

Как защитить корпоративную сеть



Дмитрий Соколов

Head of Professional Services



Андрей Жуков

Security Consultant



Андрей Куртасанов

Security Consultant



Business
Services

FORTINET®

Orange Business Services:

глобальный партнер в цифровой трансформации бизнеса

Нашими клиентами являются
мультинациональные компании по всему
миру:

2 200+
в Европе

800+
в Америке

1 500+
В России

700+
в Азии

200+
в Африке и на Ближнем
Востоке



Мы не только глобальный лидер
в корпоративных телекоммуникационных
сервисах, но и:

- поставщик профессиональных сервисов
- интегратор
- крупный игрок в цифровых инновациях



21 000

сотрудников, занятых в
корпоративном бизнесе

800

из них в России



400 разработчиков приложений и 700
экспертов IoT и big data



170 инженеров и менеджеров проектов
в области инфраструктуры организации
рабочих мест и миграции в облако



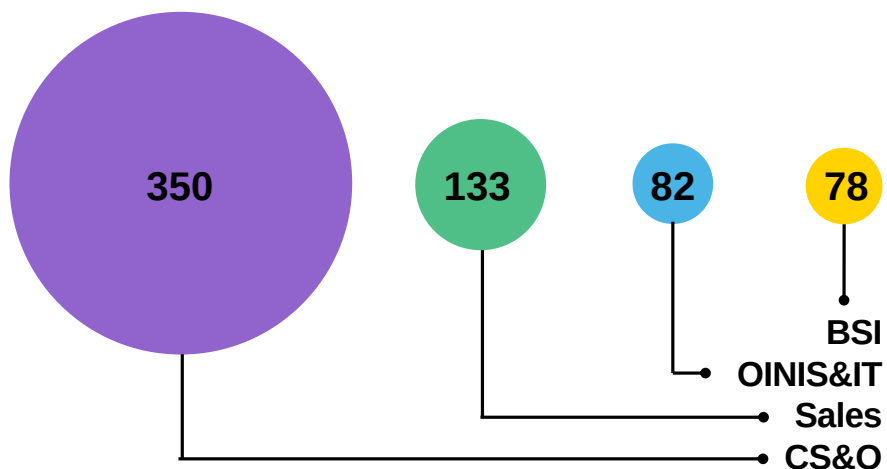
1 200
облачных
экспертов



1 000 экспертов
кибербезопасности

Orange в России

- B2B-подразделение группы Orange: провайдер цифровых сервисов с экспертизой в области телекоммуникаций
- Единственный международный оператор связи с собственной инфраструктурой
- Присутствуем в 220 странах и территориях
- Сильные местные компетенции: центр инноваций и центр мониторинга киберугроз (SOC)
- Создаем инновации для крупного бизнеса: 8 из 10 крупнейших российских компаний Forbes-2000 Top-10 – наши клиенты*



800+ сотрудников



В России с 1958 года (SITA)

