FORTINET SECURITY DAY VIRTUAL

Организация Удаленной Работы Непридуманные Истории

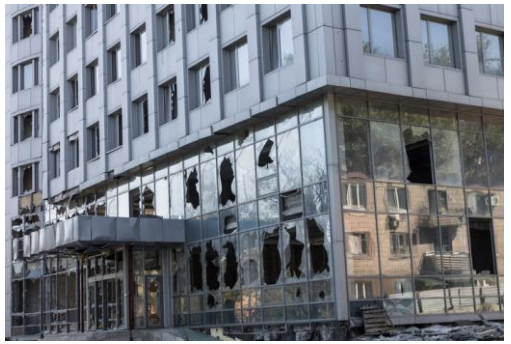
Елжан Насипов

SE Fortinet

Растущая потребность в решениях для организации удаленной работы

Кризис может принимать разные формы:

- природные катаклизмы
- глобальные пандемии
- теракты



Всё это происходит неожиданно и требует быстрой реакции

- План непрерывности бизнеса – восстановление при катастрофическом событии
- Работа сотрудников вне привычных рабочих мест
- Актуально для всех видов организаций

FORTINET

Введение чрезвычайного положения в Республике Казахстан

Дата: 15 марта 2020
Время: 18:00

Задача: Организация защищённого удалённого доступа
Кол-во сотрудников: 40 000
Инфраструктура: AD сервер, серверные ресурсы
Время на исполнение: 13 часов
Количество ресурсов доступных через VPN: много ☺

Компоненты решения: 2xFortigate-VM32, FortiAuthenticator, FortiClient VPN, Fortitoken Mobile
Затрачено времени: 10 часов(с учётом ожидания лицензий)
Кол-во задействованных сотрудников Fortinet: 2

РЕСПУБЛИКА КАЗАХСТАН

ОФИЦИАЛЬНЫЕ ДОКУМЕНТЫ

ИНИСТРАЦИ ЗИДЕНТА

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

15 марта 2020

О введении чрезвычайного положения в Республике Казахстан

В целях обеспечения безопасности населения Республики Казахстан в соответствии с подпунктом 16) статьи 44 Конституции Республики Казахстан и статьями 4, 5, 6 Закона Республики Казахстан «О чрезвычайном положении» **ПОСТАНОВЛЯЮ:**

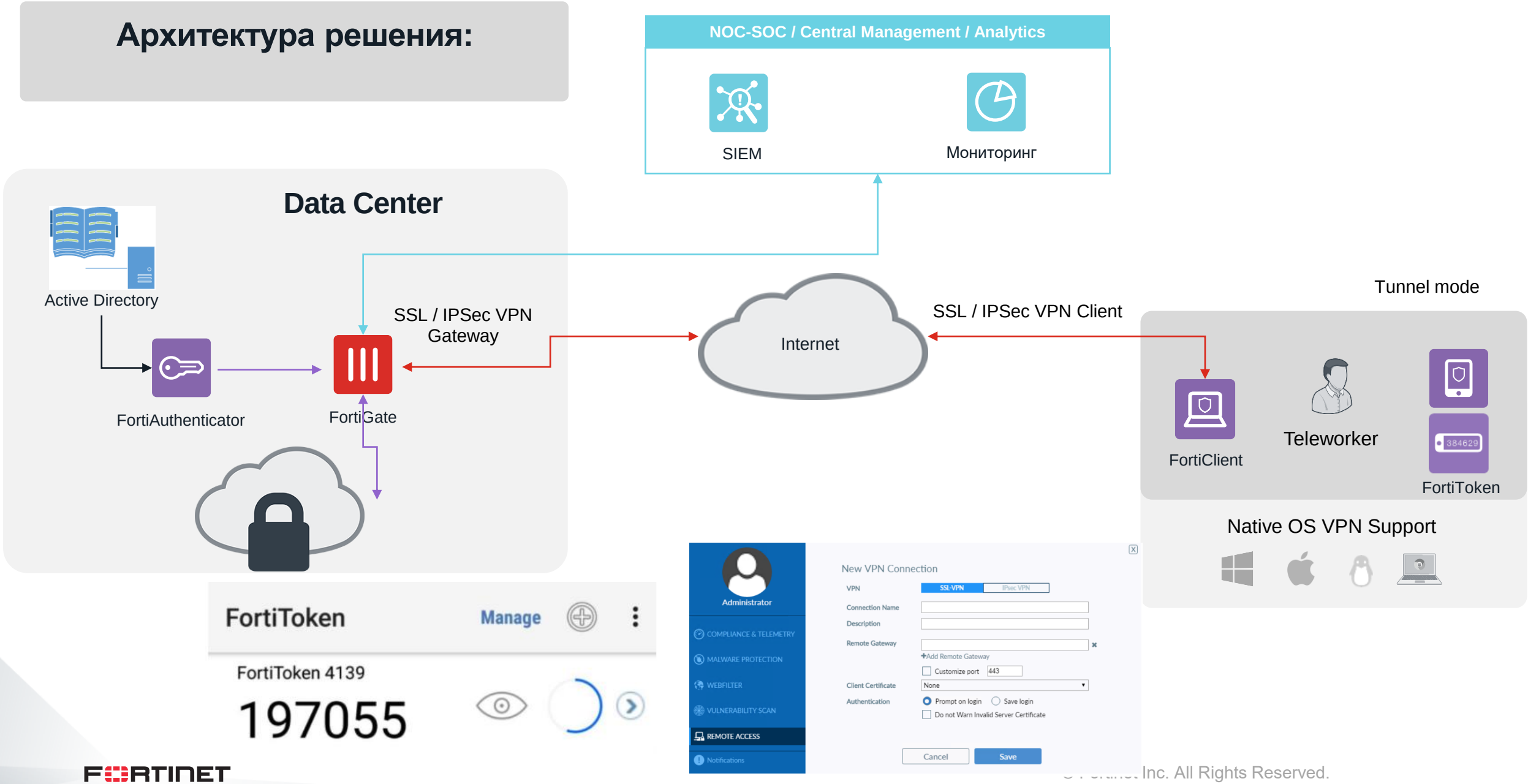
1. В связи с объявлением Всемирной организацией здравоохранения нового коронавируса COVID-19 пандемией в целях защиты жизни и здоровья граждан ввести в соответствии с законодательством Республики Казахстан на всей территории Республики Казахстан чрезвычайное положение на период с 08 часов 00 минут 16 марта 2020 года на срок до 07 часов 00 минут 15 апреля 2020 года.

