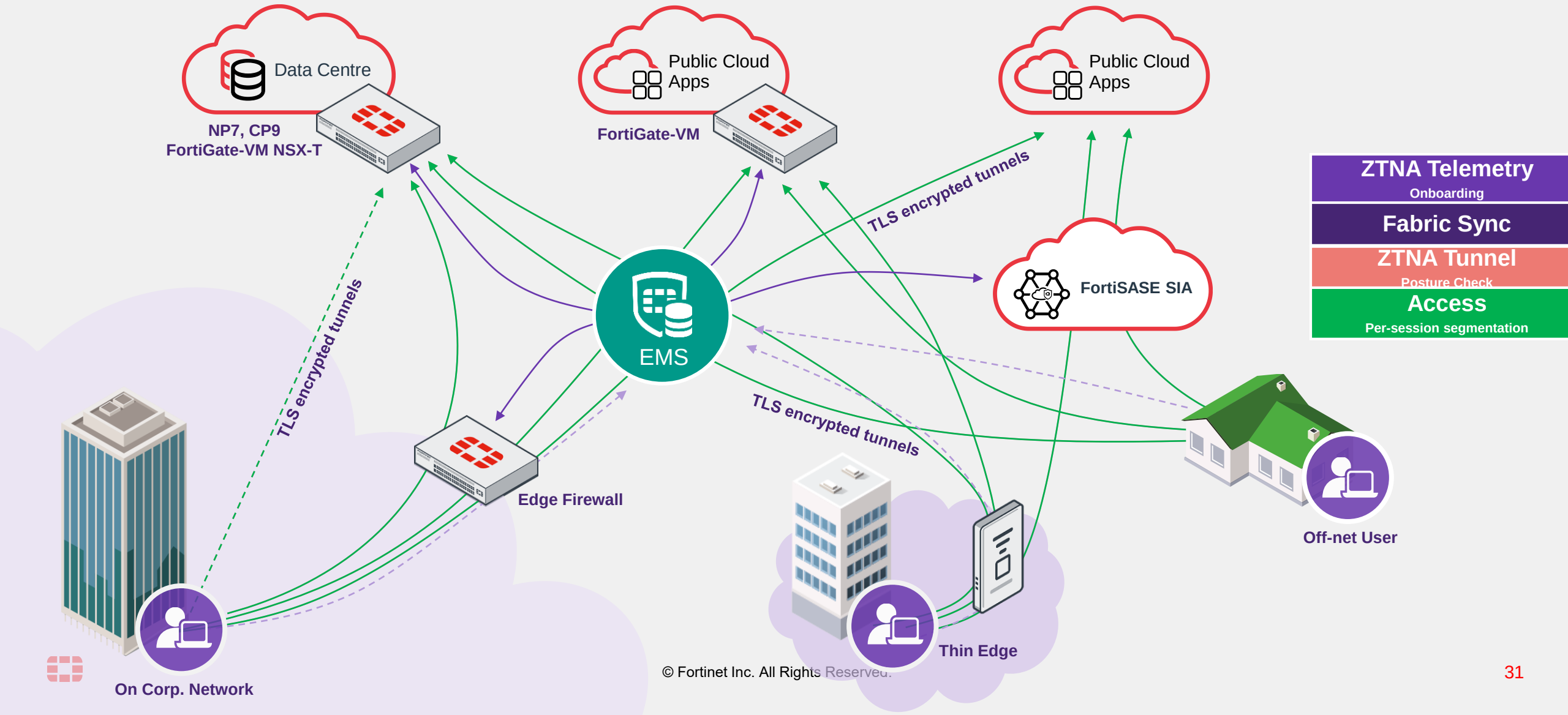
- Posture Check для каждой сессии
- Постоянная переоценка и применение политик

1

ZTNA туннелирует все сессии к защищаемым приложениям

Без установки VPN и действий пользователя

Автоматизация доступа с нулевым доверием Zero Trust для всех приложений



Выгоды для бизнеса при миграции с VPN на ZTNA

01 **Улучшение пользовательского опыта**

Автоматическое прозрачное защищенное подключение

02 **Снижение плоскости атаки**

Централизованный per session доступ к приложению

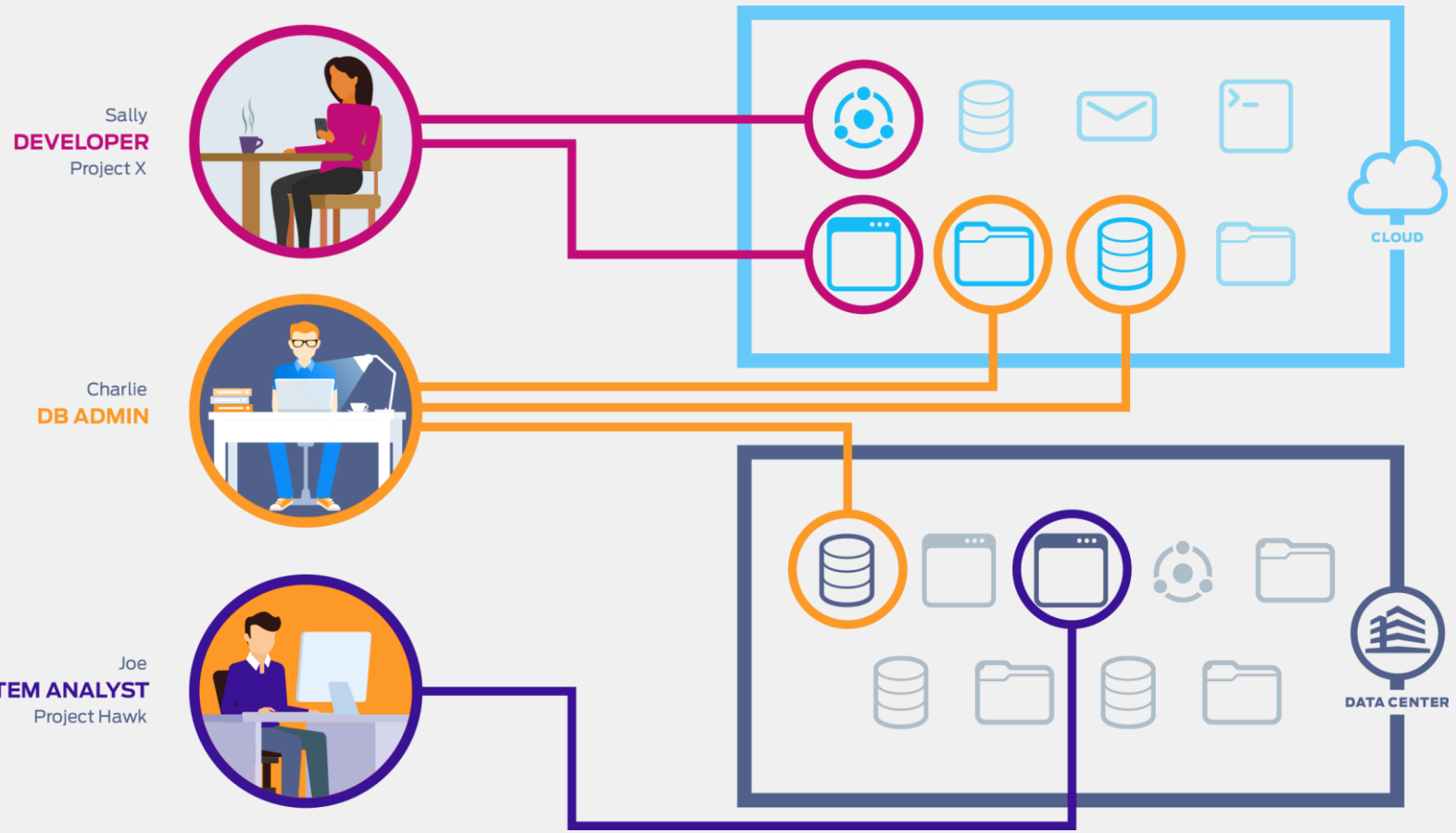
03 **Упрощение управления**

Единая политика для всех МСЭ, внутри и извне сети

ZTNA для пользователя

Пользователи независимы от местоположения

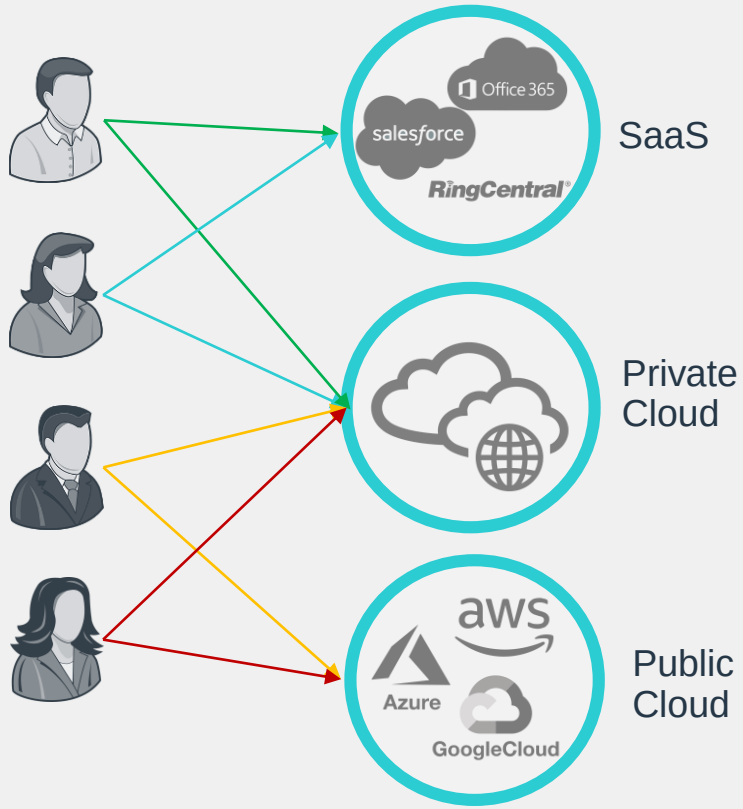
- Пользователи в / вовне Офиса
- Автоматические защищенные подключения к приложениям
- Приложения могут быть размещены где угодно
- Многофакторная аутентификация (MFA) где требуется



ZTNA для администратора

Доступ к приложениям независимо от местоположения пользователя

- Гранулярный контроль
  - Аутентификация в контексте сессии
  - Поддержка MFA
  - Оценка рисков связанных с устройствами
- Централизованное управление
  - on-prem / remote enforcement points
  - Группировка пользователей (User groups) масс конфигурации; доступность гранулярных настроек;
- Приложения могут быть где угодно
- Пользователям разрешен доступ только до необходимымх приложений и данных