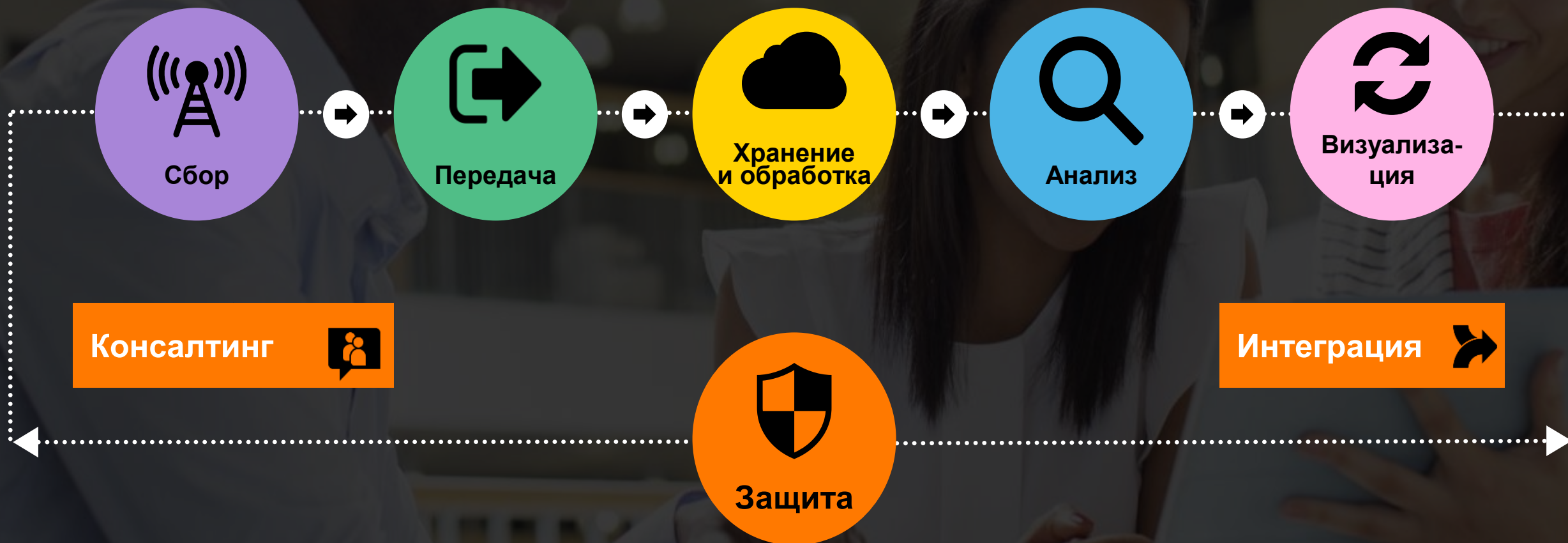
- 31 отделения
- 13 офис продаж
- 1500 корпоративных клиентов

Офисы в СНГ