2. Создать на период чрезвычайного положения Государственную комиссию по обеспечению режима чрезвычайного положения при Президенте Республики Казахстан и наделить ее полномочиями, предусмотренными Законом Республики Казахстан «О чрезвычайном положении», в составе согласно приложению к настоящему Указу.

3. Ввести на период действия чрезвычайного положения следующие меры и временные ограничения:

1) усилить охрану общественного порядка, охрану особо важных государственных и стратегических, особорежимных, режимных и особо охраняемых объектов, а также объектов, обеспечивающих жизнедеятельность населения и функционирование транспорта;

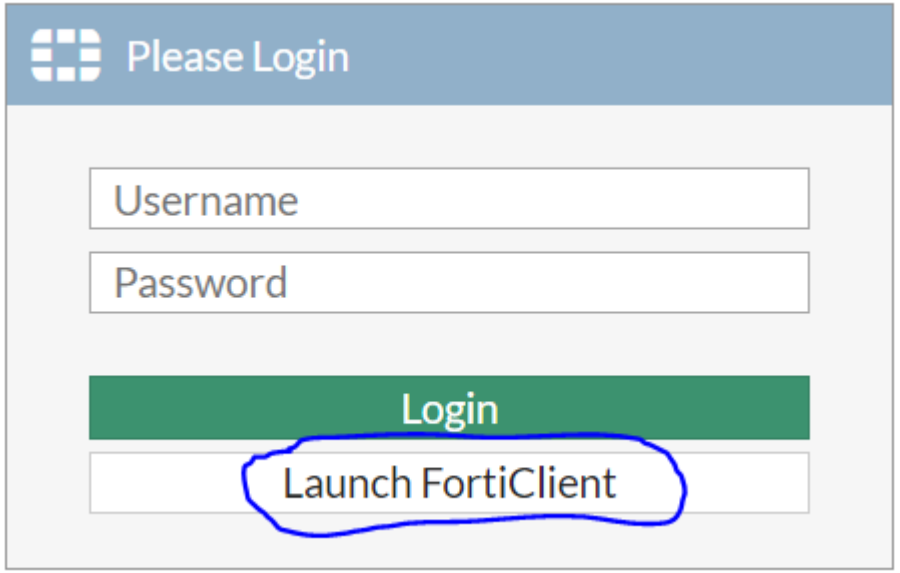
Архитектура решения:



Компоненты решения - FG-VM32

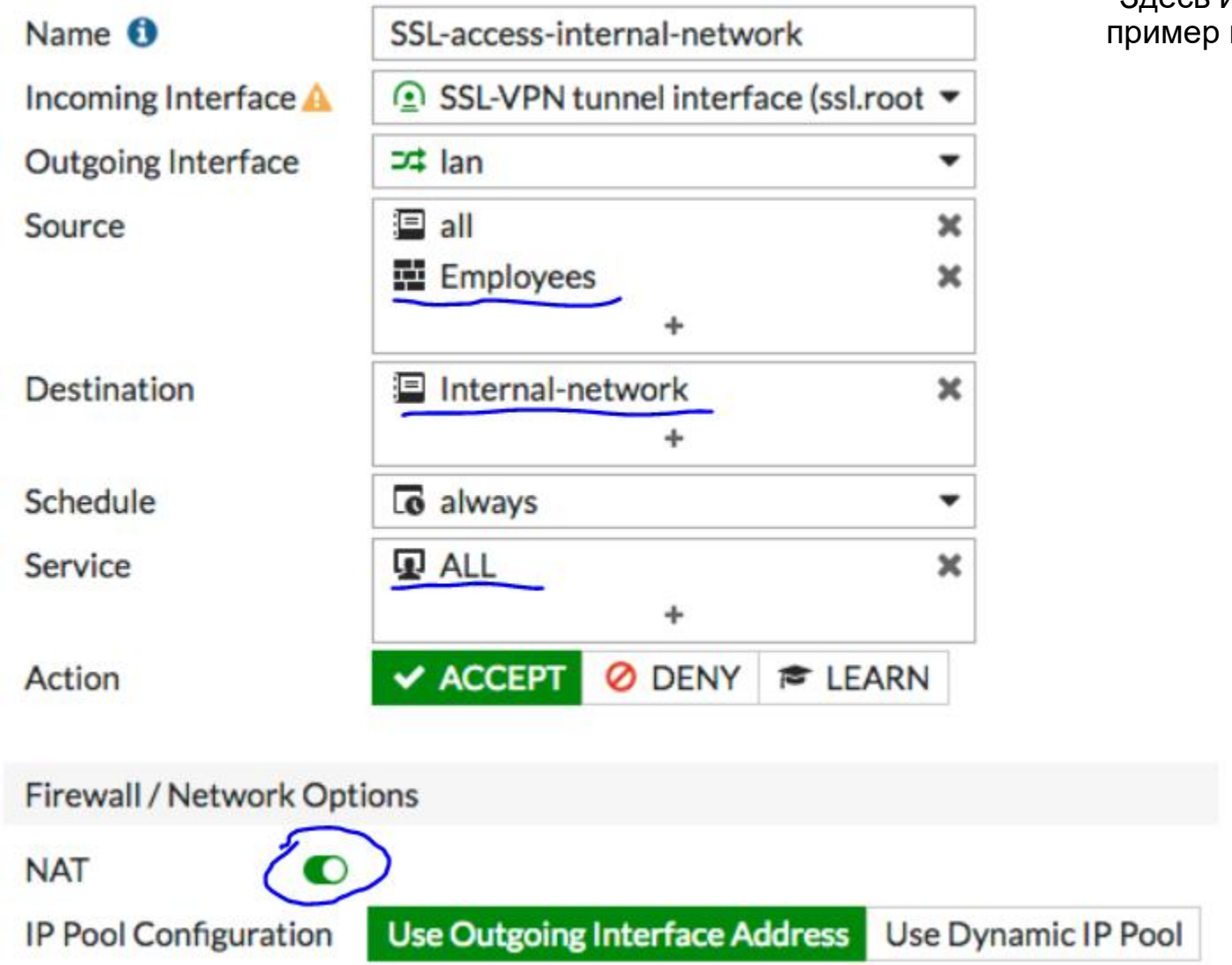
	FORTIGATE-VM32/32V/32S
Technical Specifications	
vCPU Support (Minimum / Maximum)	1 / 32
Memory Support (Minimum)	2 GB
Network Interface Support (Minimum / Maximum) [1]	1 / 24
Storage Support (Minimum / Maximum)	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	1,024 / 4,096
Virtual Domains (Default / Maximum) [2]	10 / 500
Firewall Policies	200,000
Maximum Number of Registered Endpoints	20,000
Unlimited User License	Yes
System Performance	**Non-DPDK+vNP Offloading**
Firewall Throughput (UDP Packets)	50.0 Gbps
New Sessions / Second (TCP)	
IPsec VPN Throughput (AES256+SHA1, 512 Byte)	7.0 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	
Client-to-Gateway IPsec VPN Tunnels	
SSL-VPN Throughput	8.6 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	
IPS Throughput [3]	19.0 Gbps
IPS HTTP 1M	29.0 Gbps
Application Control Throughput [4]	17.5 Gbps
NGFW Throughput [5]	16.5 Gbps
Threat Protection Throughput [6]	13.0 GBps