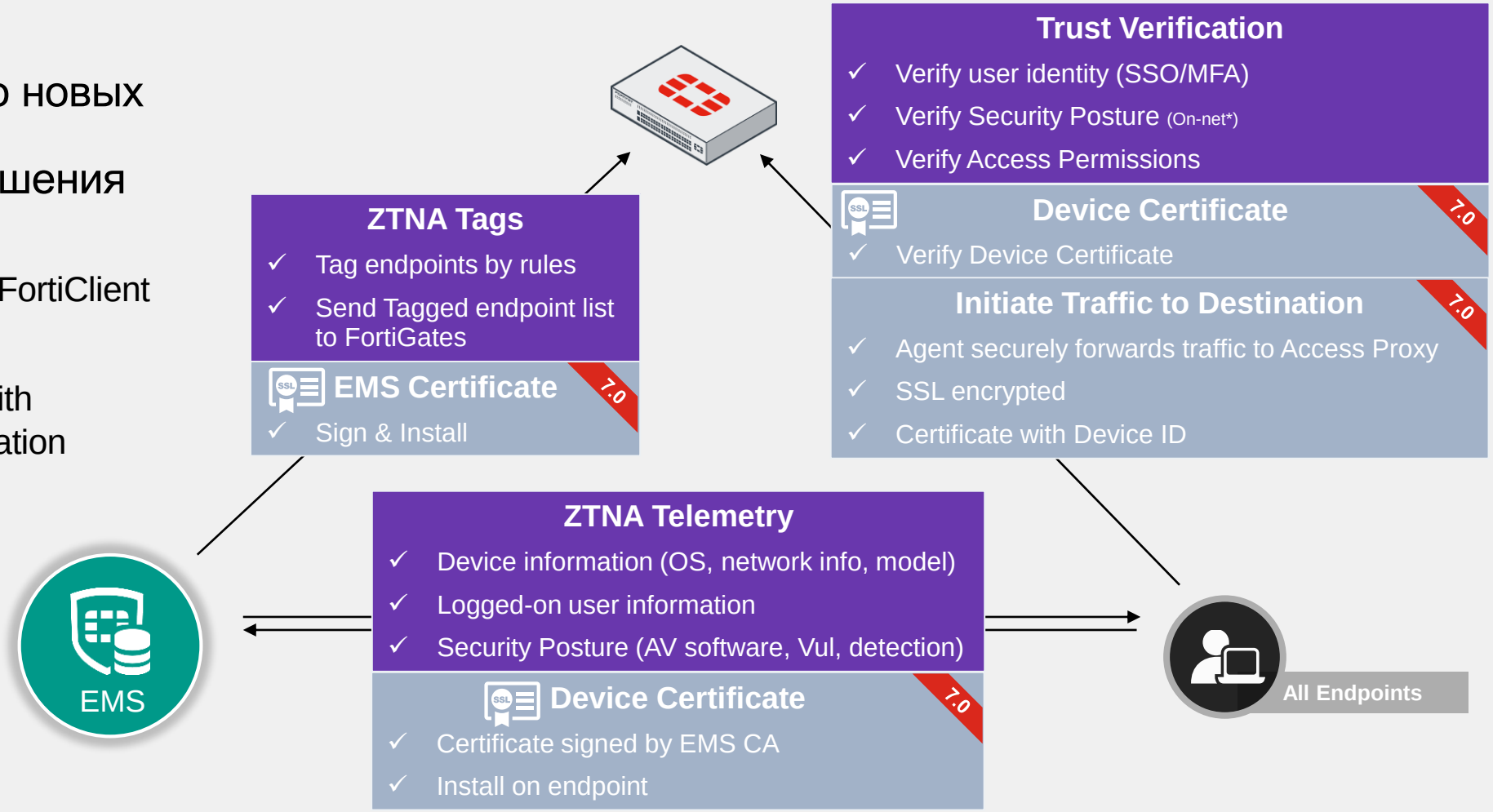


Zero-Trust Network Access

Улучшения Zero Trust в FortiOS 7.0

Добавлено несколько новых возможностей для поддержки нового решения Zero Trust

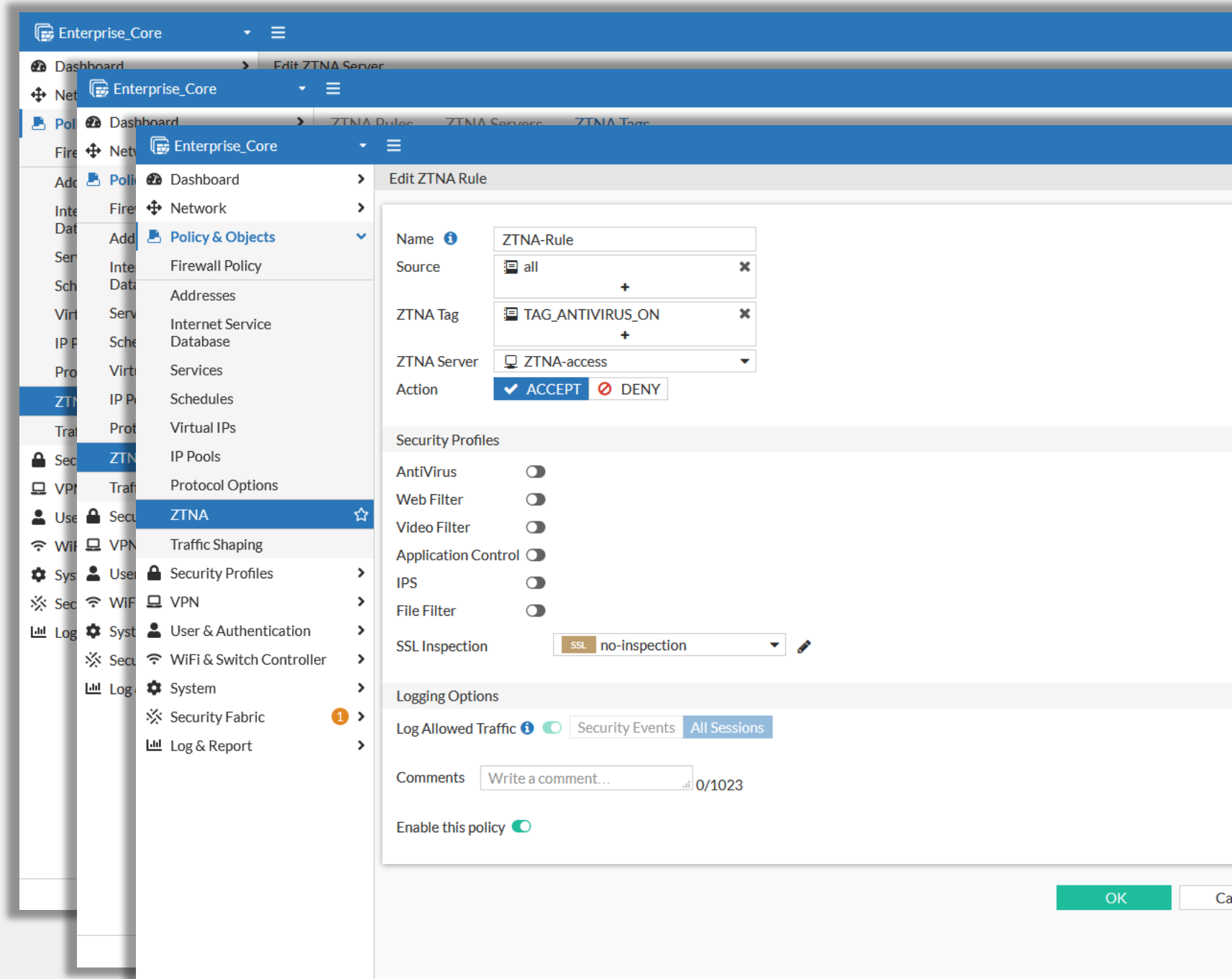
- HTTPS access proxy with FortiClient as ZTNA agent
- Support trust verification with certificate-based authentication



Настройка ZTNA

FortiGate (FortiOS 7.0)

1. Настройка публикации приложений ZTNA (servers)
2. Изучение ZTNA Tags
3. Настройка ZTNA Rules для разрешения доступа основанном на ZTNA Tags



Настройка ZTNA

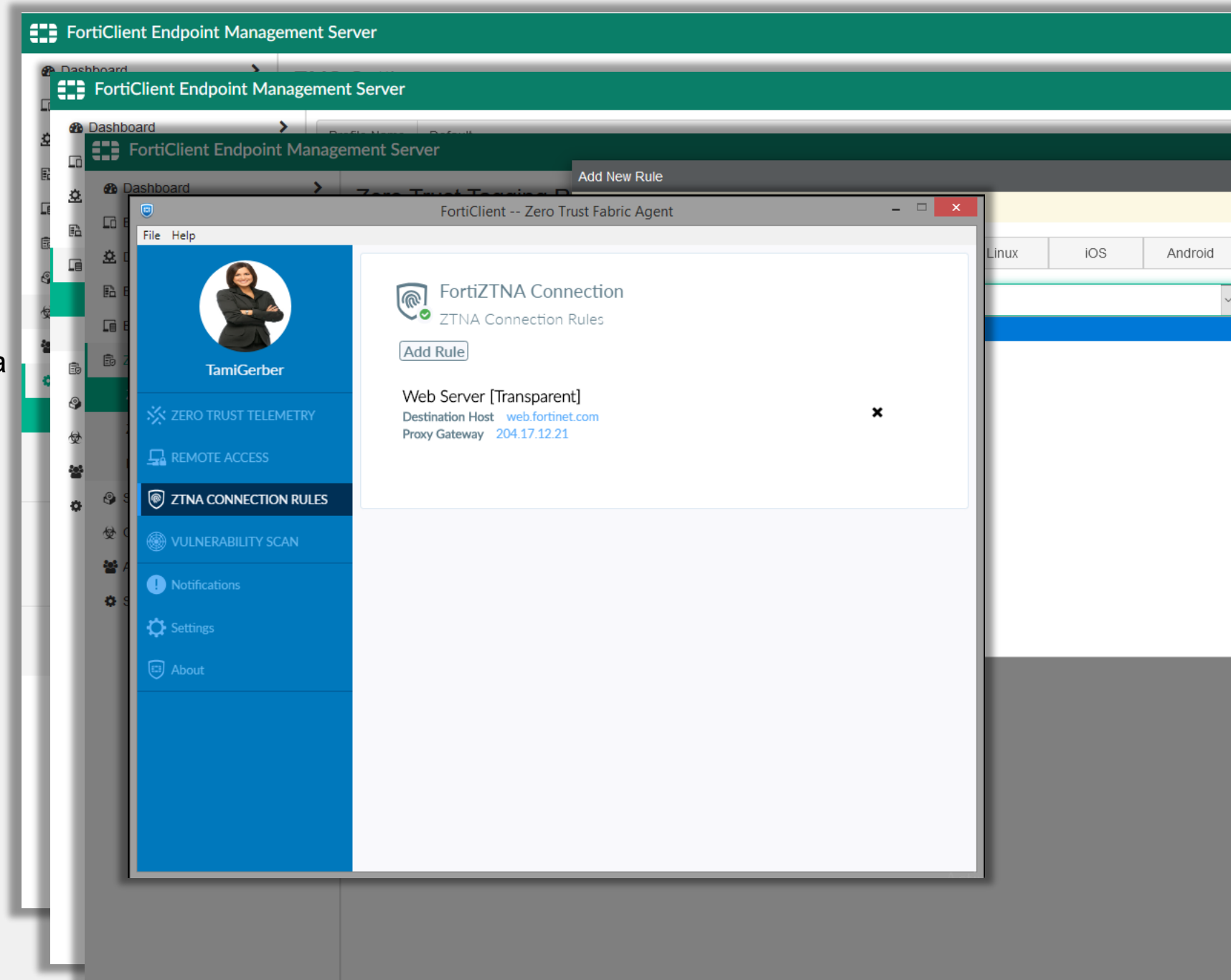
FortiClient EMS

1. CA Certificate

2. Включение ZTNA и установка сертификатов на рабочие места

3. Определение правил классификации / маркировки ZTNA Tagging Rules

4. Подключение к ZTNA приложению с рабочего места (как в примере*)



Fortinet’s ZTNA

Из чего состоит ? Использует существующие продукты и решения !

Основные Элементы

FortiGate

- FortiGate строит защищенный туннель, поддерживает таблицу доступа user group/application (FOS 7.0)

FortiClient / FortiClient EMS

- FortiClient EMS настраивает компонент ZTNA agent в FortiClient для защищенного подключения к FortiGate (FortiClient 7.0)

FortiAuthenticator

- FortiAuthenticator обеспечивает многофакторную аутентификацию и подключения SAML для SSO для облачных приложений

FortiManager

- FortiManager обеспечивает многосайтовую (в том числе с большим количеством FortiGate) координацию и управление системой

2021 ZTNA / FortiSASE SIA информация для заказа

Руководство по популярным вариантам лицензирования

	ZTNA	EPP/APT	SASE	CHROMEBOOK
IT Hygiene				
Vulnerability Agent and Remediation	✓	✓	✓	
FortiGuard Web Filtering	✓	✓	✓	✓
USB Device Control	✓	✓	✓	
Zero Trust Agent				
Zero Trust Agent	✓	✓	✓	
Central Management Via EMS	✓	✓	✓	✓
Central Logging and Reporting	✓	✓	✓	✓
Dynamic Security Fabric Connector	✓	✓	✓	
SSL VPN with MFA	✓	✓	✓	
IPsec VPN with MFA	✓	✓	✓	
Endpoint Security (EPP)				
AI-powered NGAV		✓	✓	
FortiClient Cloud Sandbox		✓	✓	
Automated Endpoint Quarantine		✓	✓	
Application Firewall		✓	✓	
Application Inventory		✓	✓	
Cloud-based Inspection				
SSL Inspection			✓	
Inline AV and Antimalware			✓	
Intrusion Prevention (IPS)			✓	
FortiGuard Web Filtering			✓	
DNS Security			✓	
Data Leak Prevention			✓	
Additional Services				
On-Premise/Air Gap Option	✓	✓		✓
24×7 Support	Included	Included	Included	Included
FortiCare Best Practice Services (BPS)	Included 1st Year	Included 1st Year	Included 1st Year	Included 1st Year

Q: Наиболее простой способ заказа ?

A: Заказ SKU (подписки) по кол-ву рабочих мест (стекируются)

Q: Наиболее простой способ продления?

A: Заказ SKU продления (подписки) по кол-ву рабочих мест (стекируются)

Q: Можно ли использовать одну лицензию on prem и Cloud ?

A: Нет, on-prem вариант имеет отдельный SKU для заказа.

Q: Когда можно заказывать новые SKU?

A: Начиная с Q1 2021, доступны для FortiClient 6.4.3 и выше.

Q: Что такое Best Practice Service?

A: BPS Service включен в 1ый год подписки, предназначен для упрощения развертывания и использования ресурсов Fortinet для внедрения согласно best practice.