Киев
Алма-Ата
Минск

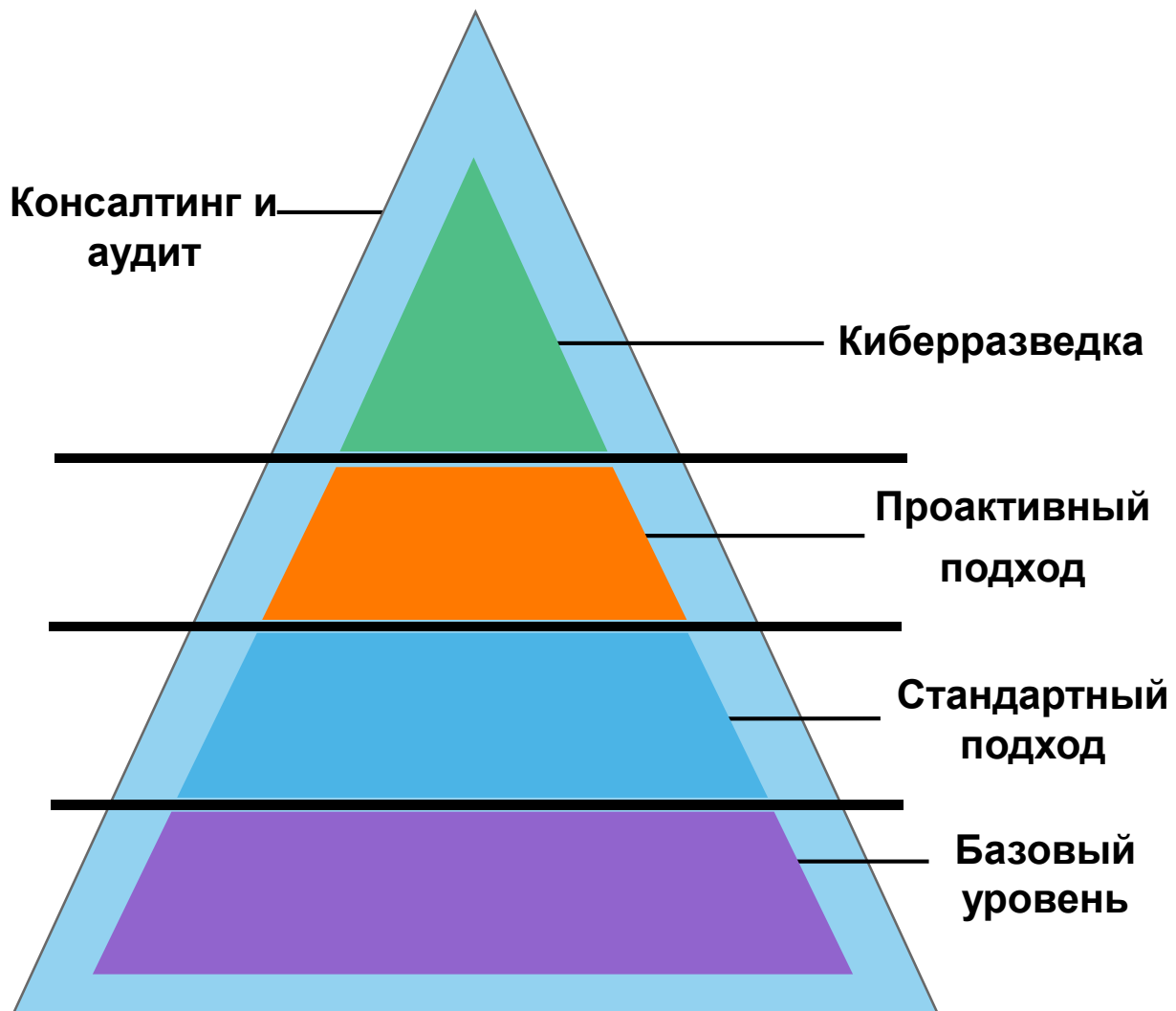
*according to Top-2000 Forbes 2018 rating

