КРОК

Выбор NGFW: функционал, кейсы, лайфхаки

2020

Общие тенденции

Рост количества
удаленных сотрудников

Удаленный доступ
к критическим сервисам

Миграция ресурсов
в Облака

Увеличение объема
сетевого трафика

70%

сотрудников будут работать удаленно
не менее 5-ти дней в месяц к 2025 году

https://usefyi.com/remote-work-statistics

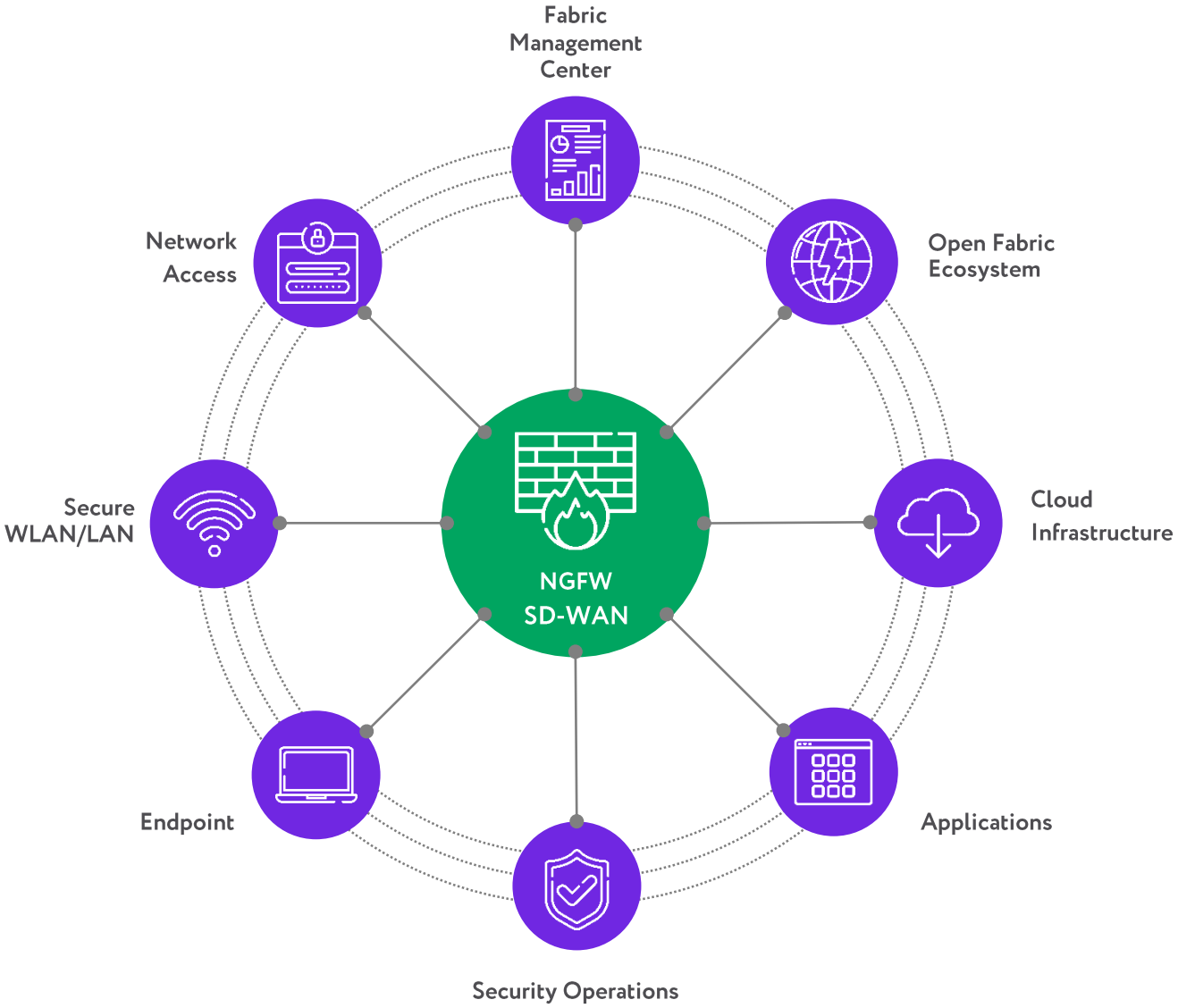
