FortiMail - Шлюз Защиты Электронной Почты онлайн семинар 17 апреля

Андрей Терехов

инженер

email: aterekhov@fortinet.com

Что такое FortiMail?

Обзор

Защита от угроз в электронной почте

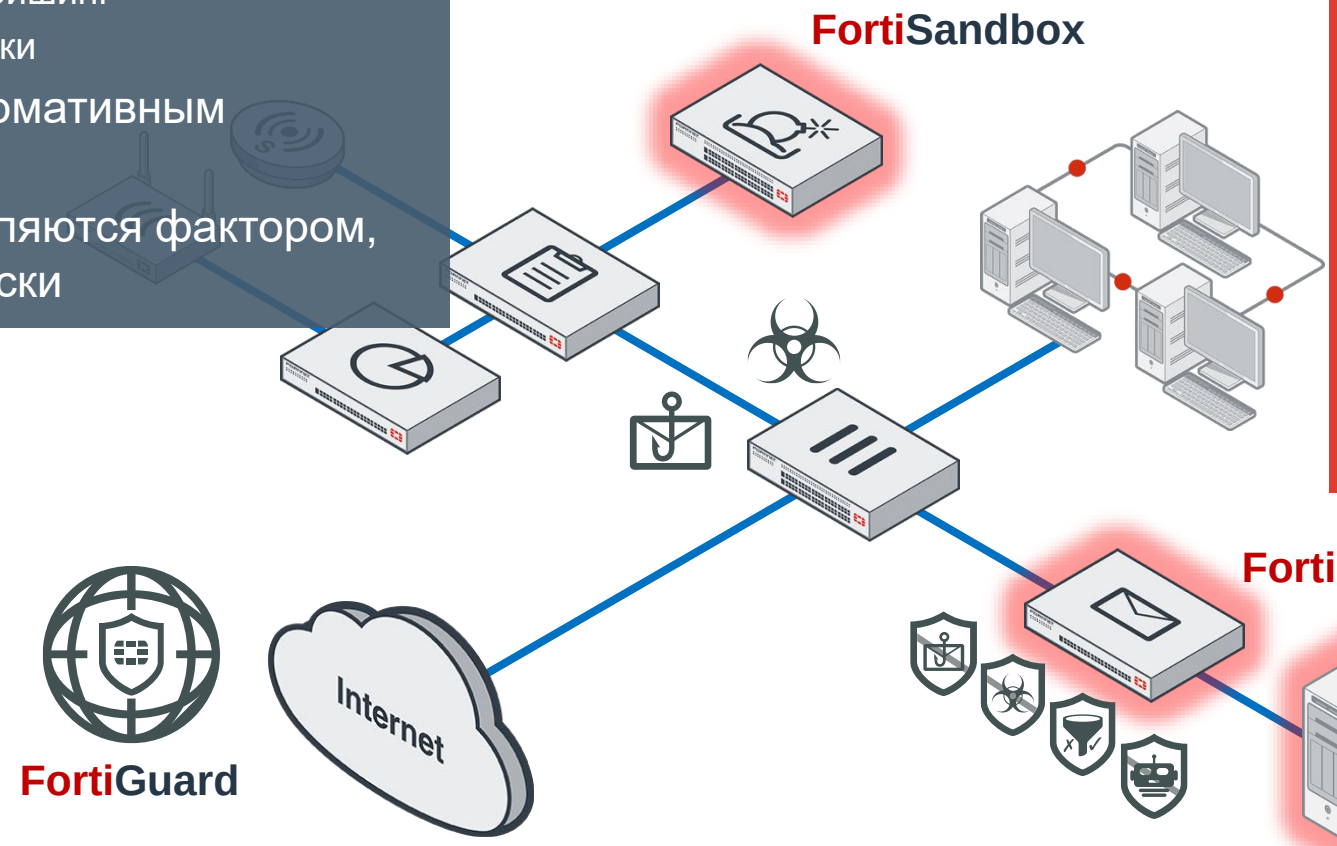
Основные проблемы

Электронная почта - "дверь" в организацию для злоумышленников

- Спам, вложения, фишинг
- Направленные атаки

Соответствие нормативным требованиям

Пользователи являются фактором, повышающим риски



Техническое решение

Шлюз электронной почты FortiMail

- Защита входящей и исходящей почты
- Защита конфиденциальности
- Интеграция со средствами защиты от продвинутых угроз