Наши компетенции для управления и защиты ваших данных



Наш подход к кибербезопасности

Комплексный подход



Участники

Решения



ИТ / ИБ
консультанты

Консалтинг
Аудит
Интеграционные услуги



Исследователи

CERT
Анализ вредоносного ПО
Анализ угроз



Аналитики CyberSOC
Ethical hackers

Корреляция событий
Мониторинг и
реагирование на
инциденты ИБ



NOC
ИТ / ИБ эксперты

Защита сети
Защита устройств
Управление учетными
данными



Все сотрудники
компании

Security awareness

Глобальное присутствие



Независимый CERT



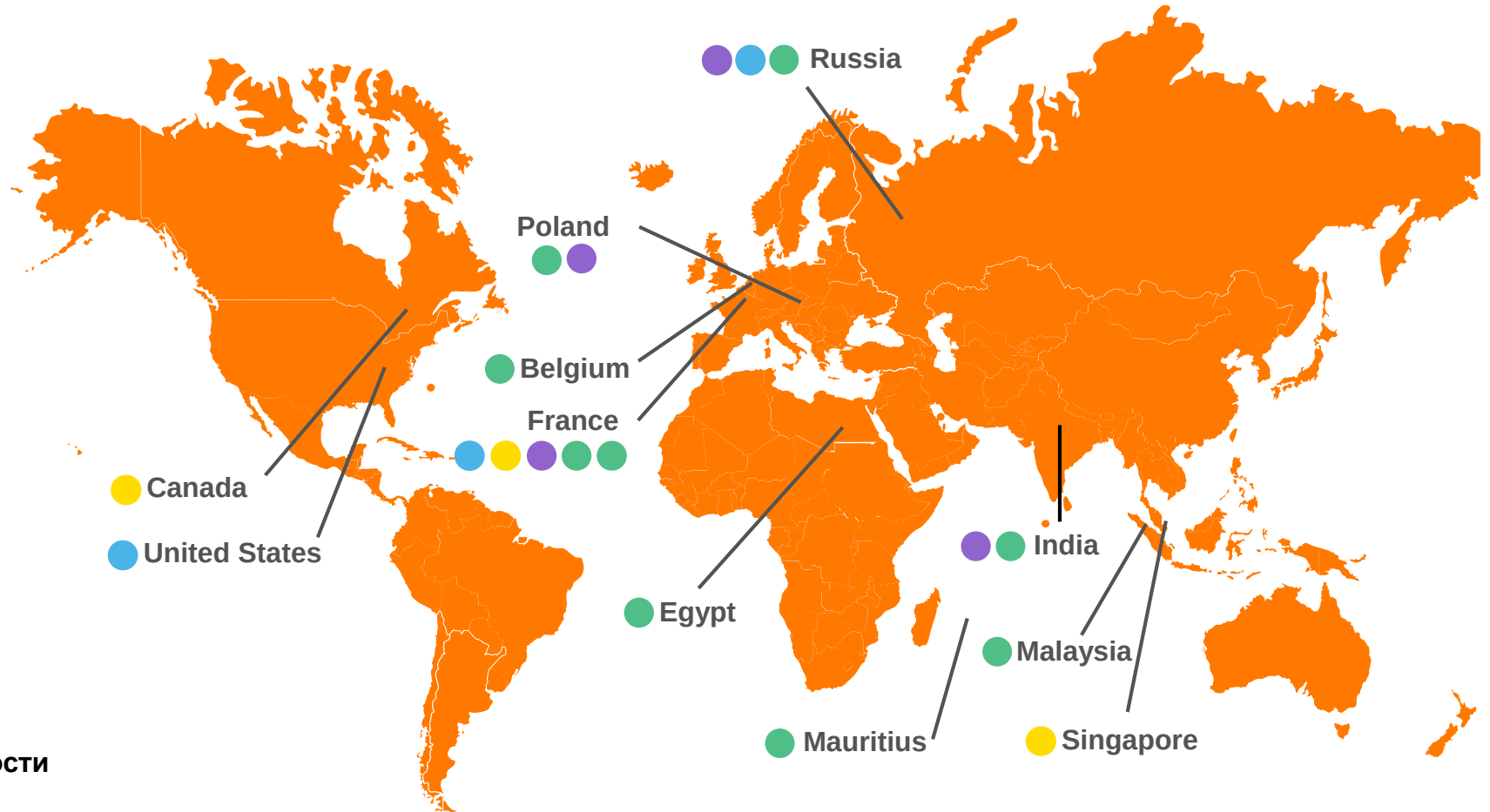
Реагирование на инциденты ИБ



Forensics



Академия кибербезопасности



● 4 **CyberSoc** : корреляция событий, реагирование на инциденты 24x7x365

● 8 **SoC** : управление устройствами безопасности 24x7x365

● 3 **CERT** : реагирование и расследование инцидентов ИБ 24x7x365

● 3 **scrubbing centers** : защита от DDoS атак 24x7x365

Особенности миграции с Microsoft TMG

Сравнение функционала TMG и решения FortiGate + FortiWeb

	TMG	FortiGate + FortiWeb
Межсетевой экран (Firewall)	✓	✓
SSL инспекция	✓	✓
Web фильтрация	✓	✓
Antivirus / Antimalware	✓	✓
Система предотвращения вторжений (IPS)	✓	✓
Интеграция с «песочницей» (sandboxing)	✗	✓
DLP	✗	✓
Режим Reverse Proxy	✓	✓
L7 load balancing	✓	✓
Портал аутентификации	✓	✓
Single sign-on (SSO)	✓	✓
Защита от атак на web приложения	✗	✓
SSL VPN	✗	✓
Traffic Shaping	✗	✓
IP reputation	✗	✓
Сертификация ФСТЭК	✗	✓

Особенности миграции с Microsoft TMG

- **Анализ конфигурации TMG**

Определение используемого функционала, подхода к формированию политик, типов публикаций на TMG

- **Выбор варианта решения**

В зависимости от функционала текущего решения на базе Microsoft TMG возможна миграция или на FortiGate + FortiWeb, или только на FortiGate