Обзор улучшений FortiOS 7.0

Поддержка аппаратных платформ FortiGate

FortiOS 7.0.0

# = available at a later time, possibly on patch releases
Grey = EoO Products

	6.2.7	6.4.5	7.0.0
FG/FWF-30E/50E Series	●		
FG/FWF-60E	●	●	●
FG/FWF-40F Series	●	●	●
FG/FWF-60F Series	●	●	●
FG-80D	●		
FG-80E Series	●	●	●
FG-80F Series	●	●	#
FG-90E Series	●	●	●
FG/FWF-92D Series	●		
FG-100D/140D Series	●		
FG-100/101E Series	●	●	●
FG-100F Series	●	●	●
FG-200/201E	●	●	●
FG-200F	●	●	#
FG-300E/500E Series	●	●	●

	6.2.7	6.4.5	7.0.0
FG-300D/400D/500D/600D Series	●	●	
FG-400E/600E Series	●	●	●
FG-800D/900D/1x00D Series	●	●	●
FG-1100E Series	●	●	●
FG-1800F Series	●	●	#
FG-2200E, 3300E Series	●	●	●
FG-2000E, 2500E	●	●	●
FG-2600F Series	●	●	#
FG-3X00D Series	●	●	●
FG-3400E/3600E	●	●	●
FG-3960E/3980E	●	●	●
FG-4200/4400F Series	●	●	#
FG-5001D/5001E	●	●	●
FG-6000/7000 Series	●	●	#

Поддержка облачных платформ и платформ SDN

FortiOS 7.0

Гипервизоры и платформы публичных облаков	7.0
VMware ESXi / vSphere	●
Microsoft Hyper-V	●
KVM	●
Citrix XEN / Open Source XEN	●
Nutanix AHV	●
Cisco CSP 2100	●
Amazon Web Services (AWS)	● (BYOL / PAYG)
Microsoft Azure	● (BYOL / PAYG)
Google Cloud Platform (GCP)	● (BYOL / PAYG)
Alibaba AliCloud	● (BYOL / PAYG)
RackSpace	● (BYOL / PAYG)
Oracle Cloud Infrastructure (OCI)	● (BYOL)
RackSpace	● (BYOL / PAYG)

Платформы SDN	7.0
VMware NSX-V, NSX-T	●
Cisco ACI	●
OpenStack	●
Nuage VSP	●
Nutanix Prism Central	●

Security-driven Networking

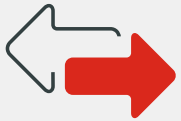
NGFW

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

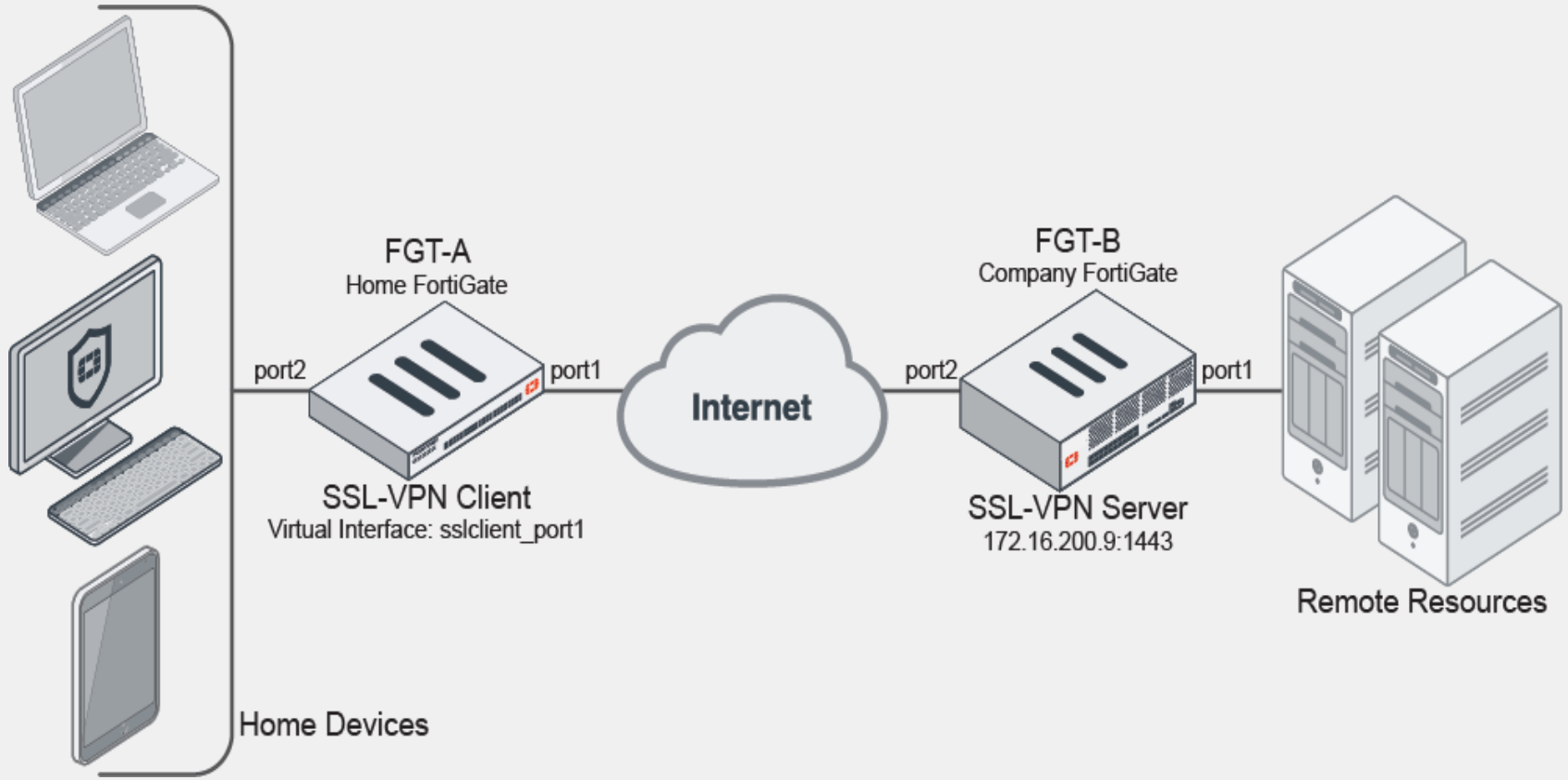
- New IPsec Interface to handle packet duplication, supports static and dialup VPNs

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

FortiGate в роли SSL VPN Client

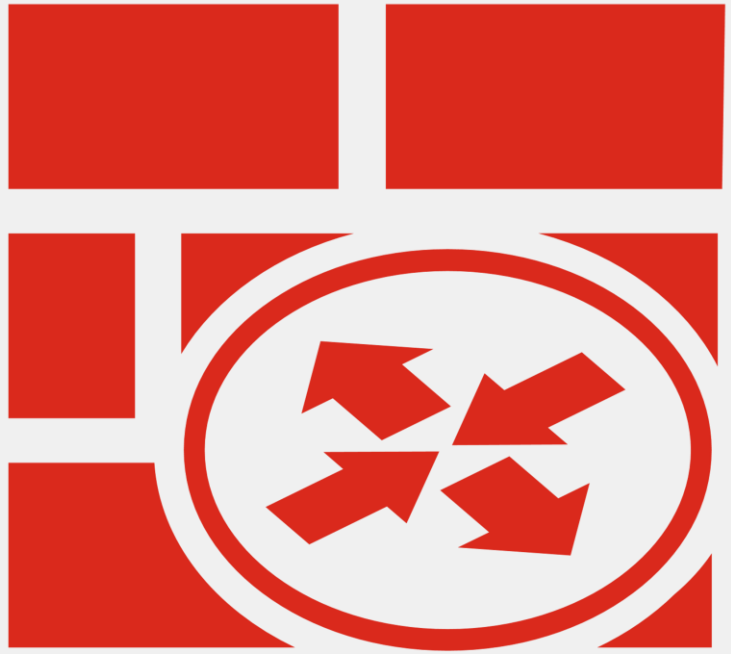


Security-driven Networking

SD-WAN - Advanced Routing

Улучшения в BGP и OSPF

- Добавлена новая опция ECMP for recursive BGP NH resolution для поддержки более сложных сценариев развертывания SD-WAN
- Поддержка рекурсивного разрешения BGP через другой BGP маршрут для сценариев Multi-Regional SD-WAN с поддержкой cross-region ADVPN
- Улучшения в GUI для конфигурации BGP и OSPF