VPN Portal

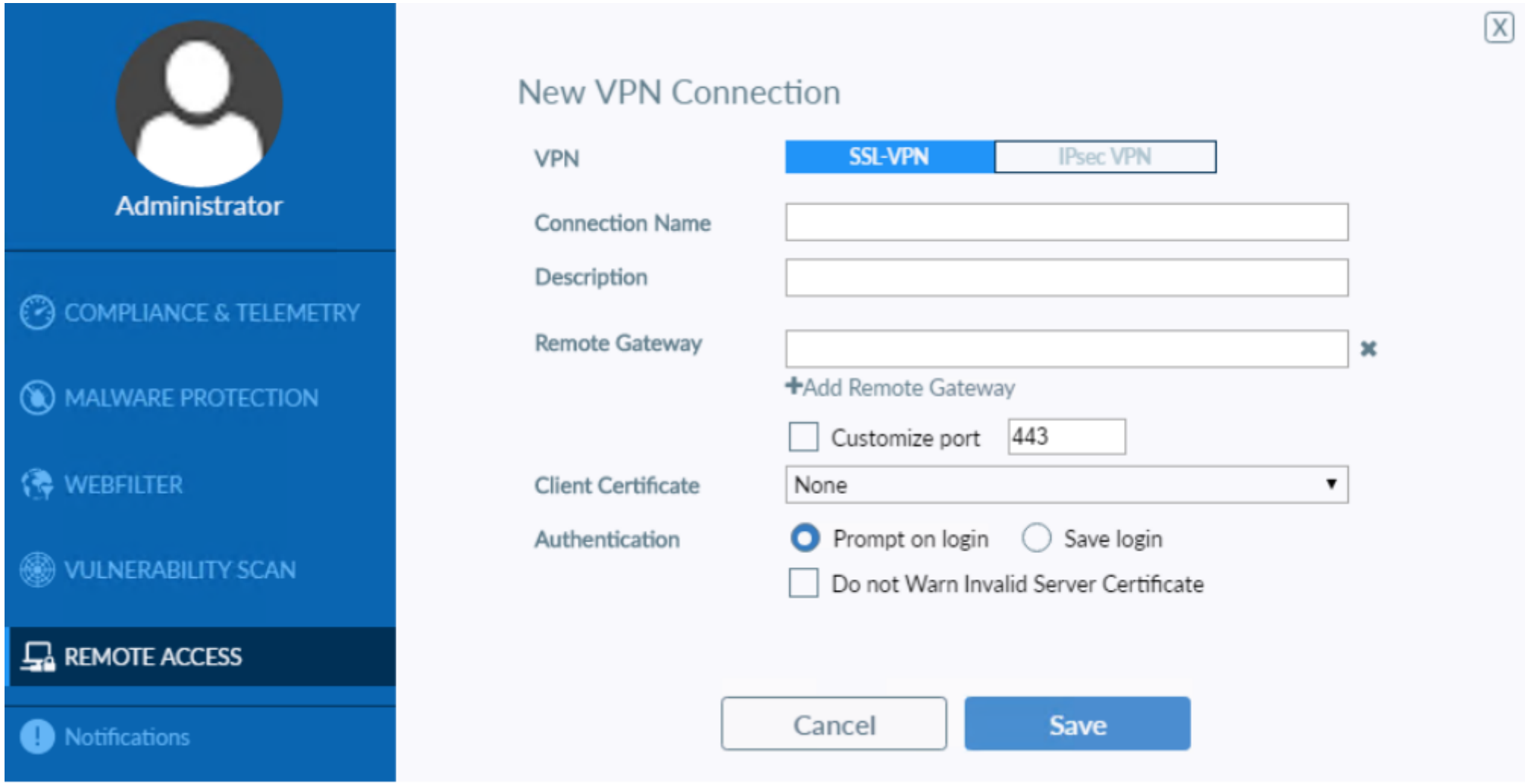


(прод.) Политики доступа

*Здесь и далее используется пример конфигурации



Компоненты решения – Forticlient VPN (бесплатный)



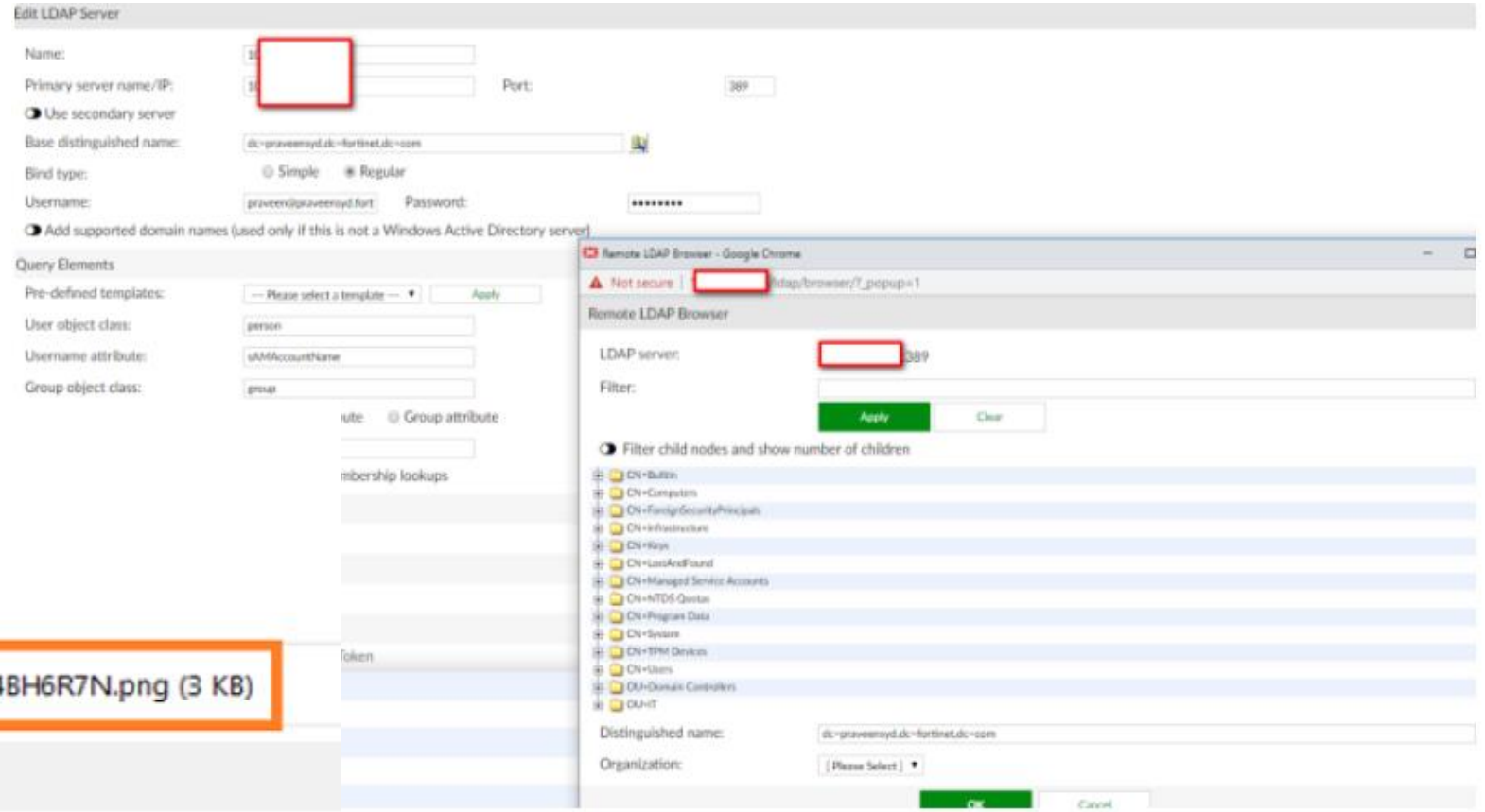
Онлайн инсталляторы: https://forticlient.com/downloads
Оффлайн инсталляторы: https://support.fortinet.com/