77%

крупных российских компаний готовы
перейти в облачные сервисы

https://www.gazeta.ru/tech/news/2019/11/28/n_13749068.shtml

Fortinet Security Fabric

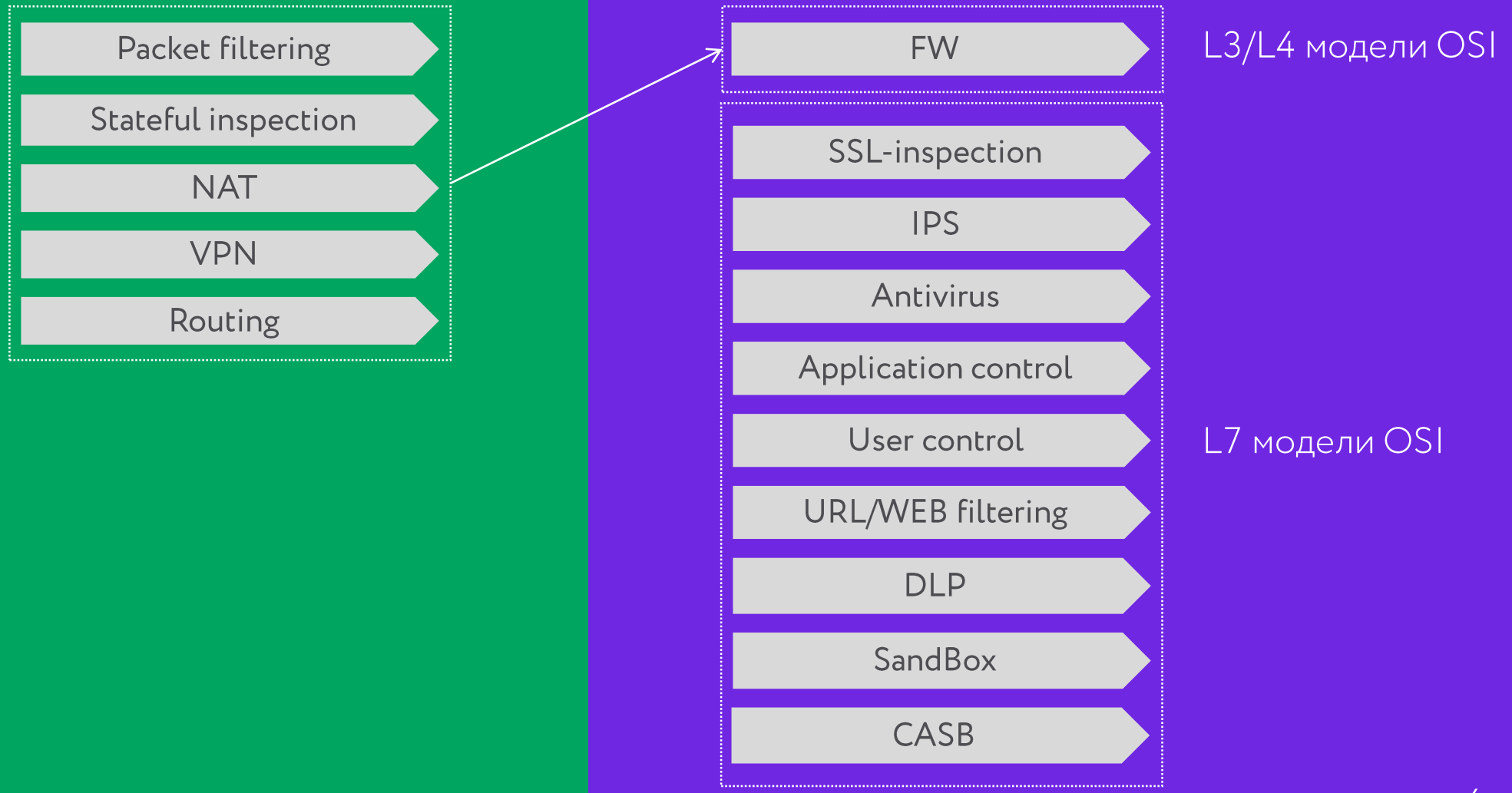
- Сети, ориентированные на безопасность
- Сетевой доступ с нулевым доверием
- Динамическая безопасность облака
- Использование искусственного интеллекта