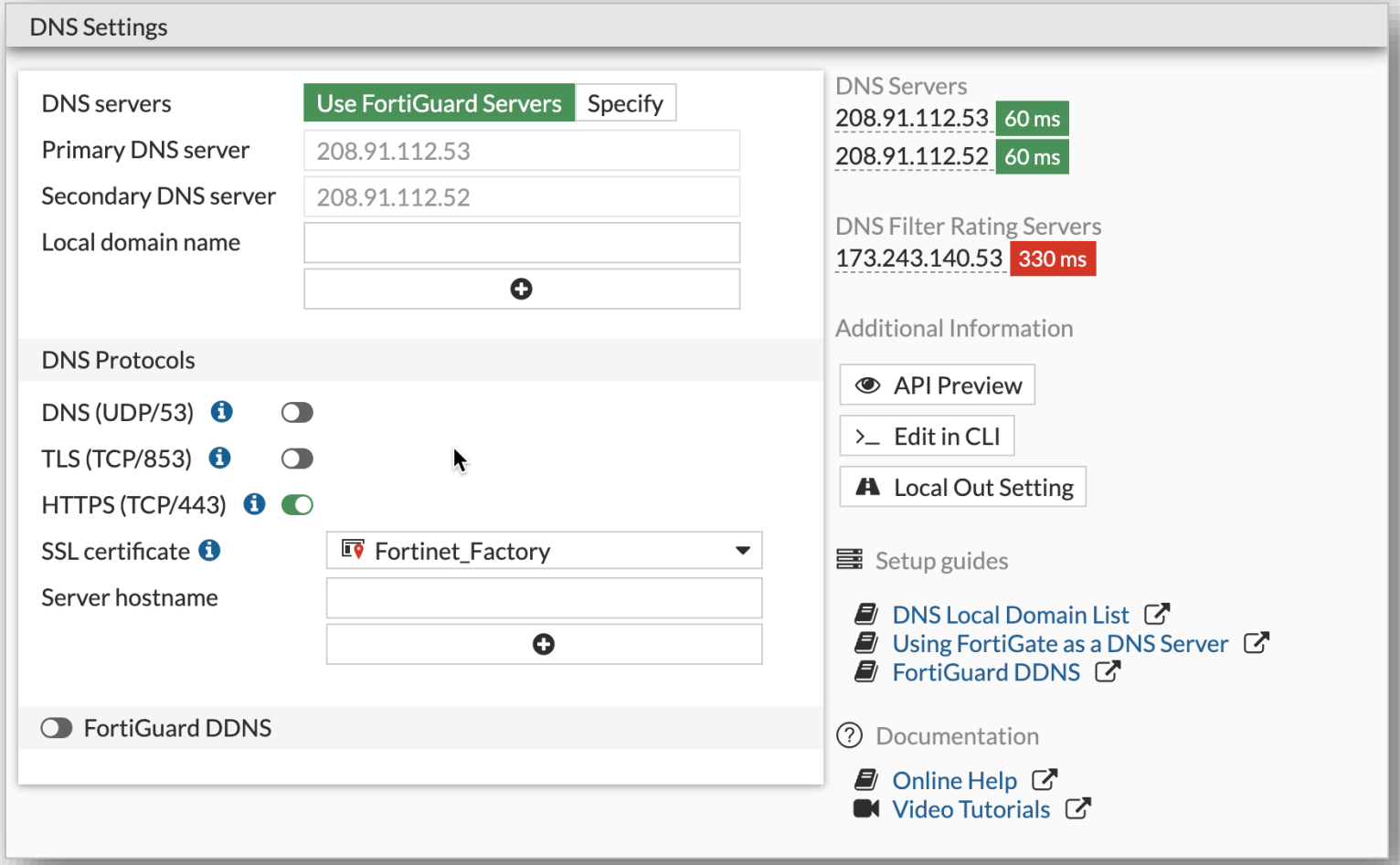


Security-driven Networking

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

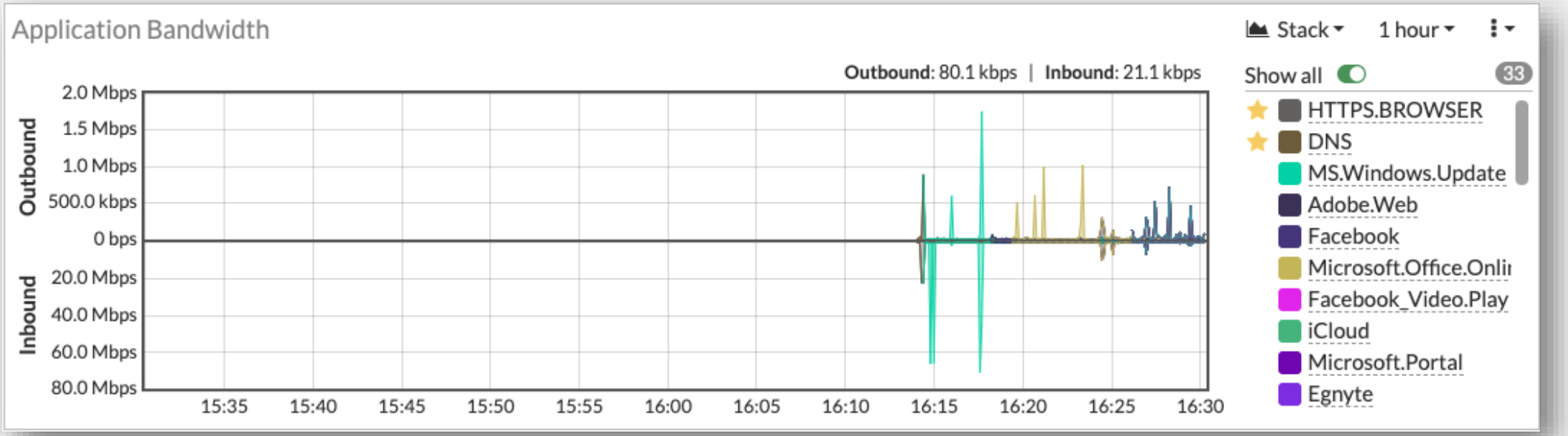


Security-driven Networking

Виджет графика загрузки сетевой полосы пропускания по приложениям

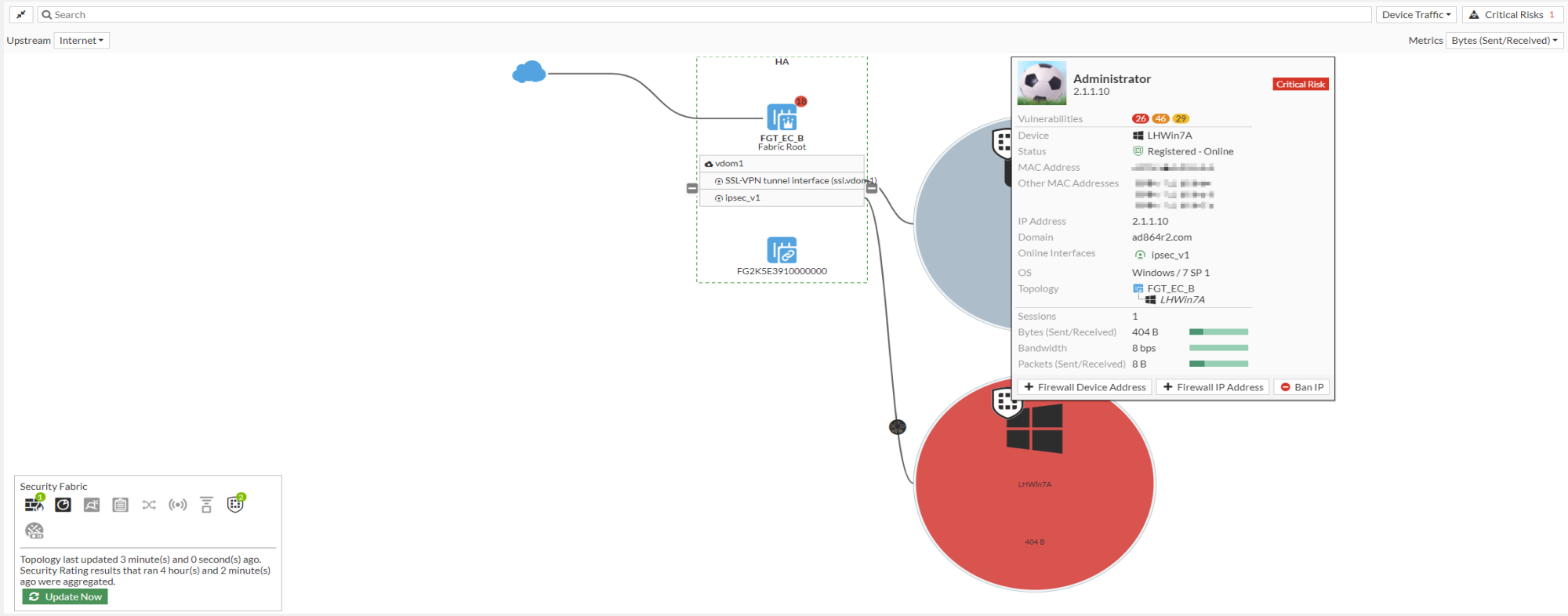
Новый виджет для визуализации загрузки полосы пропускания по приложениям

- Есть возможность фильтрации по отдельным приложениям
- Фильтр по умолчанию показывает top X наиболее значительных приложений с точки зрения загрузки полосы пропускания



Security-driven Networking

Детальная информация о пользователях, подключенных через VPN с помощью EMS

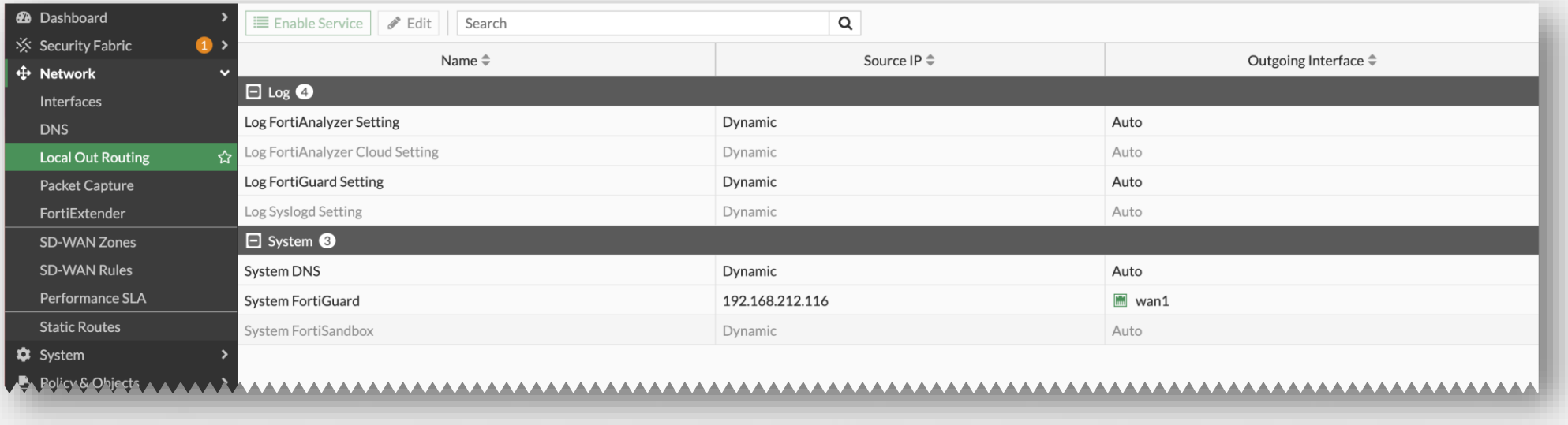


Security-driven Networking

Local Out Page

Консолидация всех настроек Local Out на одной странице Network / LocalOut Routing

- Настройки могут как на уровне глобальных настроек или на уровне VDOM

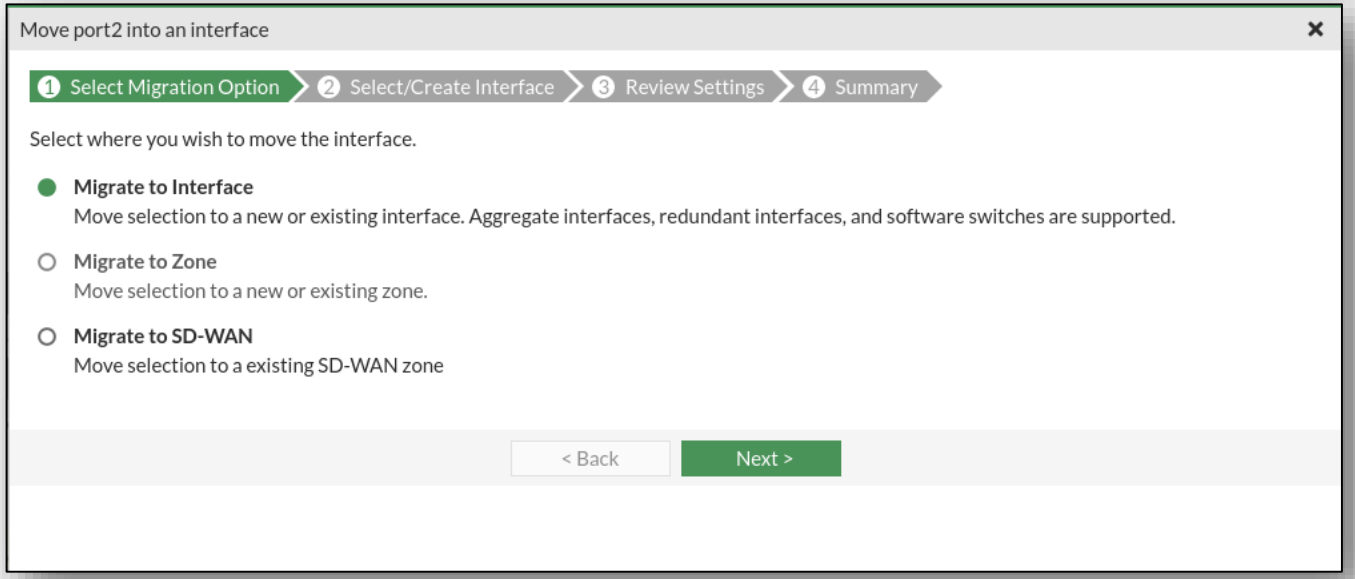


Security-driven Networking

Помощник миграции интерфейсов / Interface Migration Wizard

Специальный инструмент GUI для миграции интерфейсов из одной части конфигурации в другую.

- Обеспечивает возможность перемещения существующих объектов, даже если они имеют ссылки / привязки в конфигурации
- Примеры:
  - Смена VLAN ID после назначения
  - Перемещение интерфейсов в SD-WAN в случае, если они уже имеют привязку в политиках МСЭ
  - Добавление интерфейса в Зону в случае, если они уже имеют привязку в политиках МСЭ

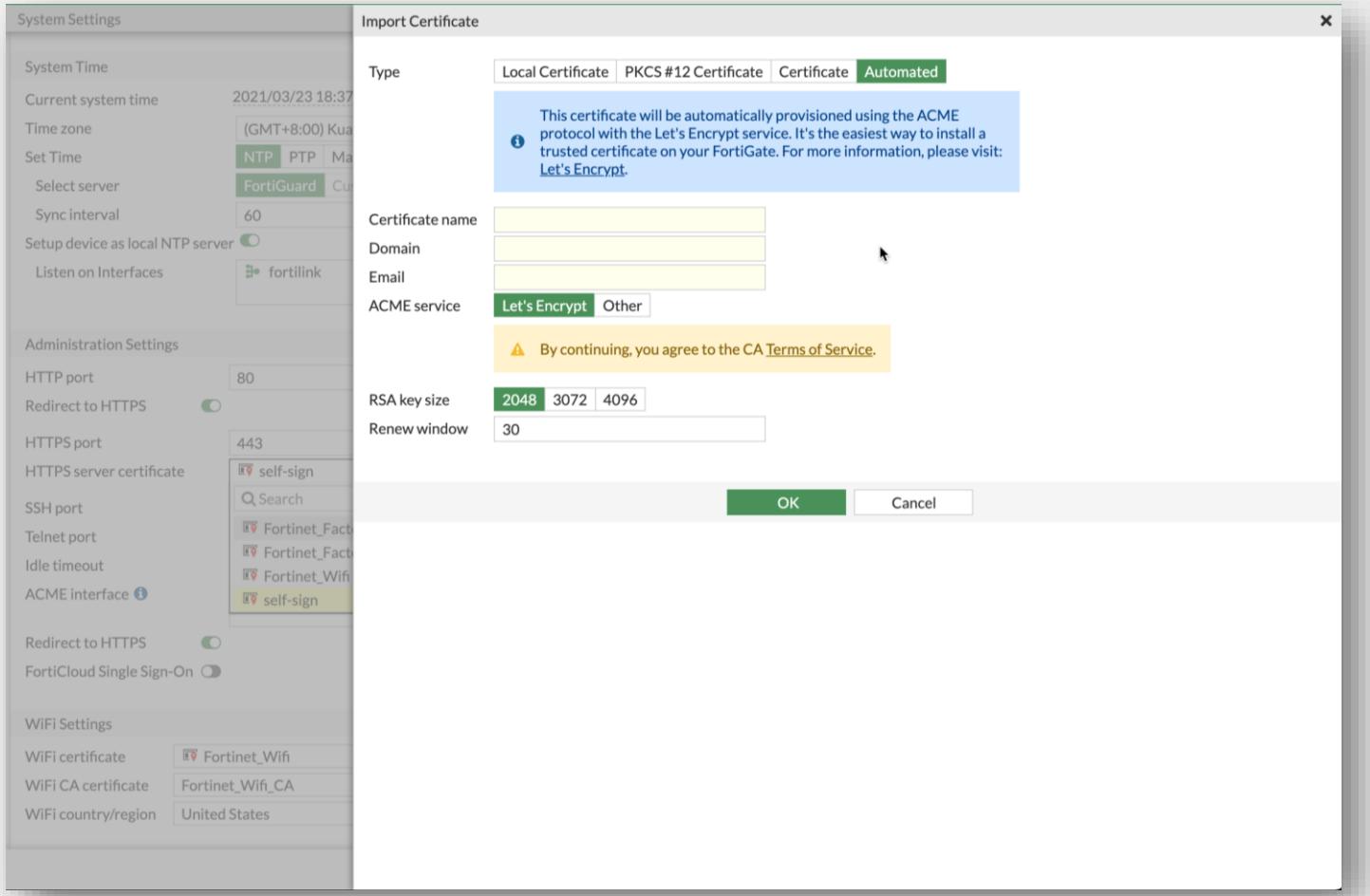


Security-driven Networking

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

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

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

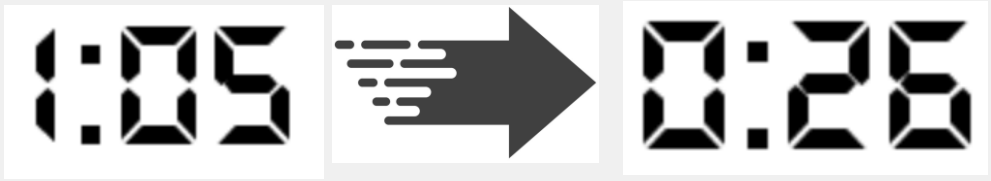
- Allow EMS side to approve connector request for the entire fabric (of FG) with a single click, when the request comes from the root of the fabric.