- **Пилотное тестирование**

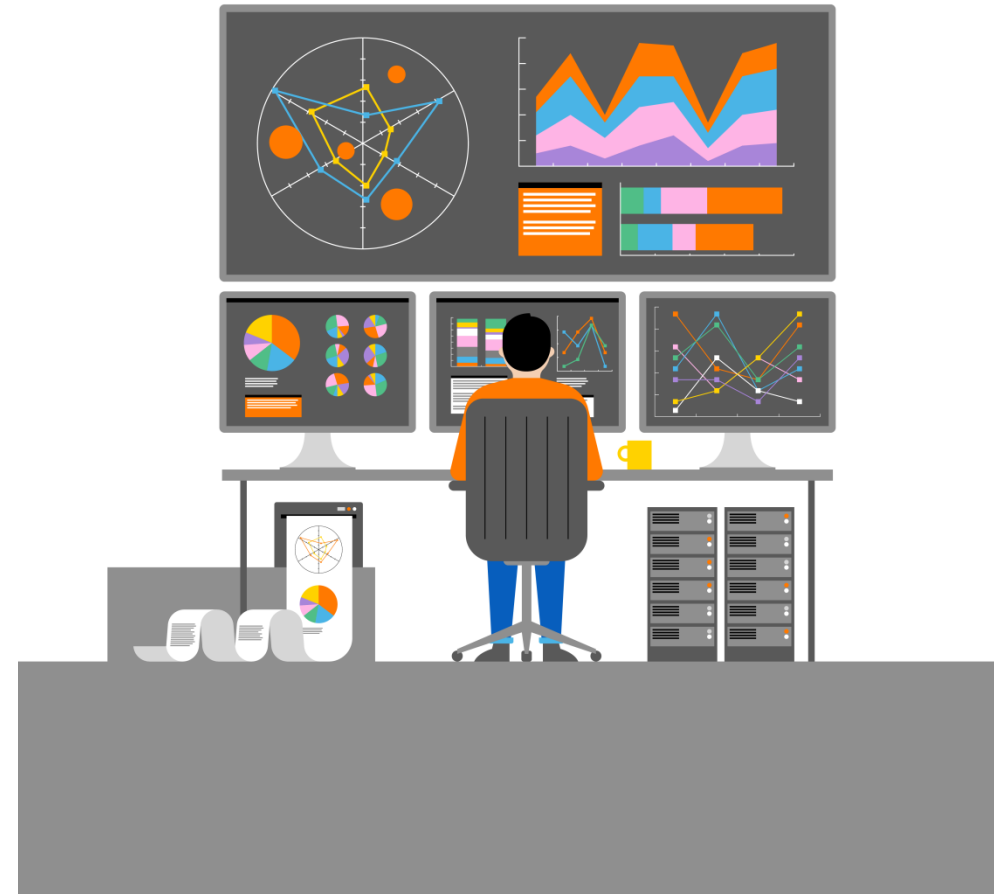
Проводится интеграция решения с системами заказчика, выполняется миграция части политик и публикаций, осуществляется проверка их работоспособности, формируется подход к миграции правил на решение Fortinet

- **Выбор режима FortiGate**

В зависимости от структуры политики выбирается режим Profile-based или Policy-Based

- **Аудит групп Active Directory**

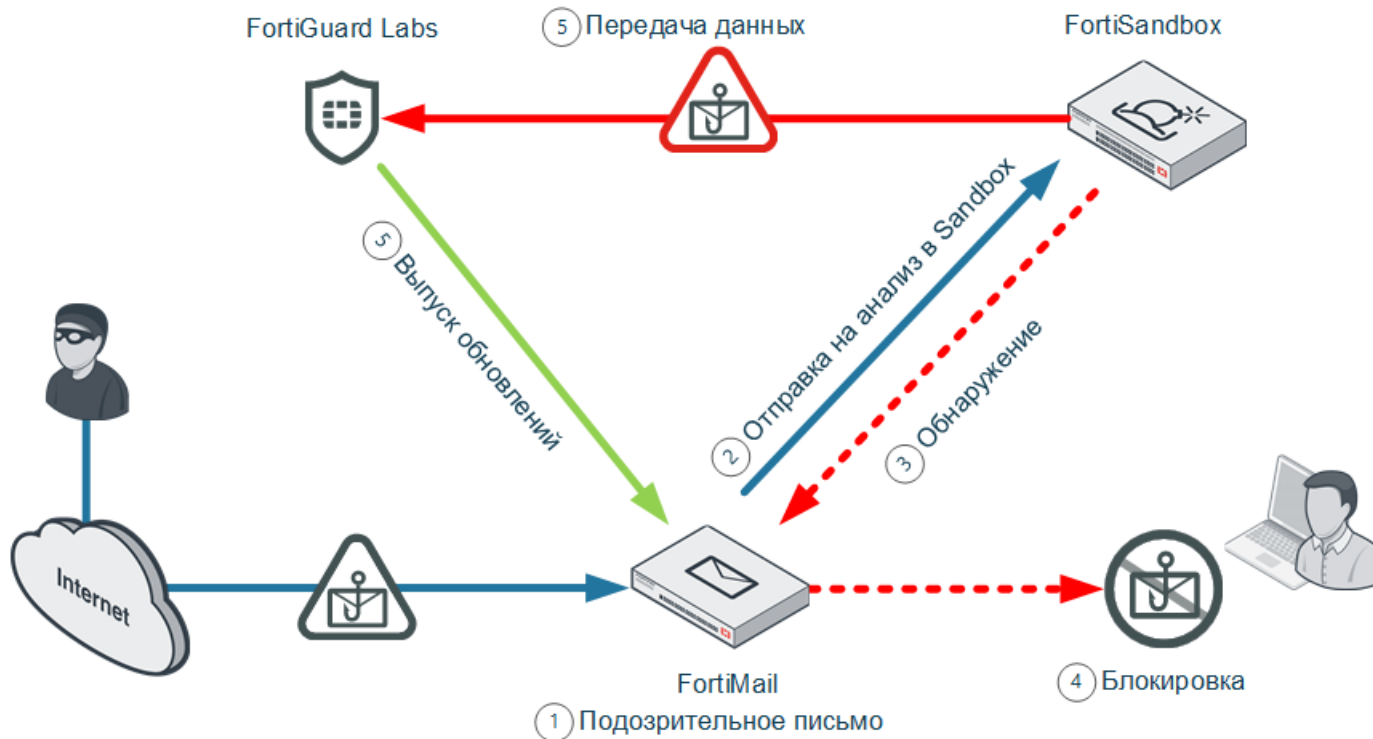
Выполняется аудит групп Active Directory, используемых в политике, и анализируется необходимость их изменения