Преимущества

- Подтвержденная эффективность антиспама - VBSpam
- 44 награды VB100
- Лучшее в отрасли по соотношению эффективности, производительности и стоимости

FortiMail - доказанная эффективность

Fortinet FortiMail

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed:

10% 50% 95% 98%

Product					Block Rate	NSS-Tested Throughput	3-Year TCO (US$)
Fortinet Advanced Threat Protection (FortiSandbox Cloud with FortiGate 600D v5.6.1, FortiMail Virtual Appliance v5.4.0 and FortiClient ATP Agent v5.6.1.1112)					99.6%	2,692 Mbps	$20,430
	Drive-by Exploits	Social Exploits	HTTP Malware	Email Malware	Offline Infections	False Positives	Evasions[1]
Block Rate	100.0%	93.3%	99.3%	99.0%	100.0%	0.00%	88.6%
Additionally Detected	0.0%	6.7%	0.5%	1.0%	0.0%	0.00%	NA

Product			Breach Detection Rate[1]	NSS-Tested Throughput	3-Year TCO (US$)
Fortinet FortiSandbox-2000E v.3.0.0 & **FortiClient (ATP Agent)** v.5.6.6.1167			99.0%	8,667 Mbps	$130,405
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware (Executables)	HTTP Malware (Docs & Scripts)	SMTP Malware
0.93%	100.0%	100.0%	99.9%	100.0%	99.9%
Offline Infections		Stability & Reliability		Evasions Detected	
100.0%		PASS		370/374	

Fig. 2 – 1,224 ATD-Email Test Runs

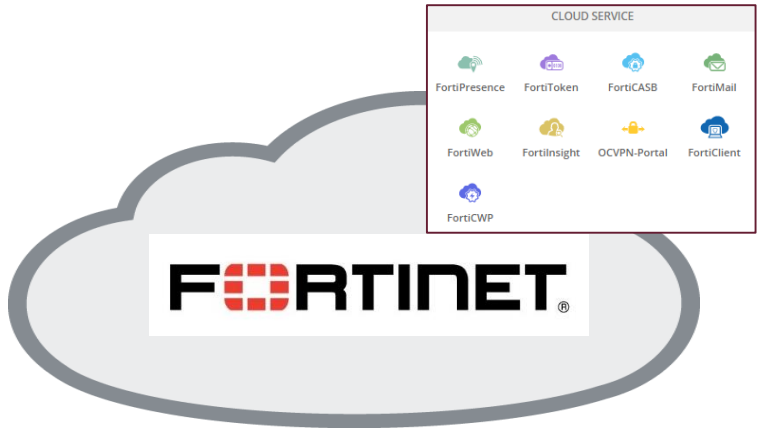
Варианты исполнения для любых потребностей

Программно-аппаратные комплексы

- Линейка моделей
- Фильтрация от 30 тысяч до 2 миллионов писем в час
- Поддержка 10GE интерфейсов
- **Количество пользователей не ограничено**

Виртуальные машины

- Линейка вариантов
- Лицензирование по количеству ядер и защищаемых доменов
- **Количество пользователей не ограничено**