К 2025 году рынок NGFW вырастет на 79%

https://www.globenewswire.com/news-release/2020/04/21/2019553/0/en

FW vs NGFW


Packet filtering
Stateful inspection
NAT
VPN
Routing
FW
SSL-inspection
IPS
Antivirus
Application control
User control
URL/WEB filtering
DLP
SandBox
CASB
L3/L4 модели OSI
L7 модели OSI

Наши кейсы

Кейс №1

Увеличение объема трафика

Проблема

Производительности существующих межсетевых экранов недостаточно

Старое решение

- Отключение «прожорливых» функций безопасности
- Ограничение Интернета для сотрудников

Риски и угрозы

- Риск заражения и взлома
- Снижение производительности труда

Кейс №1

Увеличение объема трафика

Наше решение

Заменить межсетевой экран
на современный производительный
FortiGate

Лайфхак №1

**Закладывать запас
по производительности
на 30-50%**

Лайфхак №2

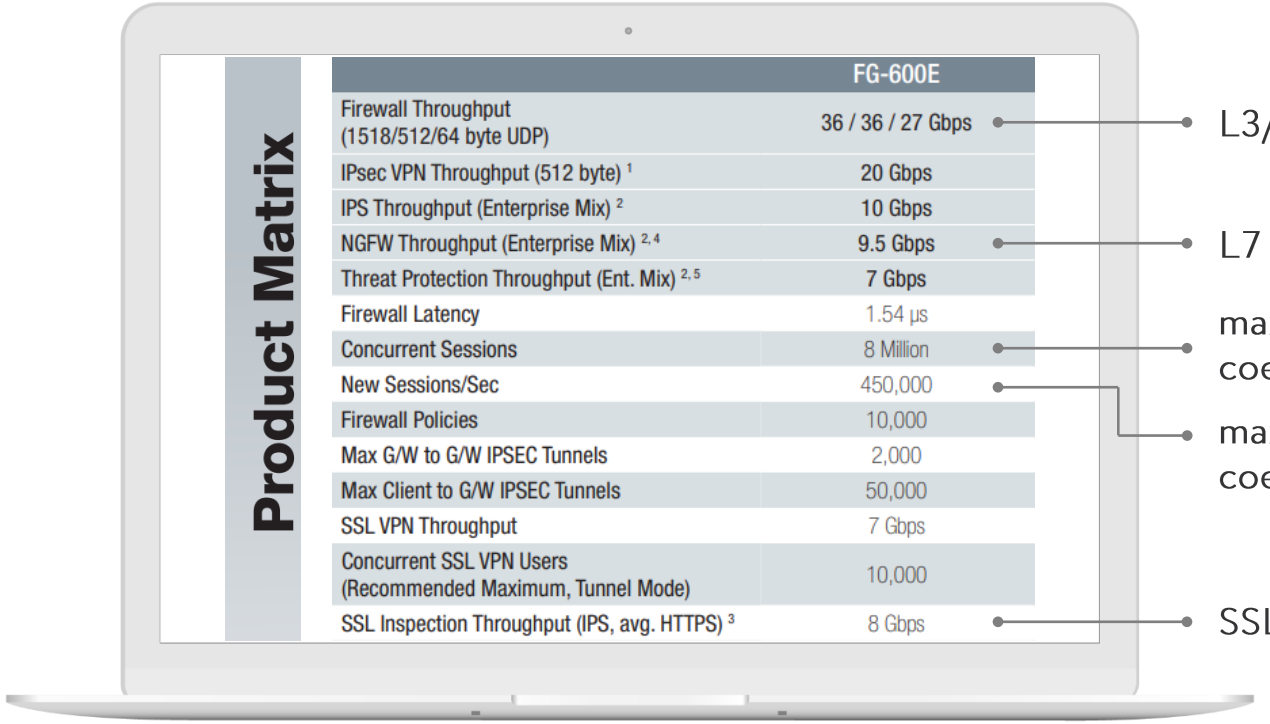
**Не забывать про уменьшение
пропускной способности
при наращивании функционала**