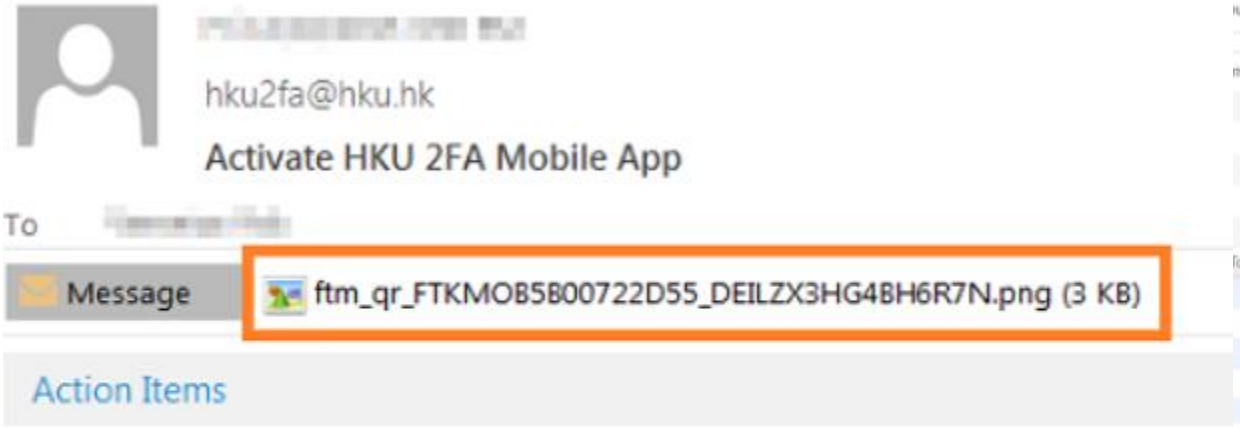
Компоненты решения – Fortiauthenticator VM

+ Интеграция с AD сервером

+ Возможность использования объектов Active Directory непосредственно в политике

+ Доставка кода активации токена





Dear colleague,

Thank you for registering to use HKU Two-Factor Authentication (2FA)

Компоненты решения – FortiToken Mobile

+ Поддерживается технология Push notification

+ Дополнительная защита приложения с помощью PIN кода с поддержкой Touch ID и Face ID