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

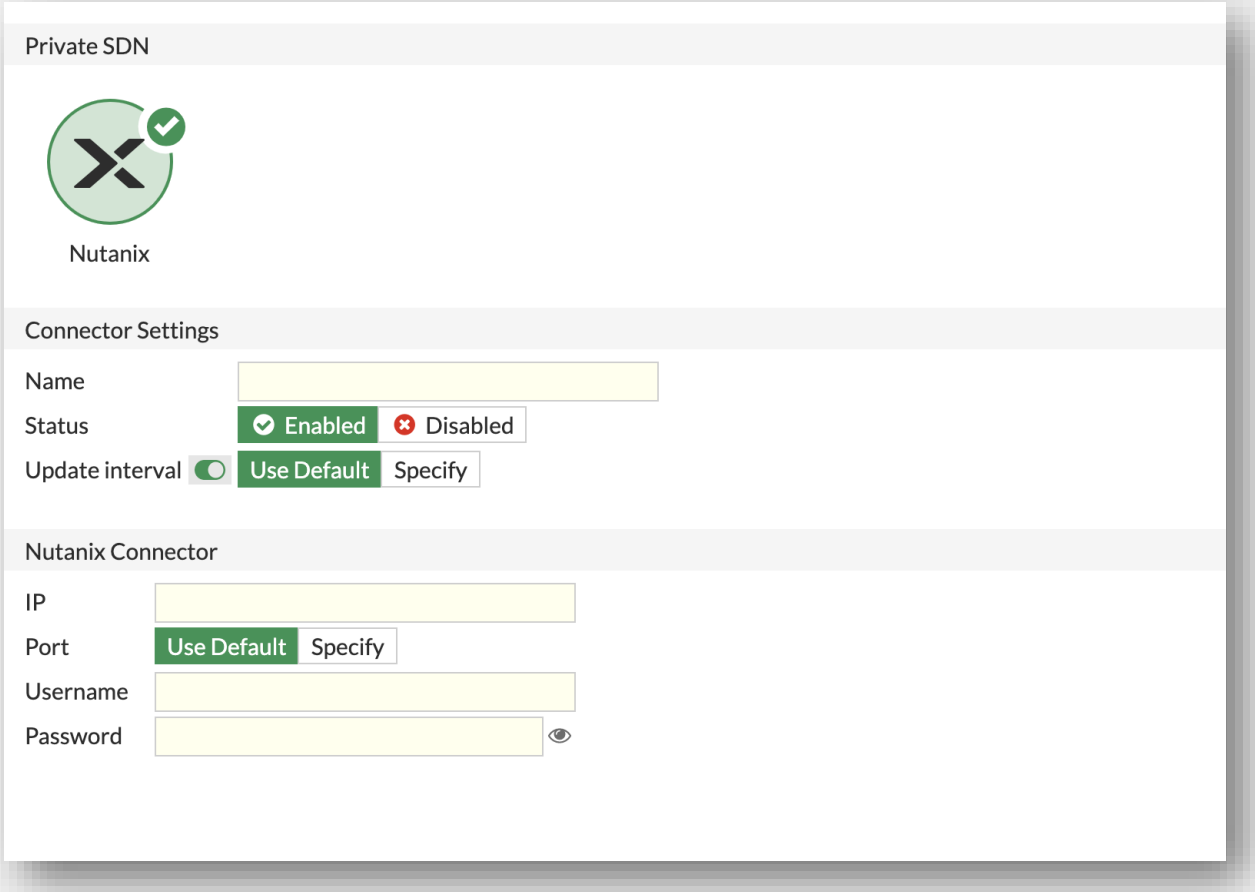
```
config switch-controller
   set nac-periodic-interval <5-60 sec>
end
```

Dynamic Cloud Security

Nutanix Connector

API коннектор к Nutanix Prism Central

- Аналогичный OpenStack Connector



AI-driven Security Operations

Обнаружение вредоносного ПО с помощью AI

Замена старого эвристического движка на новый с поддержкой AI

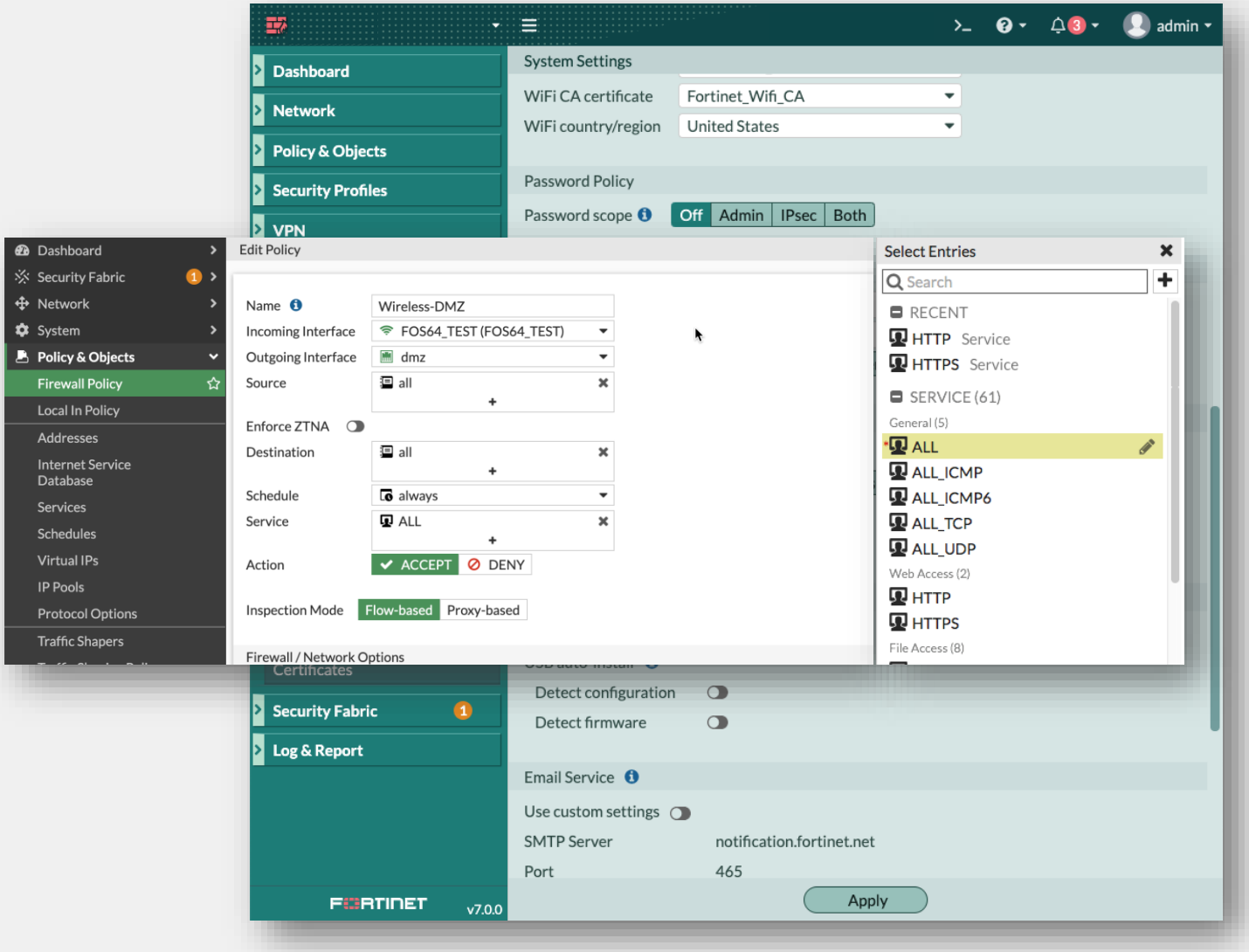
- Разрабатывался командой AV/Sandbox engine в последние 4 года.
- Тот же движок используется в FortiClient 6.4

Fabric Management Center

Улучшения в интерфейсе GUI

Представлен новый дизайн GUI (unified UX design), который будет выравниваться для всех продуктов Security Fabric

- Улучшения в функции “Global Search”
- Другие примеры
  - Часто используемые объекты могут быть показаны ближе к верху
  - Сортировка результатов поиска / фильтров по алфавиту или релевантности
  - Добавлена поддержка вложенных подсказок для инструментов
- Добавлены больше тем, включая ретро 3.0



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.

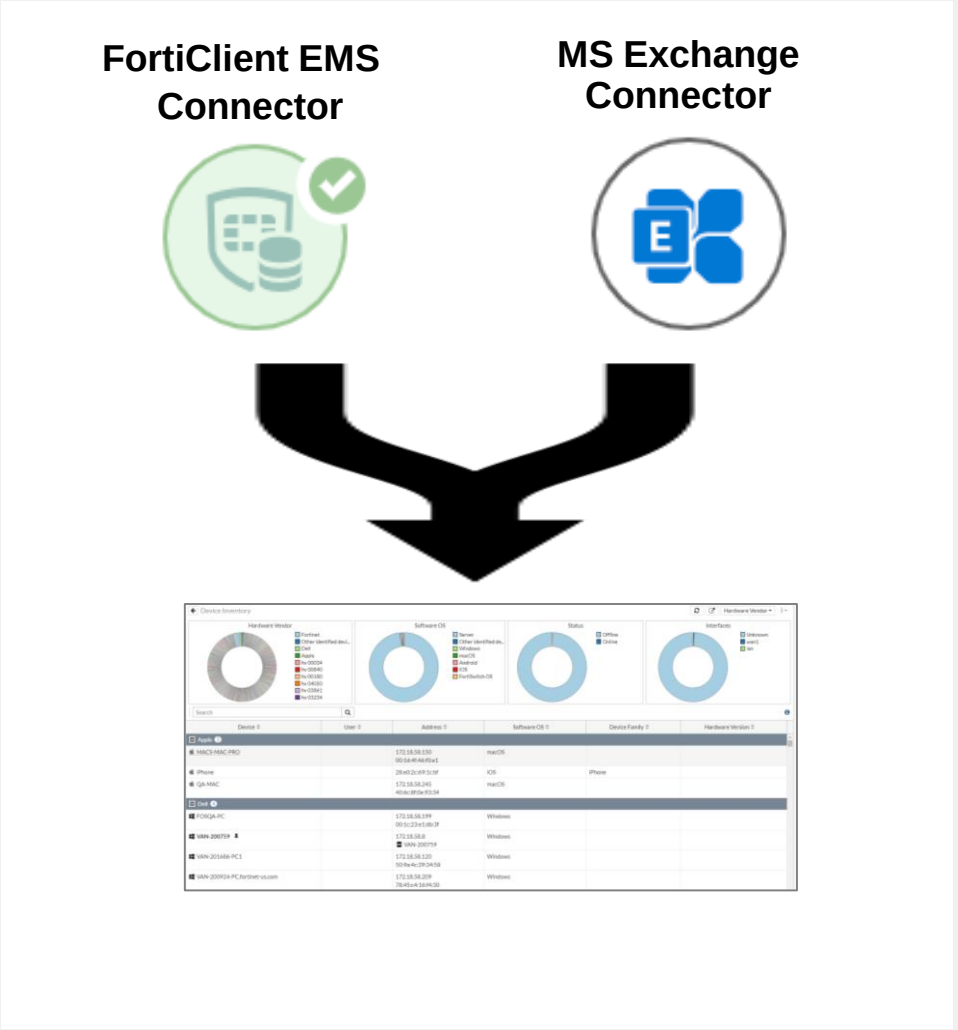
```
config switch-controller managed-switch
  edit "FSW"
        set firmware-provision [ enable |
        disable ] firmware-provision-version <
        major.minor.build >
  next
end
```