Кейс №1

Увеличение объема трафика

Наше решение

Заменить межсетевой экран на современный производительный FortiGate



L3/L4 модели OSI

L7 модели OSI

max количество одновременных соединений

max количество новых соединений в секунду

SSL-инспекция

Кейс №2

Безопасный удаленный доступ

Проблема

- Устройства удаленных сотрудников не проверяются
- Не проводится комплаенс устройств при подключении в сеть компании

Риски и угрозы

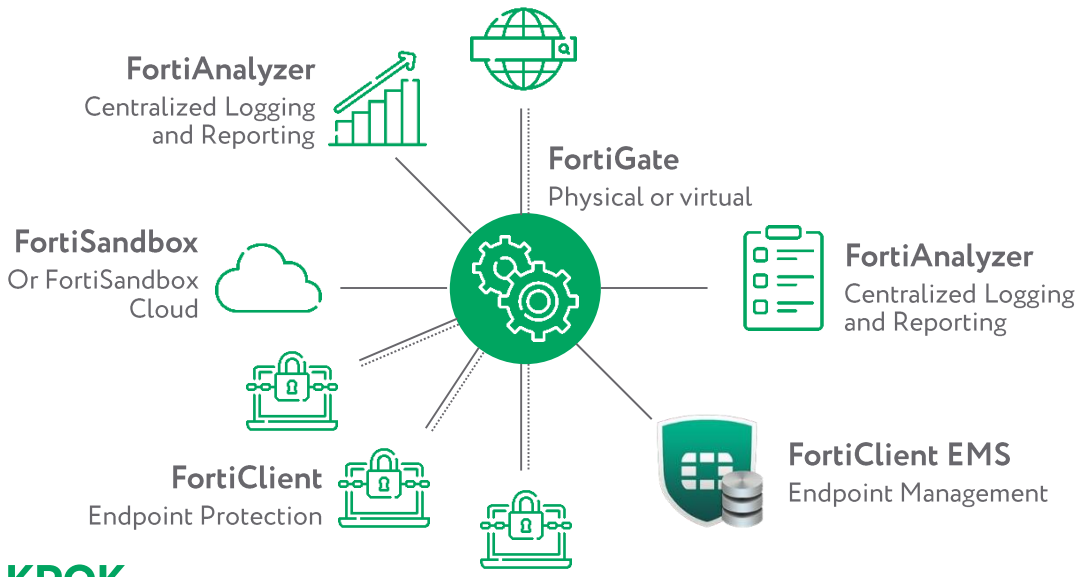
- Заражение ресурсов компании вирусами
- Получение несанкционированного доступа к ресурсам компании