+ 6 или 8 символов в качестве OTP, с обновлением каждые 30 или 60 сек

+ Поддержка активации через QR Code

ANDROID APP ON Google play

Download on the App Store

Download from Windows Store

+ Android

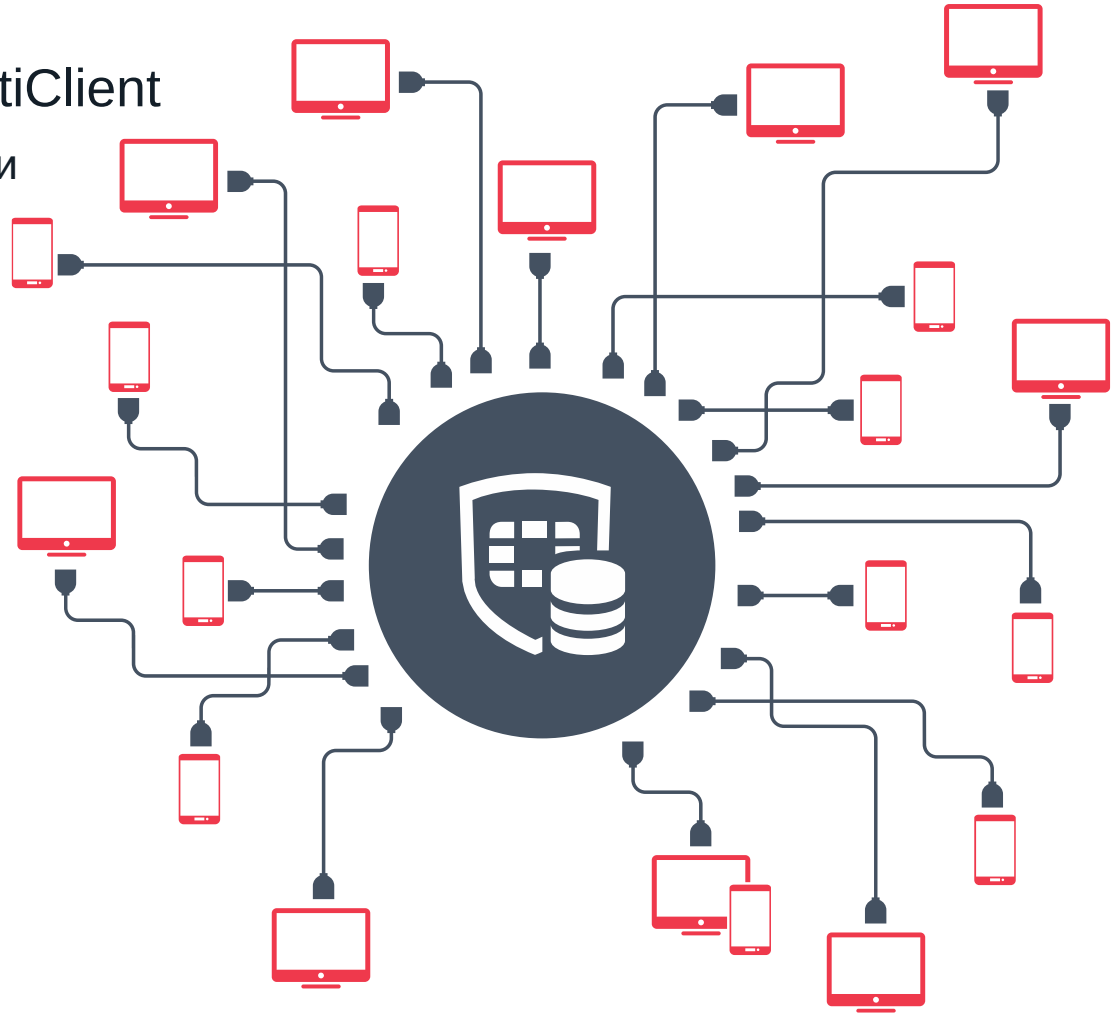
+ iOS

+ Windows mobile

Что можно было улучшить?

Enterprise Management System (EMS)

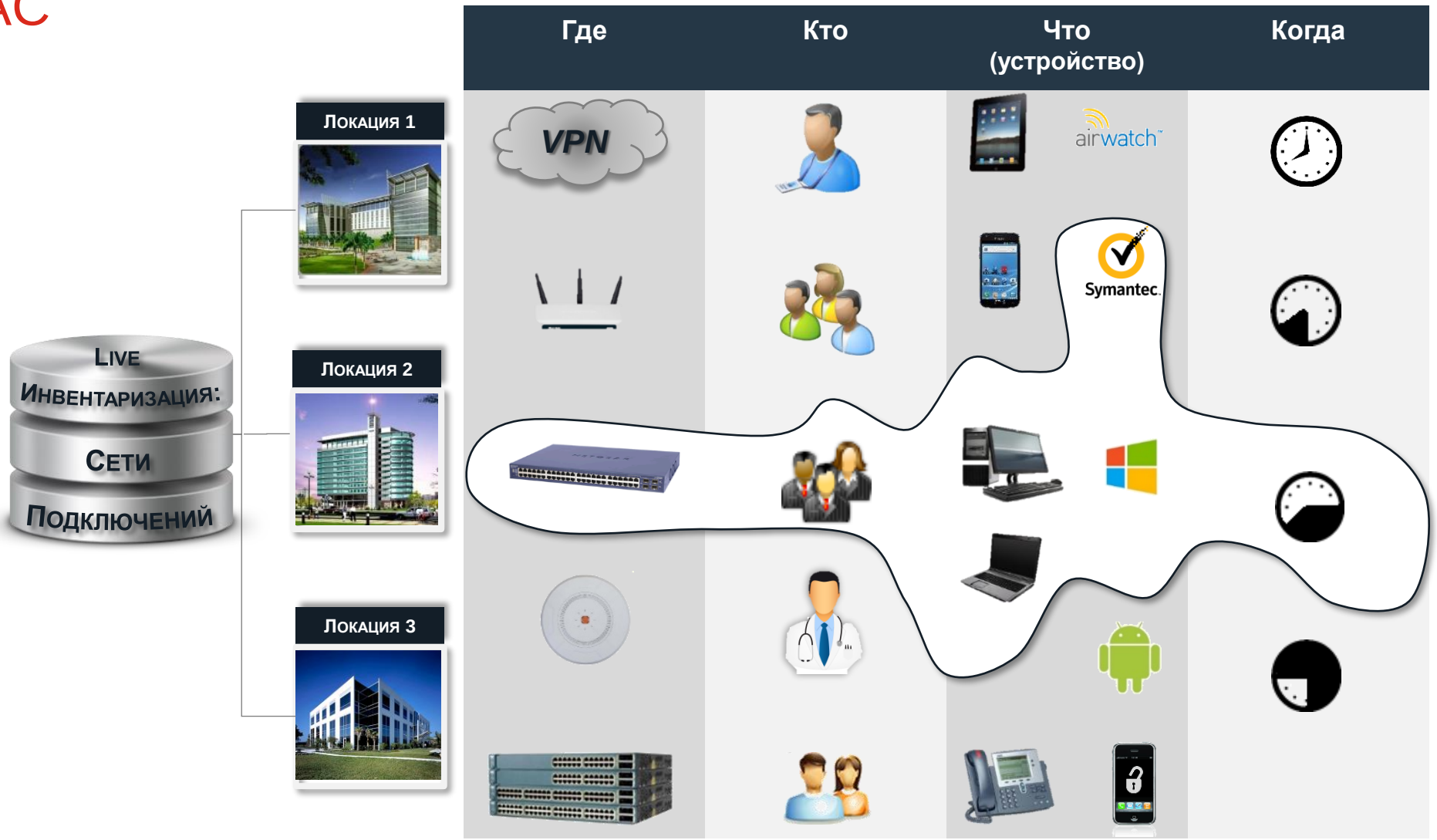
- Подготовка и развертывание дистрибутивов FortiClient
  - Интеграция с AD и другими корпоративными системами
- Оценка соответствия политикам безопасности
- Мониторинг клиентов в реальном времени
- Сводка по угрозам, оповещения
- Управление клиентами, в т.ч.
  - Сканирование на ВПО
  - Сканирование на уязвимости
  - Помещение в карантин
- Инвентаризация ПО
- Масштабируемое решение