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

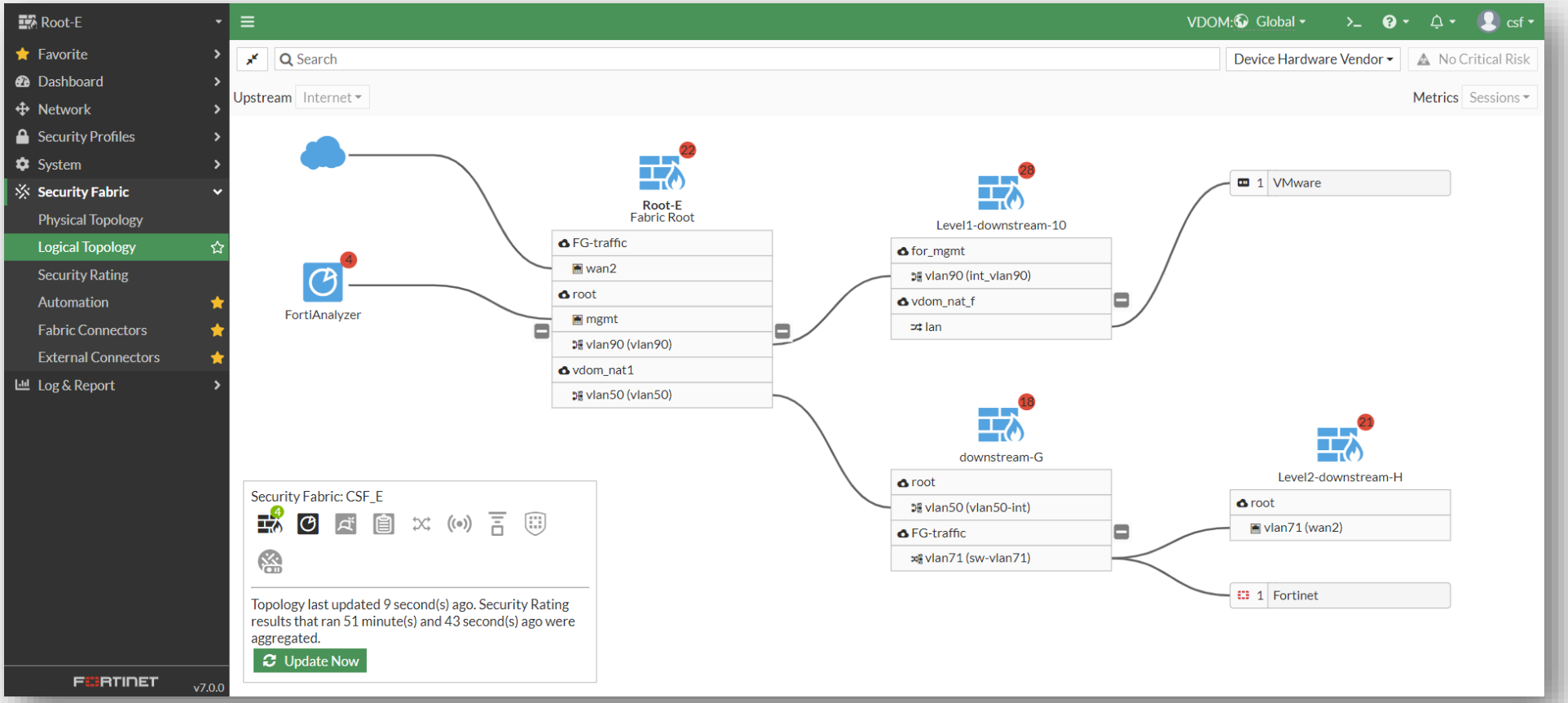


Fabric Management Center

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

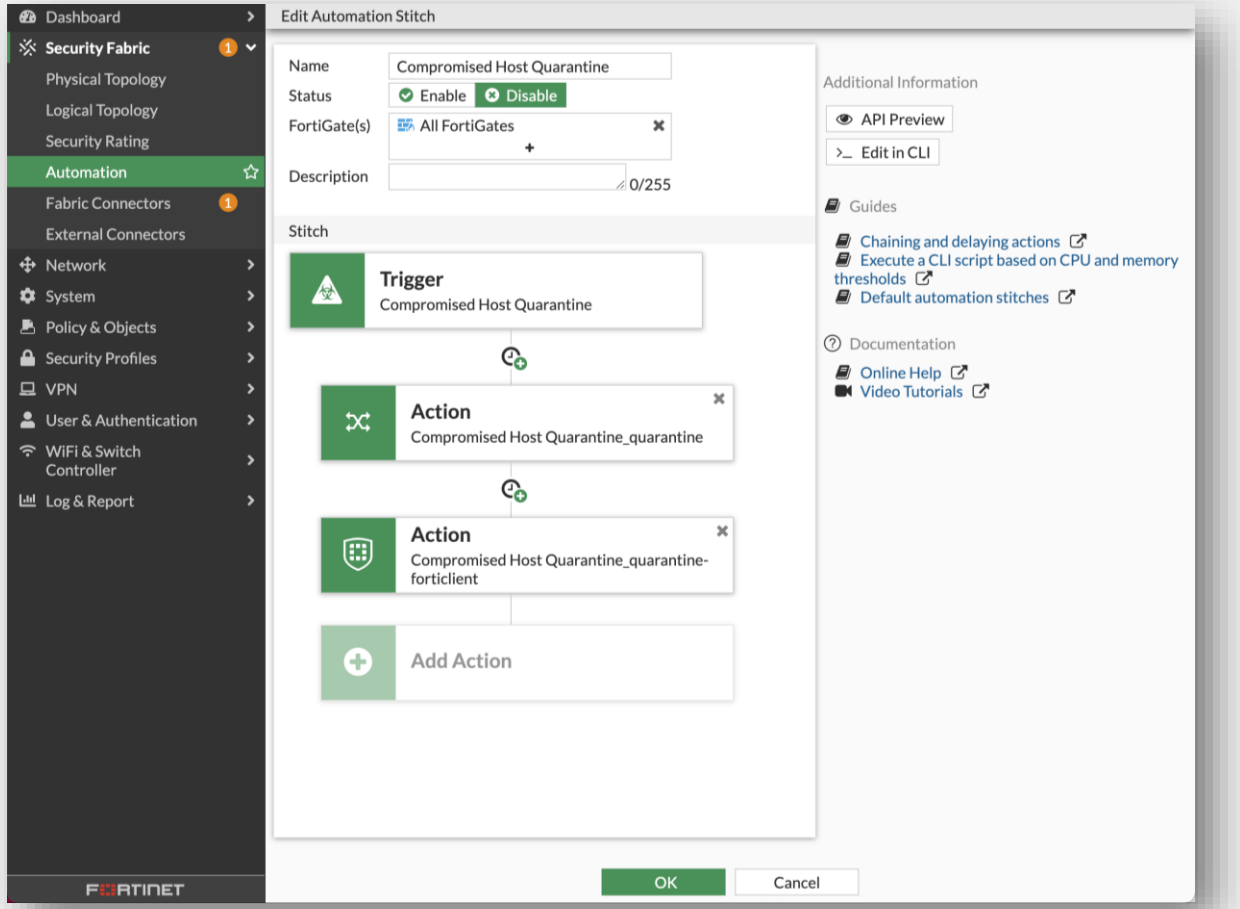


Fabric Management Center

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

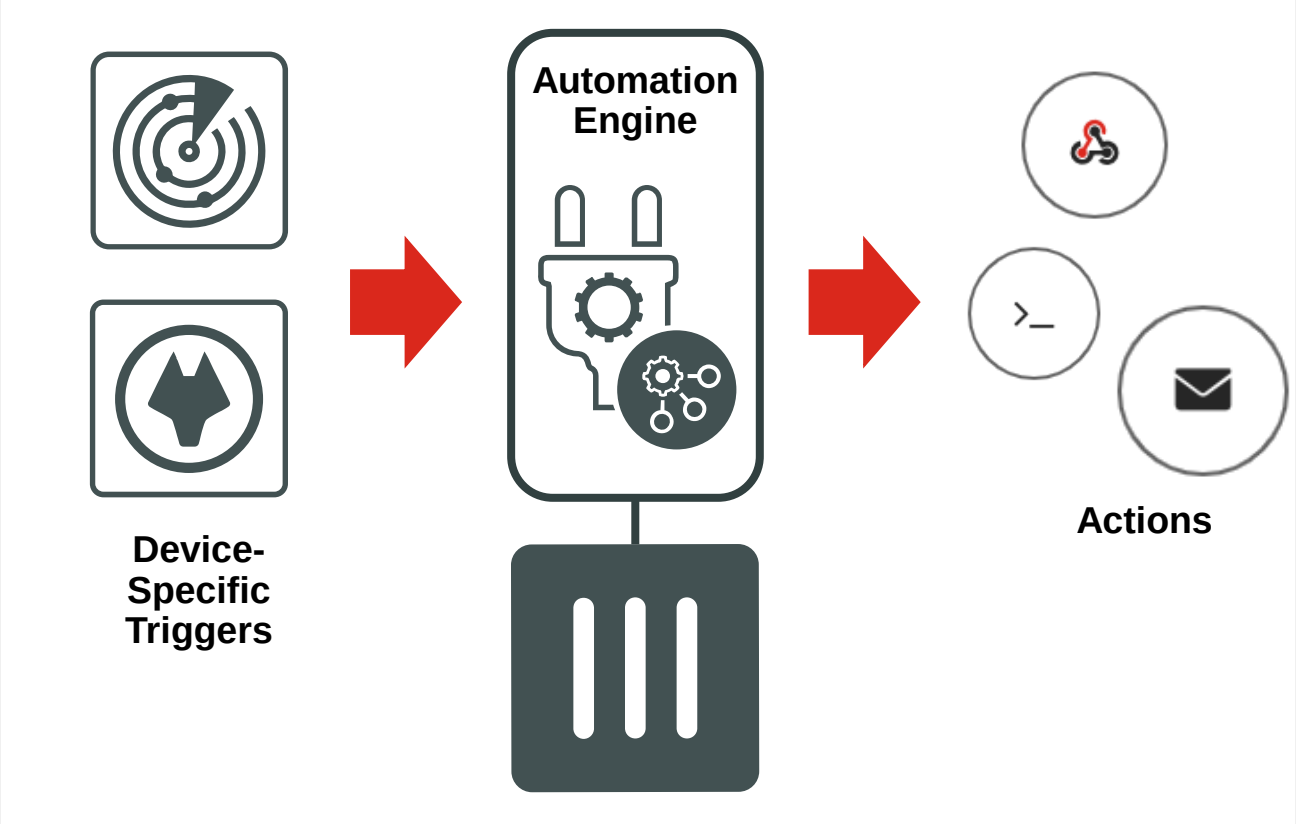


Fabric Management Center

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

Интеграция с FortiAI, FortiDeceptor, FortiTester, and FortiWeb

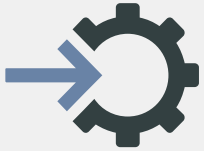
Fabric integration with more Fortinet products to yield unique solutions

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

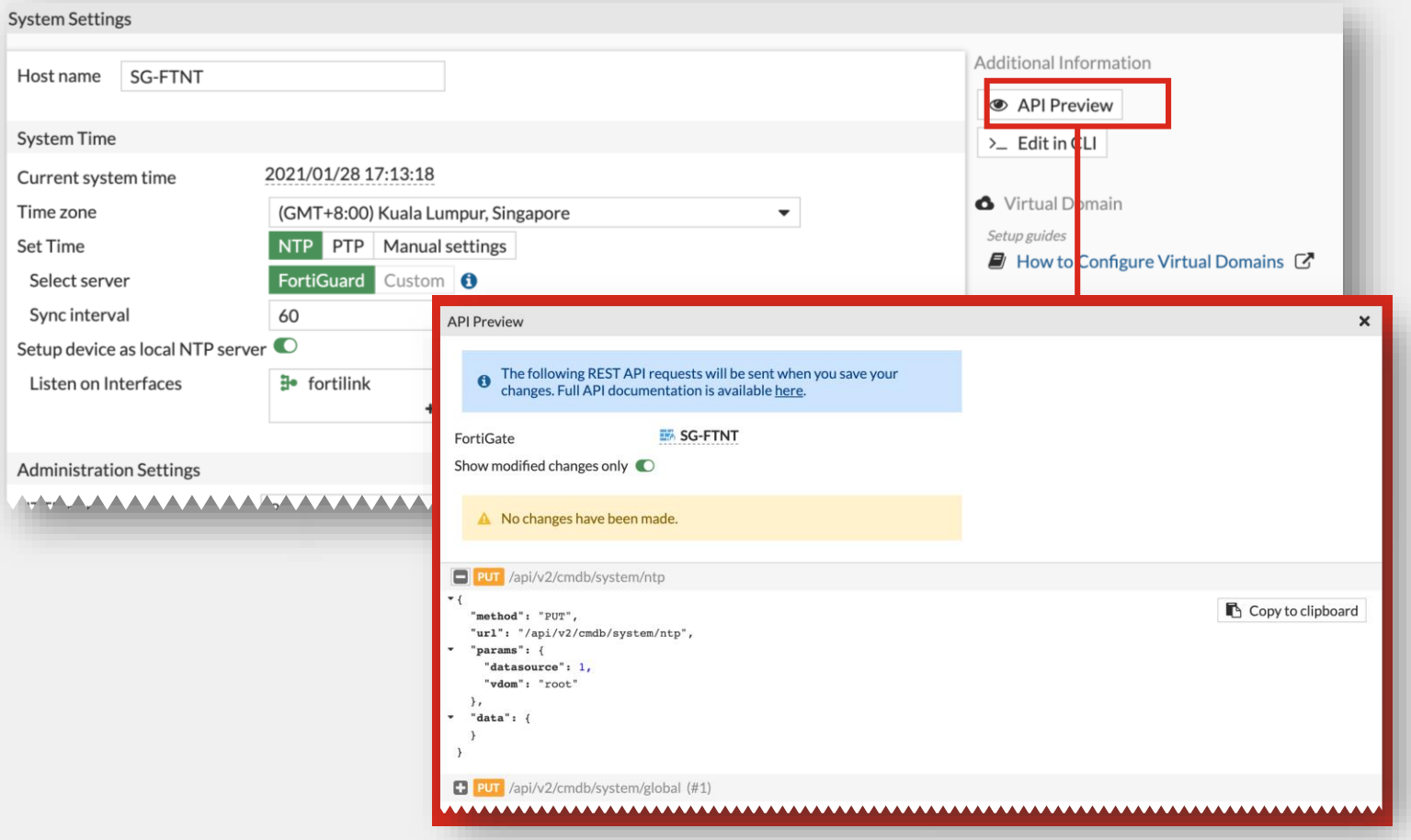
- Extends Threat Feed connectors to each VDOMs

Fabric Management Center

Просмотр эквивалента команд REST API для действий GUI

Добавлена поддержка просмотра команд REST API соответствующих действиям в GUI

- Добавлена кнопка API Preview на вкладка справа, позволяющая пользователю просматривать какие запросы к API выполняются в FortiOS при нажатии "OK" или "Apply".
- Если для этого требуется множественные запросы, то они будут показываться в множественных закладках