Защита почты с помощью FortiMail + FortiSandbox

FortiMail

- Повышение уровня защиты почтовых сервисов от входящего и исходящего спама, вирусов, червей, фишинга и шпионских программ
- Замена старых систем фильтрации
- Интеграция с текущими системами безопасности Fortinet



Что? Где? Куда?

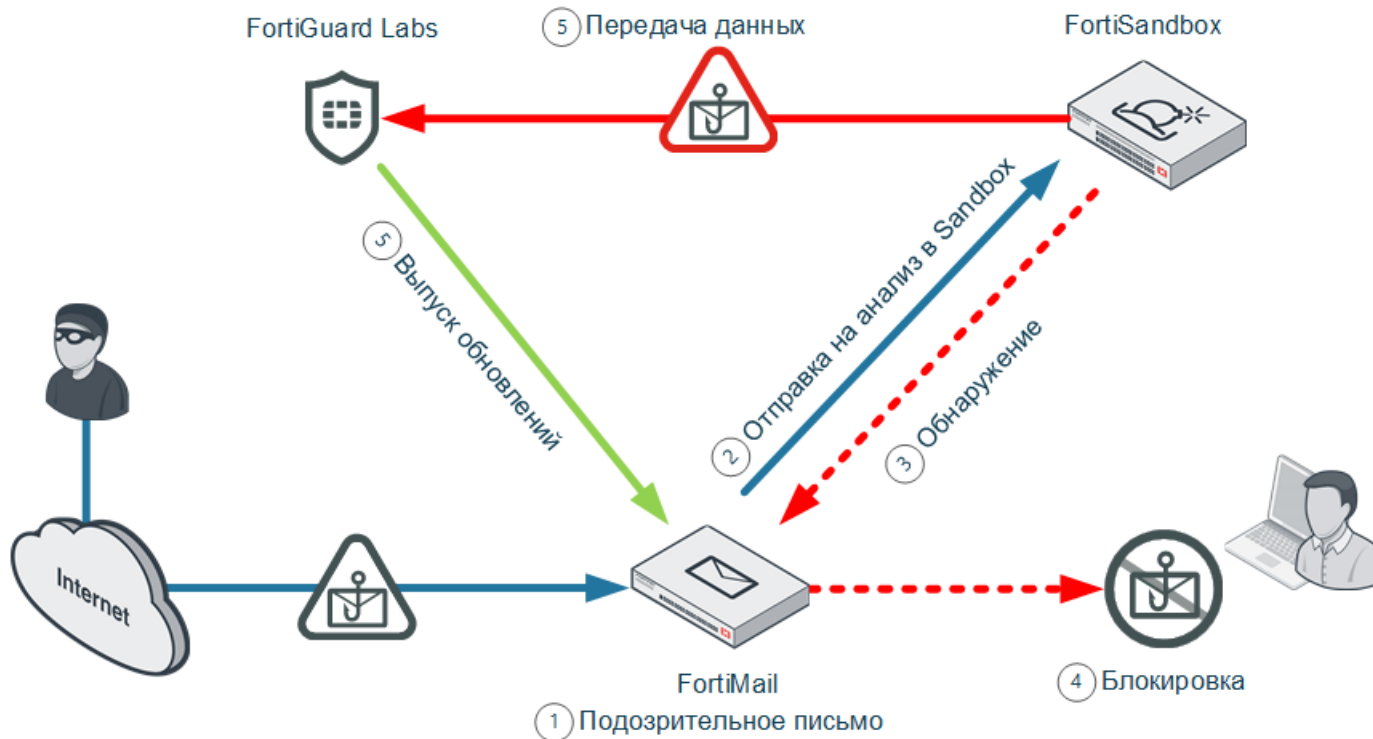
Перепроверь правила

Понимание задачи

Не спеши за
обновлениями

FortiSandbox

- Повышение уровня защиты почтовых сервисов от входящего и исходящего спама, вирусов, червей, фишинга и шпионских программ
- Замена старых систем фильтрации
- Интеграция с текущими системами безопасности Fortinet



Типы файлов?

Какие VM?