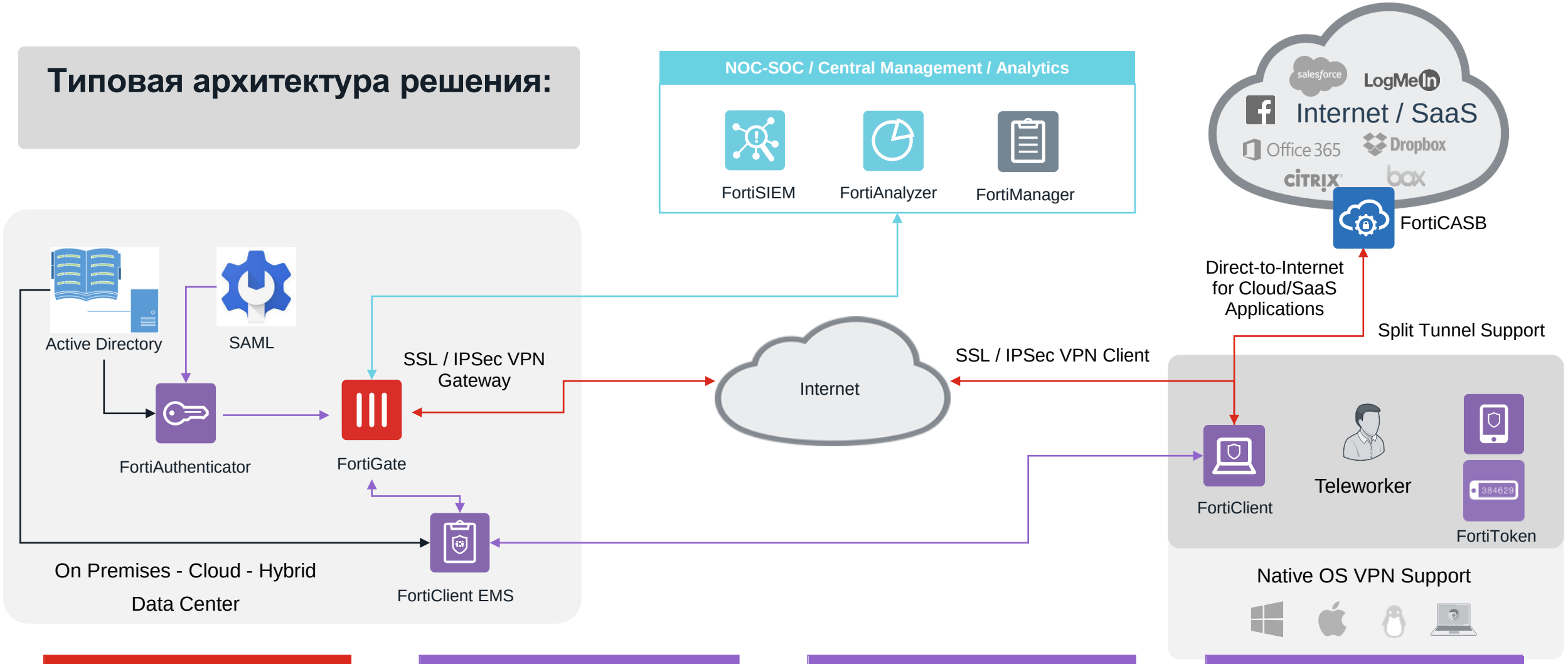
FORTINET

(прод.) Что можно было улучшить?