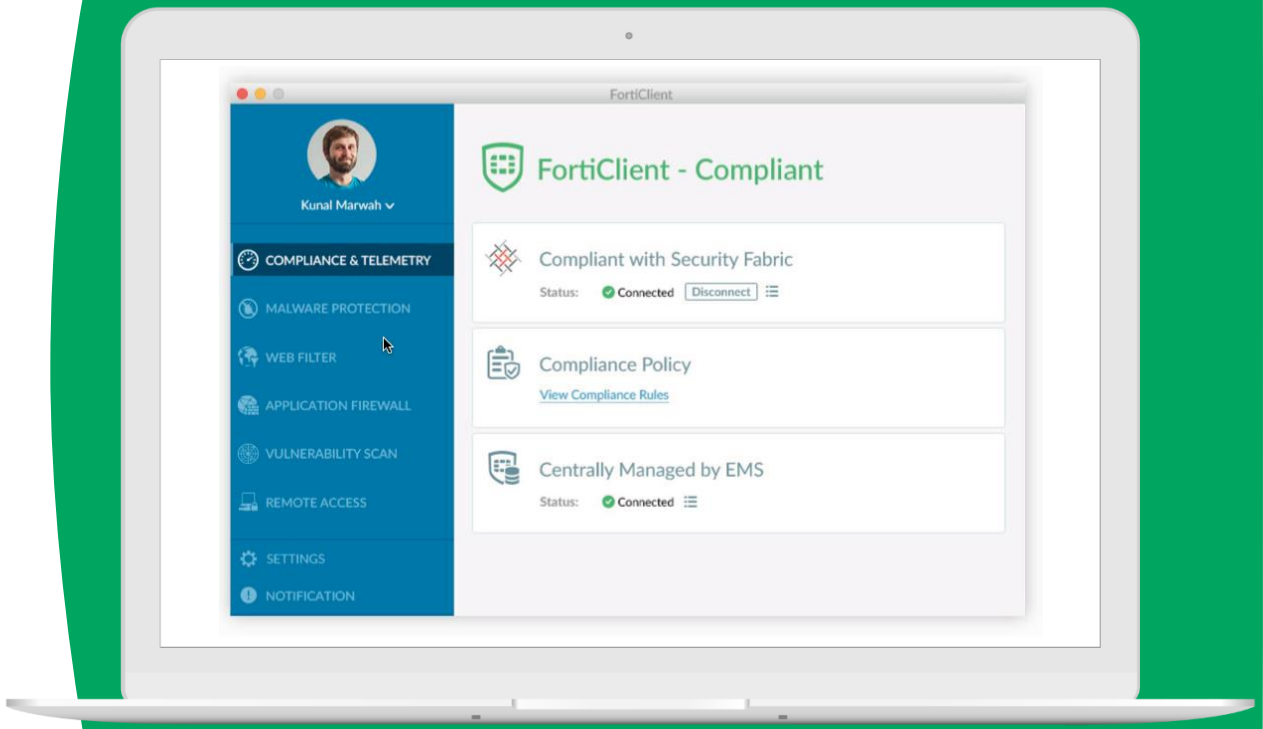
Кейс №2

Безопасный удаленный доступ

Наше решение

Заменить межсетевой экран на связку FortiGate + FortiSandbox + EMS + FortiClient





КРОК

Кейс №3

Контроль доступа в Интернет

Проблема

- Пользователи используют «опасные» приложения (TeamViewer, AnyDesk, и др.)
- Пользователи используют рабочее время не для работы