Один тип файлов –
одна VM

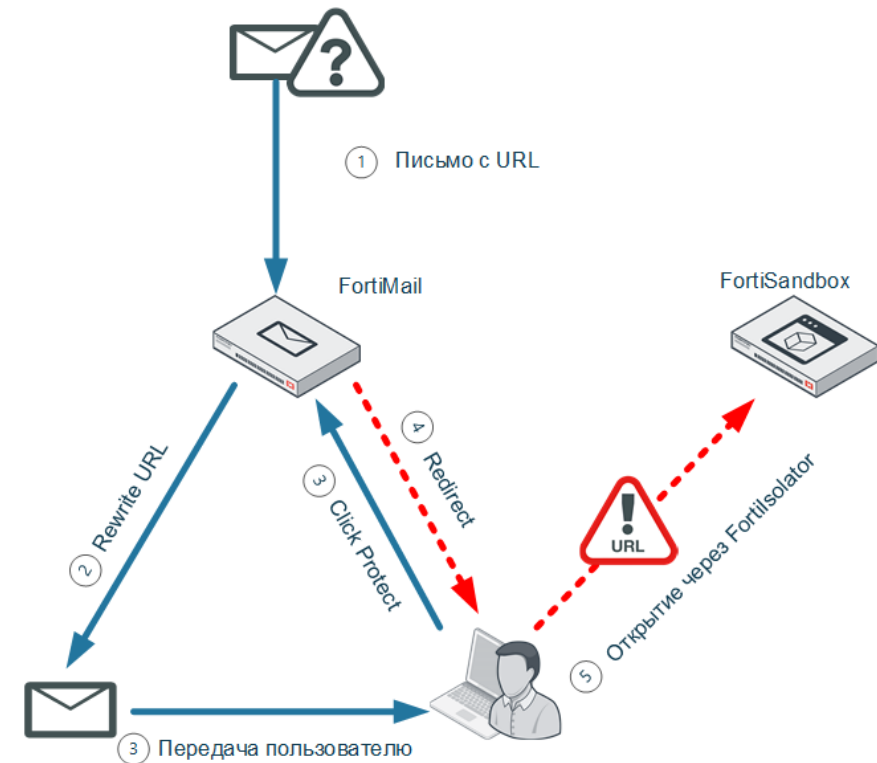
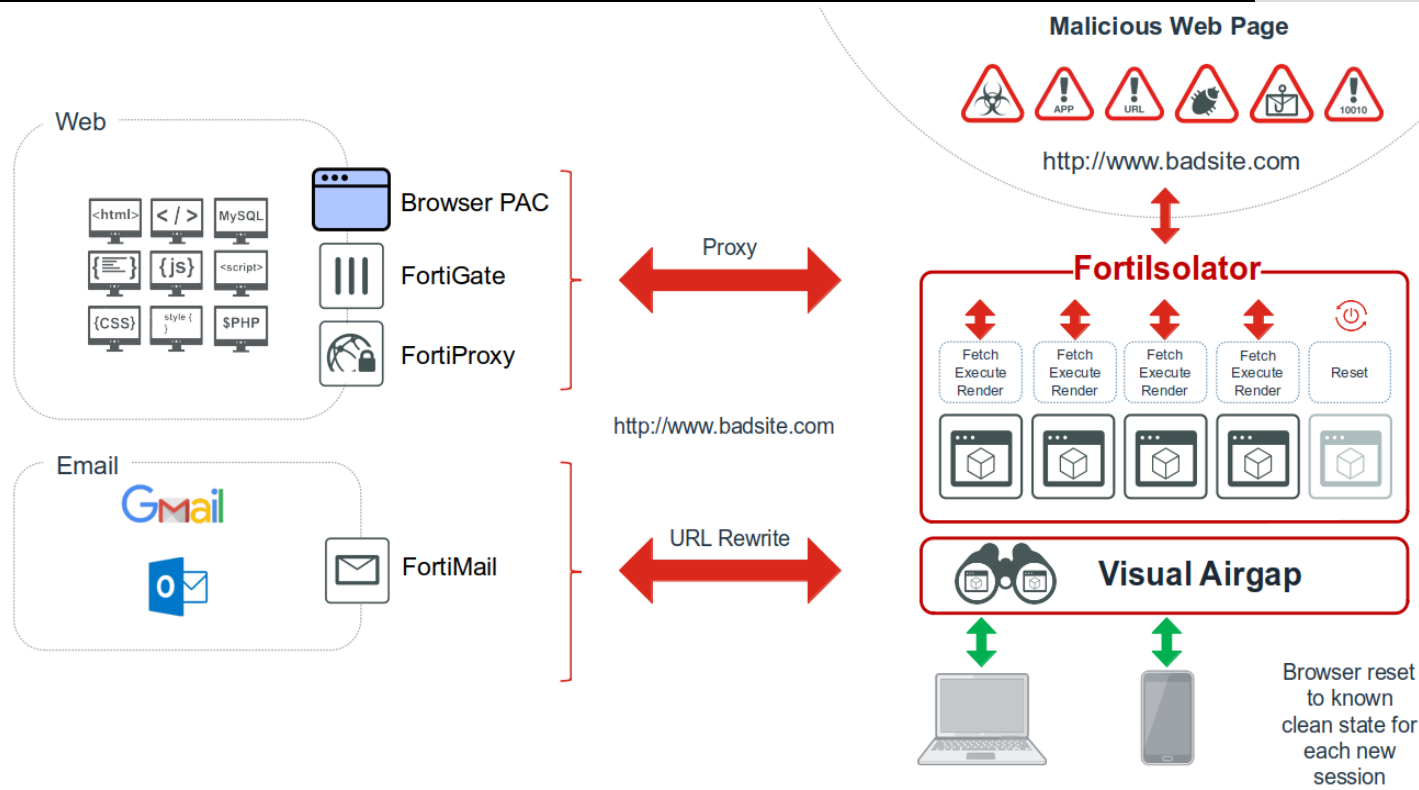
Будет ли prefilter?

Фильтрация пользовательского контента с помощью Fortislator

Fortisolator

- Дополнительный уровень безопасности
- Просмотр веб-сайтов в изолированной среде
- Интеграция с FortiGate, FortiMail

- Где будет установлен Fortisolator?
- Необходима ли аутентификация?



Fortisolator

ДО

20+ Scripts

Tracking cookies & scripts

3rd party
scripts &
content from
iFrame

ПОСЛЕ

2 Fortisolator Scripts

No external scripts, iFrames, imports

[illegible]

```
<!doctype html>
<html style="overflow: hidden;">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width">
    <link rel="stylesheet" href="https://10.1.0.1:8887/ftnt.css">
    <script src="https://10.1.0.1:8887/jquery.js"></script>
    <script src="https://10.1.0.1:8887/ftnt.js"></script>
    <title>Yahoo</title>
  </head>
  <body>
    <script src="https://10.1.0.1:8887/ftnt.js"></script>
    <div id="statusDiv" hidden="hidden"></div>
    <canvas id="mainCanvas" width="150" height="979" style="cursor: default;">
    <canvas id="popupCanvas">
  </body>
</html>
```


Спасибо!



**Business
Services**

FORTINET®