FortiNAC



Типовая архитектура решения:



FortiGate VPN Gateway

- VPN Services
- Enforcement / Admission control
- NGFW
- Fabric Connectors
- Dynamic policy

FortiAuthenticator

- Authentication Management
- LDAP / Radius / SAML Integration
- MFA / Token Management
- Certificate Authority

Endpoint Management Server (EMS)

- VPN Client configuration
- Endpoint policy / profile management
- Fabric Connector
- FortiClient Deployment

FortiClient

- Endpoint telemetry
- Vulnerability management
- Malware prevention
- Web filtering/Application Firewall
- VPN / MFA Support

https://docs.fortinet.com/teleworking

2020 Fortinet Security Fabric

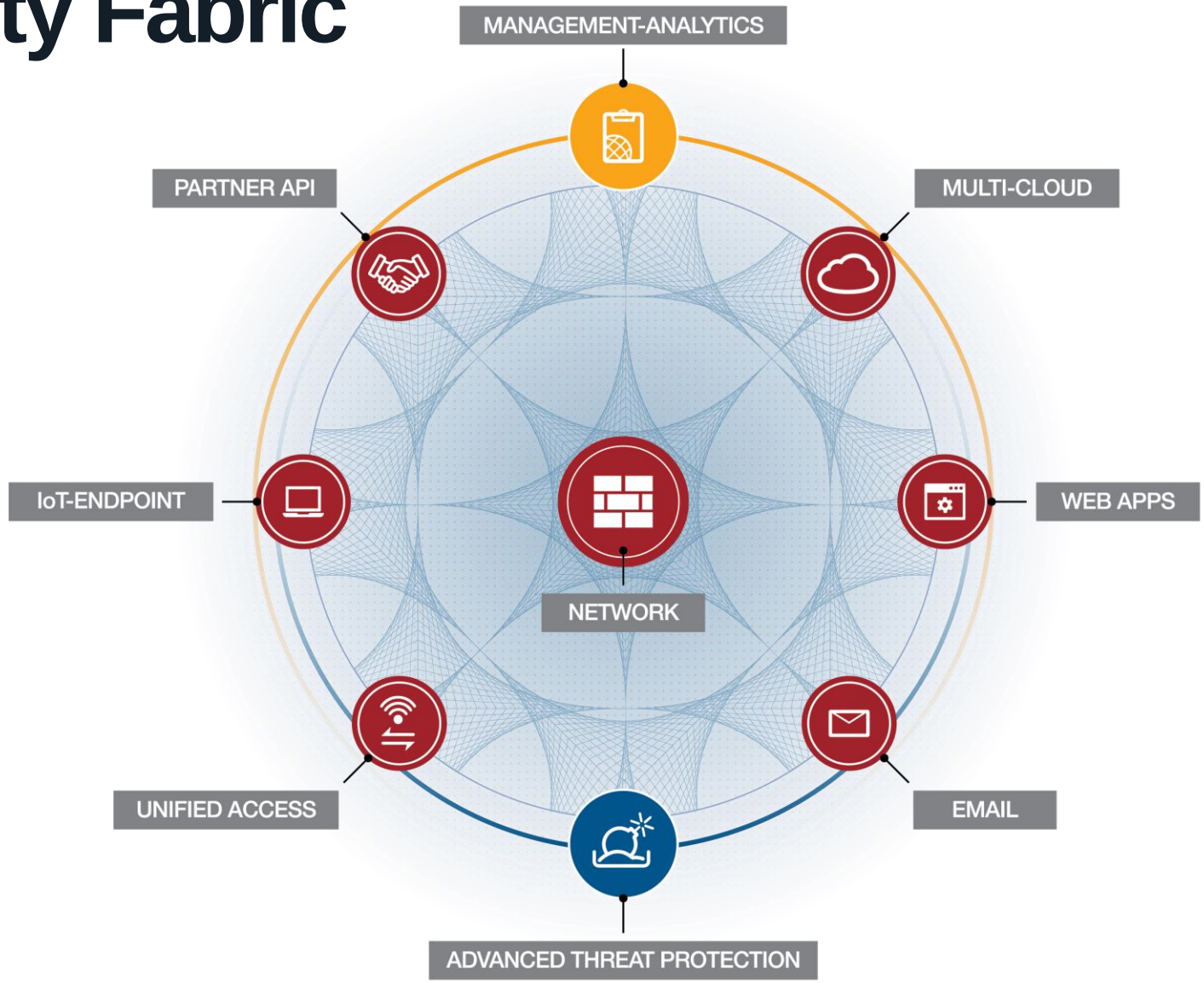
Архитектура безопасности, которая обеспечивает:

ОСВЕДОМЛЕННОСТЬ
Прозрачность и защита цифровых поверхностей атаки

ИНТЕГРАЦИЯ
Обнаружение продвинутых угроз

АВТОМАТИЗАЦИЯ
Противодействие и проверка активов

Доступны в виде:



FORTINET

KZ@fortinet.com