Риски и угрозы

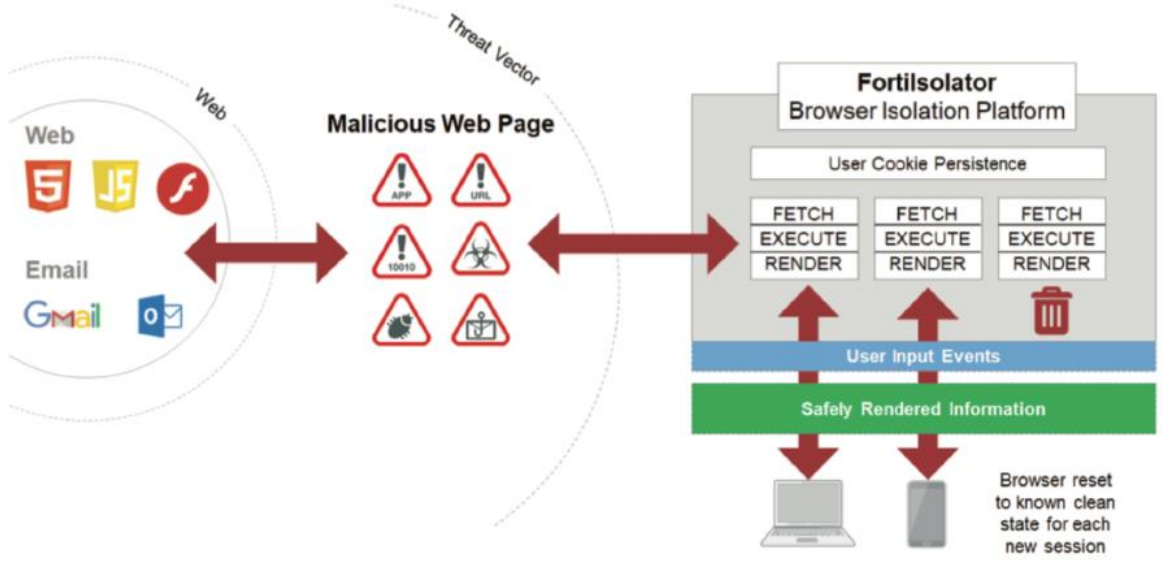
- Несанкционированное удаленное управление и утечка информации
- Снижение производительности труда

Кейс №3

Контроль доступа в Интернет

Наше решение

Заменить межсетевой экран на FortiGate с функциями Application Control, User Control, SSL-inspection, URL/WEB-filtering



Лайфхак №1

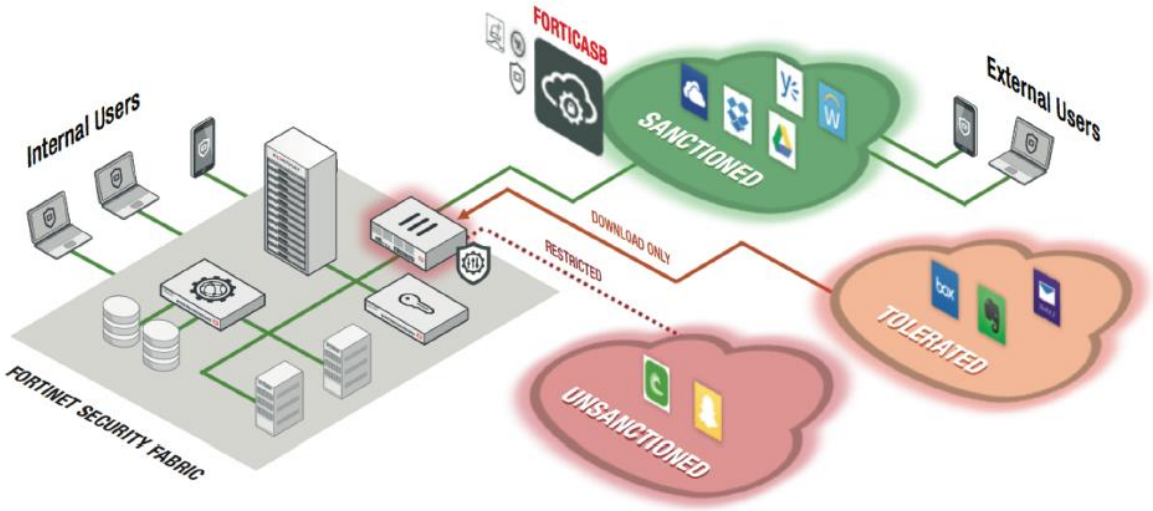
Для продвинутой защиты использовать платформу изоляции браузеров FortiIsolator