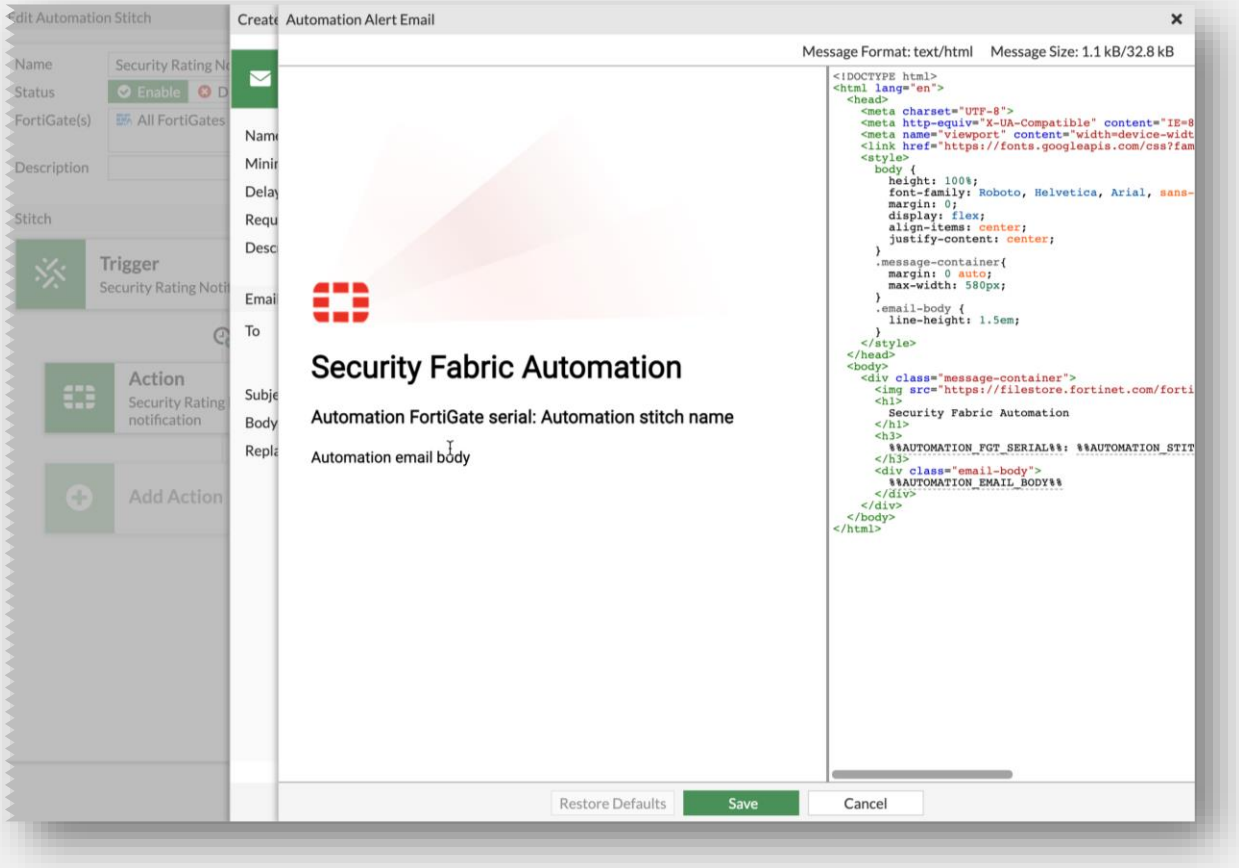


Fabric Management Center

Использование replacement message для рассылки уведомлений по email

Действие автоматизации Email Action может теперь использовать форматированные шаблоны писем.

- Замена plain text в “Email body” в действии “Email”



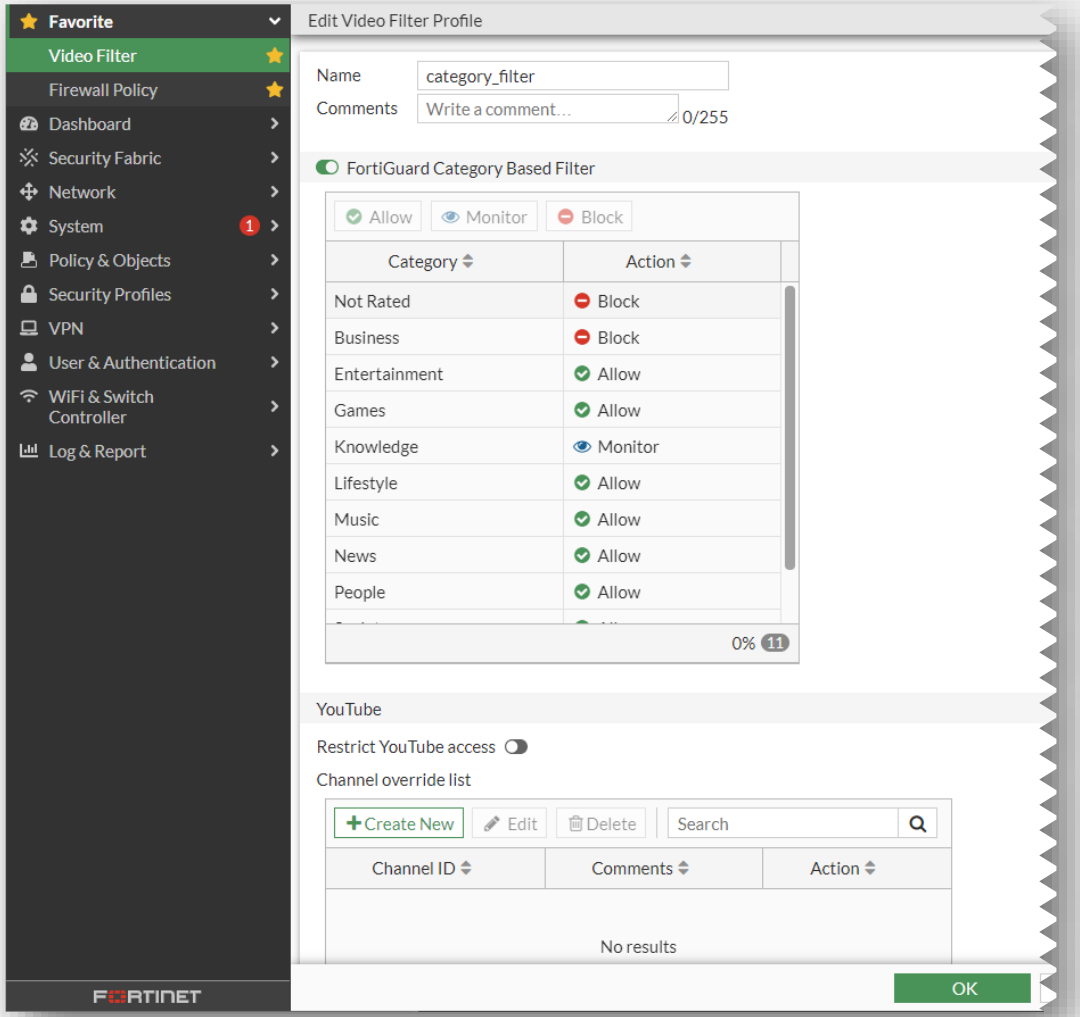
Новые сервисы FortiGuard для FortiOS 7.0

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
- Для работы необходима подписка Web & Video Filtering (ранее Web Filtering)



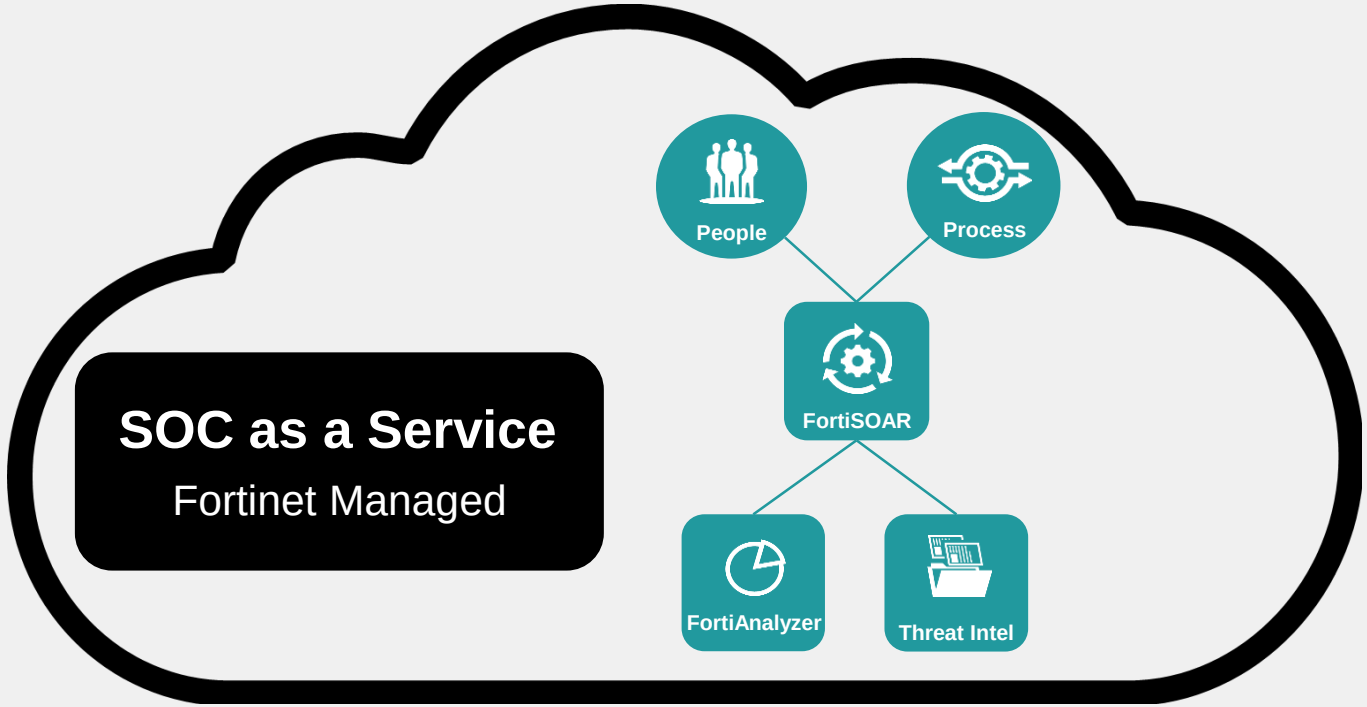
Новые сервисы FortiCloud для FortiOS 7.0 (FortiCloud SOCaaS)

Собственный SOC и управляемый SOC (Fortinet)

На основе программного стека Fortinet AI-Driven Security Operations Technology Stack

- Технологии Fortinet SOC уже присутствуют в пользовательском SOC

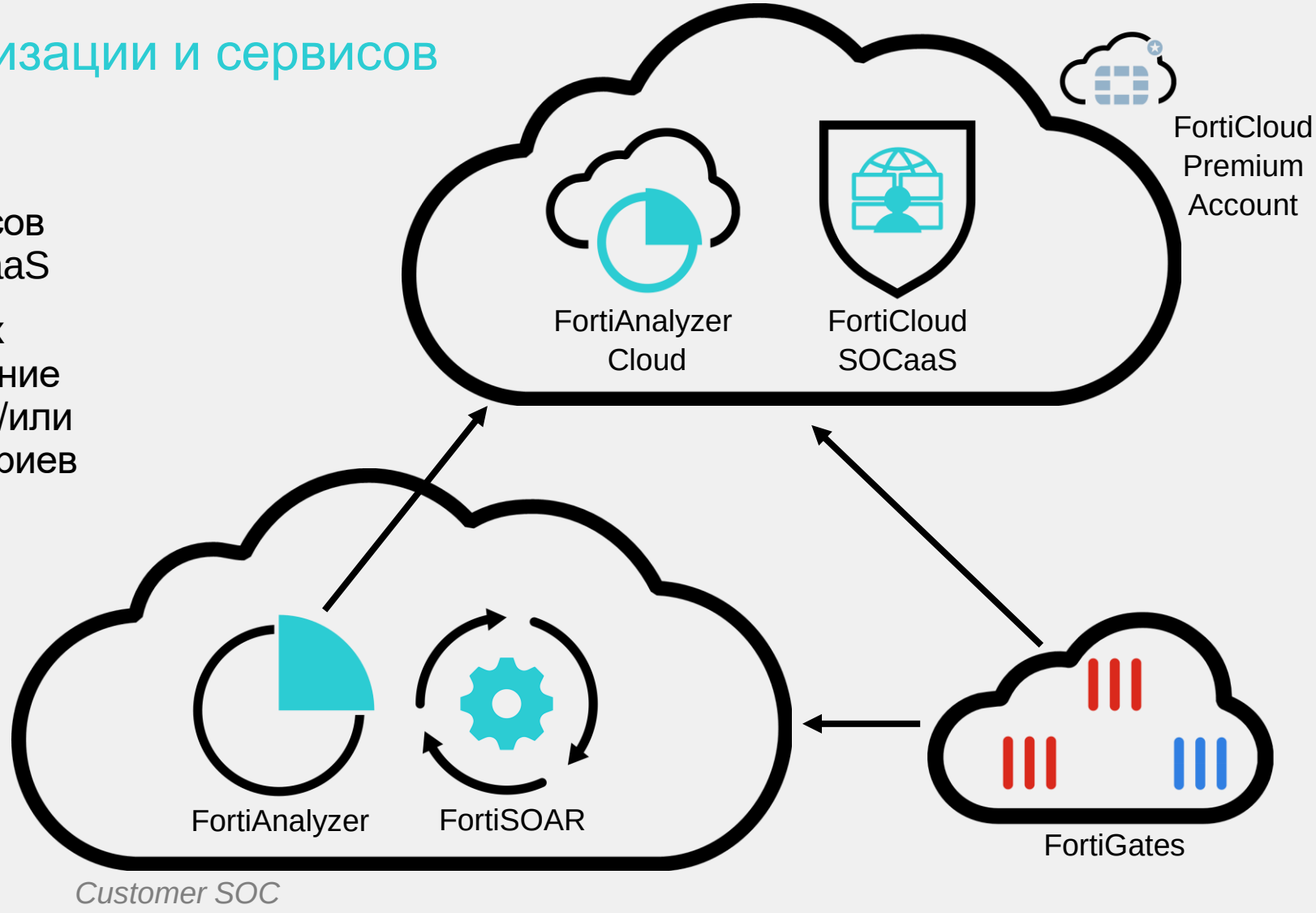
- SOCaaS построен на тех же технологиях Fortinet SOC и предоставляется по сервисной модели потребления



Расширение возможностей пользовательского SOC

Использование автоматизации и сервисов

- Расширение покрытия путем перенаправления обычных кейсов использования на Fortinet SOCaaS
- Использование подготовленных ресурсов Fortinet и сосредоточение усилий на более продвинутых и/или бизнес ориентированных сценариев
- Варианты развертывания
  - Напрямую с FortiGate в FAZ Cloud
  - Перенаправление журналов с пользовательского FortiAnalyzer

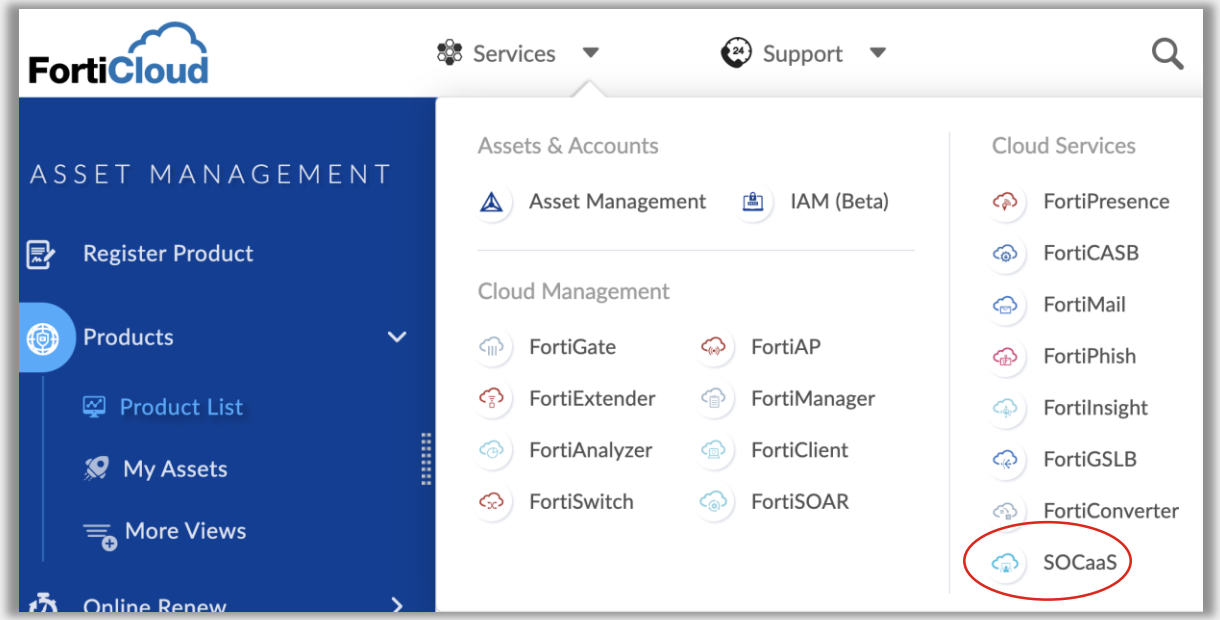


FortiCloud SOC-as-a-Service

Автоматизированные услуги SOC

Аналитики облачного управляемого сервиса Fortinet SOC отслеживают пользовательскую сеть на предмет событий безопасности и эскалируют в заказчика инциденты связанные обнаруженными угрозами

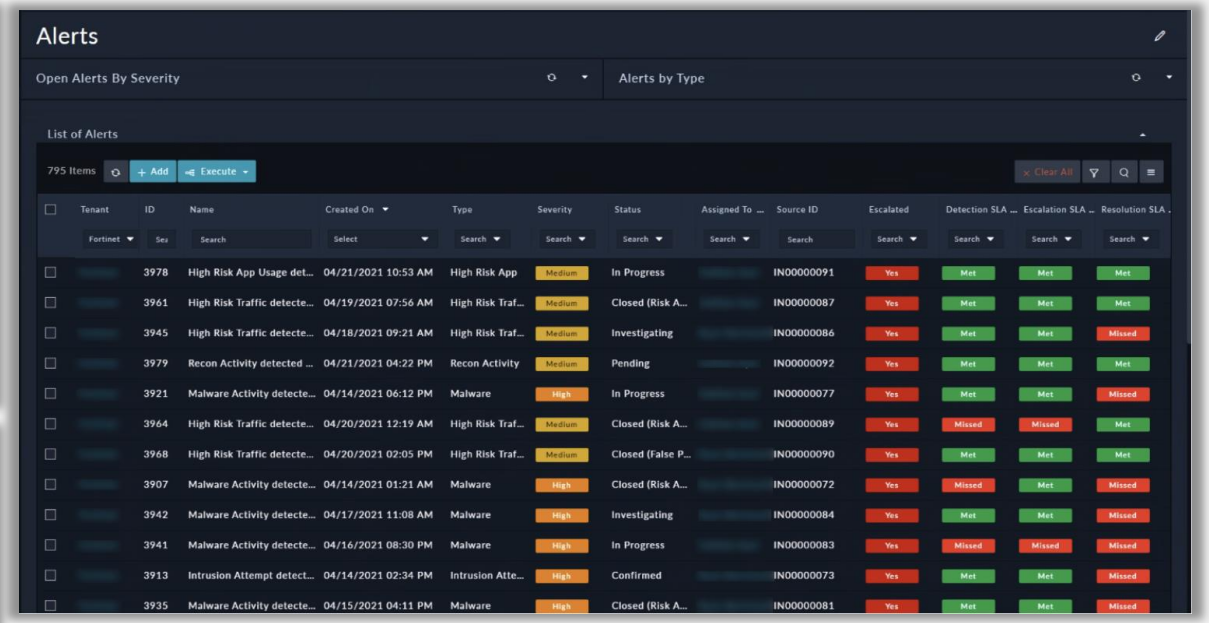
1. **Мониторинг и обнаружение (24x7x365)**
   - Нарушение политик, проникновение вредоносного ПО и попытки эксплуатации уязвимостей
   - Мониторинг C&C и ботнетов
   - Обнаружение следов сбора данных и горизонтальное распространения и т..д
2. **Расследование и анализ**
   - Автоматизация корреляции, анализа, обогащение контекста
   - Приоретизация тревожных сообщений, анализ инцидентов, проверка группой экспертов аналитиков
   - Экскалация инцидентов в пользователя с помощью телефона и электронной почты
3. **Изоляция и реагирование**
   - Удаленная поддержка в процессе верификации инцидента
   - Рекомендации для подавления угрозы и изоляции
4. **Отчетность**
   - Еженедельные отчеты о тревогах и система заявок SOCaaS Portal
   - Ежемесячный сводный отчет об инвентаризации активов
   - Ежеквартальный обзор сервиса
5. **Доступ через портал SOCaaS Portal**
   - Просмотр информации о тревогах и инцидентах
   - Загрузка отчетов
   - Запросы на сервисное обслуживание

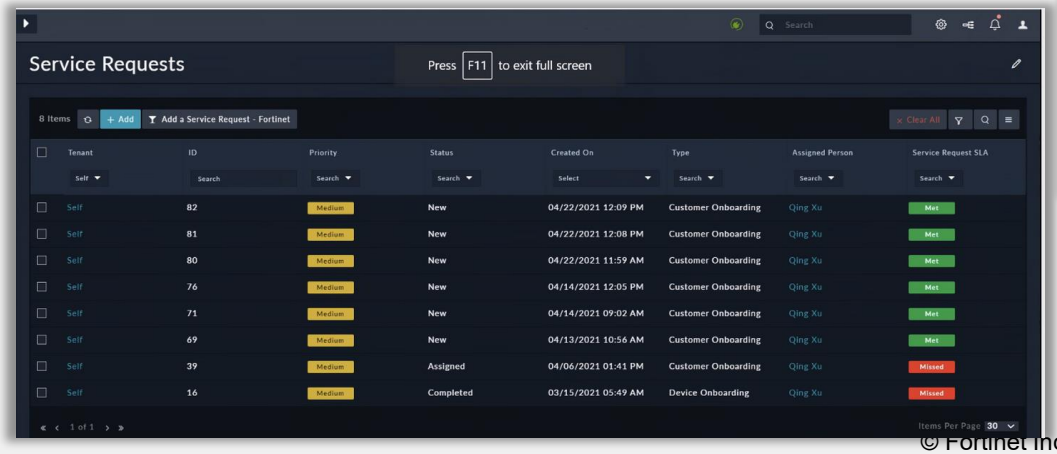


FortiCloud SOC-as-a-Service

FortiCloud SOCaaS Portal

Обеспечивает полную видимость в сервисе – позволяет пользователю отслеживать эскалированные тревожные события SOC, видеть детальную информацию об обнаруженной угрозе и отправлять новые заявки на сервисное обслуживание



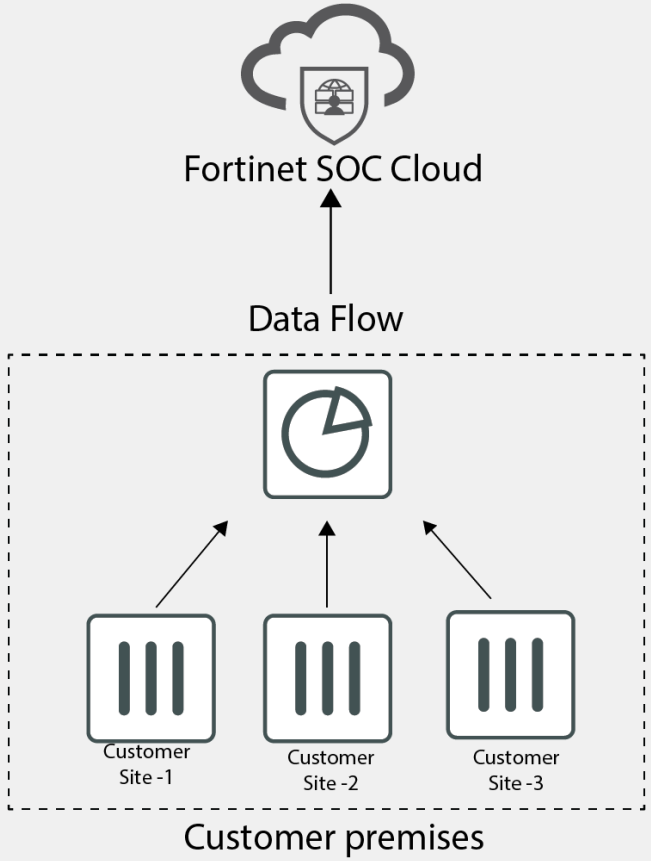


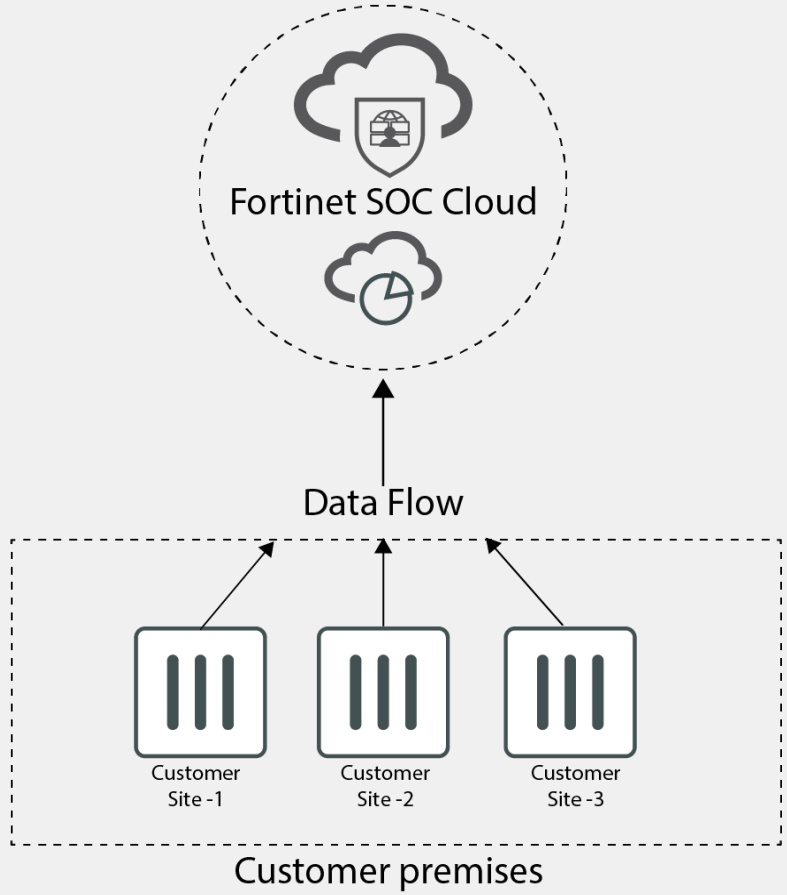
FortiCloud SOC-as-a-Service

Как начать использовать ?

Отправляйте журналы FortiGate в SOCaaS с помощью On-premise FortiAnalyzer или FortiAnalyzer-cloud

1. Необходима подписка FortiCloud Premium
2. Необходима подписка на каждый FG
   - Варианты:
     - В составе 360 Bundle
     - Отдельно (FortiCloud SOCaaS)
3. Откройте заявке в технической поддержке FortiCare для подключения сервиса
   - Форма для подключения
   - Матрица эскалации
4. Отправляйте журналы FG в SOCaaS, варианты:
   - Из **On-prem** FAZ в SOCaaS
   - Из FAZ-**Cloud** в SOCaaS





Лицензирование

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 7.0 3. IPAM service EoO

Bundles	Advanced Threat Protection	Unified Threat Protection	Enterprise Protection	360
FortiManager Cloud				•
FortiAnalyzer Cloud				•
FortiCloud SOCaaS NEW				•
SD-WAN Overlay Controller VPN Service				•
SD-WAN Cloud Assisted Monitoring				•
SD-WAN Orchestrator Entitlement				•
FortiConverter Service			•	•
FortiGuard IoT Detection Service			•	•
FortiGuard Industrial Service			•	•
FortiGuard Security Rating Service			•	•
FortiGuard Anti-Spam Service		•	•	•
FortiGuard Web & Video[2] 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]


FORTINET