Кейс №3

Контроль доступа в Интернет

Наше решение

Заменить межсетевой экран на FortiGate с функциями Application Control, User Control, SSL-inspection, URL/WEB-filtering



Лайфхак №2

Для контроля Office 365 использовать сервис обеспечения безопасности облачных приложений FortiCASB

Кейс №4

Сайзинг виртуального устройства

Задача

Защитить корпоративные ресурсы в Облаке

Проблема

Нет возможности спрогнозировать трафик на переносимые в Облако ресурсы

Риски и угрозы

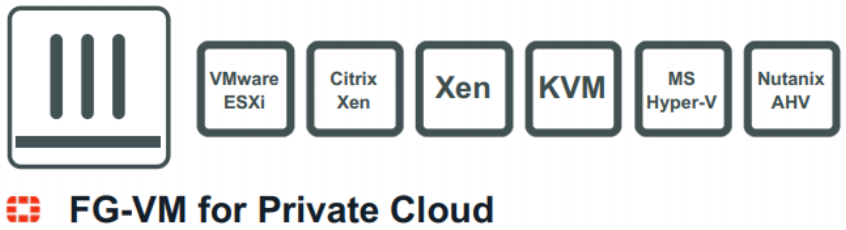
Невозможно правильно подобрать FotiGate-VM

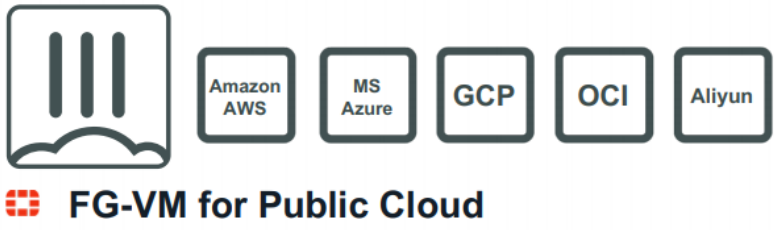
Кейс №4

Сайзинг виртуального устройства

Наше решение

Оценить сайзинг ВМ для FortiGate-VM
на пробных лицензиях





Запускаем FortiGate на пробных лицензиях

Понимаем необходимые характеристики

Переходим на боевые лицензии

Кейс №5

Сведения об угрозах в сети

Проблема

Нет сведений о типах и количестве угроз в сети

Старое решение

Самостоятельное разворачивание тестового устройства и анализ трафика

Риски и угрозы

Неполное представление о решении, возможностях и состоянии угроз в сети

Наше решение

Использовать программу СТАР для оценки киберугроз

Программа оценки киберугроз (CTAP)

Быстро и Бесплатно

Цель программы (CTAP) — предоставить организациям подробные сведения о типах и количестве киберугроз, которые могут проникнуть в корпоративные сети в обход существующих средств защиты

Основные этапы CTAP

Определение необходимой модели FortiGate	Установка FortiGate в сеть заказчика	Сбор информации о сетевых взаимодействиях и угрозах в течении недели	Отправка собранной информации для анализа в лабораторию Fortinet	Генерация отчета с подробной статистикой по трафику и наличие уязвимостей в сети	Совместный анализ полученных результатов
KPOK				KPOK + Fortinet	KPOK + Клиент

Стало интересно?
Получи помощь экспертов

https://promo.croc.ru/fortinet

Почему КРОК

01 Оптимальный подбор решений

02 Профессиональное внедрение

03 Техническая поддержка 24x7, 8x5

04 Бесплатное тестирование по программе СТАР

05 Услуги по модели MSSP в Облаке КРОК

КРОК

ИНТЕГРИРУЕМ
БУДУЩЕЕ

Юрий Гостюнин
Ведущий эксперт
направления сетевой
безопасности

+7 (495) 974-22-74
+7 (903) 347-73-70

ygostyunin@croc.ru