Облачный сервис

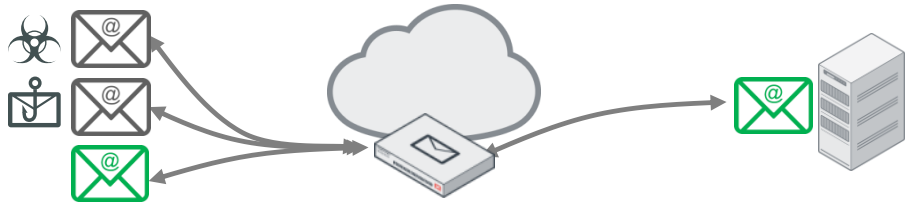
- Режим Gateway или Server
- Стандартный или Премиальный
- Настраивается Fortinet, управляется совместно
- Погодовое лицензирование по количеству пользователей

Сценарии внедрения

- Fortinet поддерживает уникальные сценарии внедрения:

Шлюз (Gateway)

» **Наиболее распространённый - MTA**

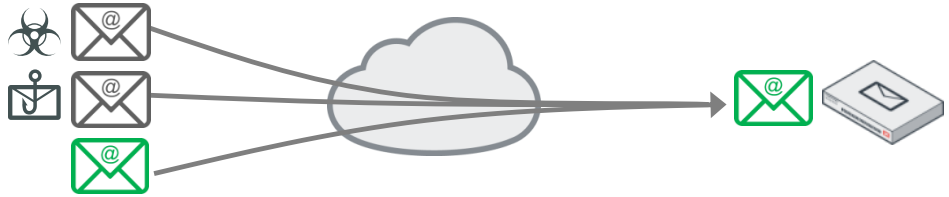


Прозрачный (Transparent)

» Включается в разрыв прозрачно для остальных узлов Не требуется изменений конфигурации в существующей почтовой инфраструктуре

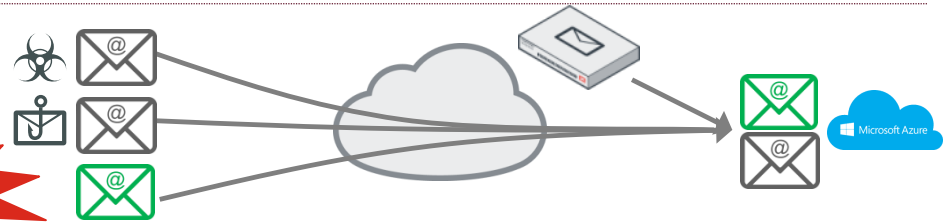
Сервер (Server)

» FortiMail функционирует как сервер почтовых ящиков с функцией общего календаря, с доступом к почте по POP3, IMAP и Webmail



Режим O365

» Извлечение



New

Полный набор защитных мер

SECURED BY FORTIGUARD®

24x7 + Enterprise ATP Bundle

24x7 + Base Bundle

Антиспам сервис

- Репутация отправителей
- Категорирование URL
- Репутация хеш-сумм вложений и писем
- Выявление новостных и рекламных рассылок

Доступна отдельно

Антивирусный сервис

- Сигнатуры по признакам
- Эвристические правила
- Эмуляция
- Извлечение из упаковщиков
- Запатентованный движок (CPRL)

Доступна отдельно

Outbreak Prevention

- Репутационный антивирус
- Защита от новых кампаний рассылки спама и ВПО
- Использует threat intelligence для совместной борьбы с ВПО

Доступна отдельно

Облако FortiSandbox

- Облачный сервис сетевой песочницы
- Включает все этапы анализа
- По подписке
- Не требуется отдельная песочница

Доступна отдельно

Нейтрализация контента (CDR)

- Удаляет активный контент - источник риска
- Поддерживает форматы MS Office и PDF
- Исходные документы могут автоматически сохраняться

Защита кликов

- Запрос репутации в момент клика
- Идентифицирует недавно скомпрометированные сайты и защищает от новых фишинговых кампаний

Анализ подмены отправителя

- Идентифицирует маскировку отправителя под сотрудника
- Динамически строит признаки
- Дополняет аутентификацию отправителей

Общие вопросы

Обзор

Документация FortiMail

Портал документации: https://docs.fortinet.com/

Состав документации FortiMail:

Admin Guide - Руководство администратора

Cookbook - Примеры и рекомендации по настройке

CLI Reference - Руководство по интерфейсу командной строки

REST API Reference - Описание прикладного программного интерфейса

Release Notes - Заметки к релизу

Жизненный цикл ПО и оборудования

Политика и состояние жизненного цикла:
https://support.fortinet.com/Information/ProductLifeCycle.aspx

Лучшие практики по выбору версии ПО ForiMail :

Актуальная версия «0» (04/2020 - 6.2) – для тестирования и новых внедрений

Версия «-1» (04/2020 - 6.0) – в общем случае

Лучшие практики по обновлению версии

Планирование процедур обновления и отката (см. «Release Notes»)

Мотивированное обновление (см. «Release Notes»)

Поиск ответов на вопросы

Официальные ресурсы:

Форум пользователей Fortinet: https://forum.fortinet.com/

База знаний TAC: https://kb.fortinet.com/

Полный индекс статей базы знаний: https://pub.kb.fortinet.com/index/

Неофициальные ресурсы:

Канал в telegram, на русском языке: https://t.me/fortichat

Канал в reddit: https://www.reddit.com/r/fortinet/

К кому можно обратиться за помощью

Вопросы по тестированию и внедрению

Системные интеграторы, партнёры Fortinet в России: https://www.fortinet.com/partners/partner-program/find-a-partner/emeapartners.html

Консультации по работе ПО, решение технических проблем

Центр технической поддержки (TAC): https://support.fortinet.com/

Консультации по работе подписок, устранение ложных срабатываний

Лаборатория FortiGuard: https://fortiguard.com/faq

Общие технические вопросы

Группа системных инженеров Fortinet в России, Казахстане и Украине: cis_se@fortinet.com

Взаимодействие с TAC

Инструкция по заведению тикетов: https://fortinet.egnyte.com/dl/x92xaf0MHR

Описание сервисов с указанием SLA: https://fortinet.egnyte.com/dl/yEv1X0N5VH

Лучшие практики эффективной работы с TAC:

Ознакомьтесь с SLA и устанавливайте приоритет соответственно критичности

Для диагностики сложных проблем запросите удаленную сессию

Если необходима реакция «здесь и сейчас» - позвоните или напишите в чат: https://www.fortinet.com/support/contact.html

Если нарушен SLA – сообщите нам: cis_se@fortinet.com

Обратная связь по работе защитных мер

Веб-страница с формами обратной связи: https://fortiguard.com/faq

Варианты взаимодействия по проблемам с детектированием:

Спам – переслать в виде вложения на submitspam@fortinet.com

Не спам – переслать в виде вложения на removespam@fortinet.com

Некорректная репутация IP - https://fortiguard.com/learnmore#as

ВПО – переслать в виде запароленного архива на submitvirus@fortinet.com

Прочие вопросы - https://fortiguard.com/faq/antispam-contact

Систематически повторяющиеся проблемы – заявка в TAC

FortiMail

Обзор лучших практик

FORTINET

Многоуровневая фильтрация сообщений

Сессия
Репутация
EHLO
черные/белые
списки

Анти Вирус
Outbreak
хеш/CPRL

Анти Спам
Outbreak
Эвристика
Поведение

Контент
Момент
клика
CDR
Архивация

Песочница
URL
Вложения

DLP
Признаки
Правила
регулярные
выражения

Доставка
Последующее
действие
DKIM
SMIME
IBE
Маршрутизация

Промежуточное действие
Маркировка темы
Вставка заголовка/предупреждения
Доставка до альтернативного MTA
BCC / Оповещение / Архивация

Следующий Профиль

Финальное действие
Отбросить / Отклонить
Карантин

Многоуровневая фильтрация сообщений Лучшая практика

- Современный SEG реализует десятки мер защиты
- Освойтесь с их последовательностью
- FortiMail Admin Guide -> Order of execution

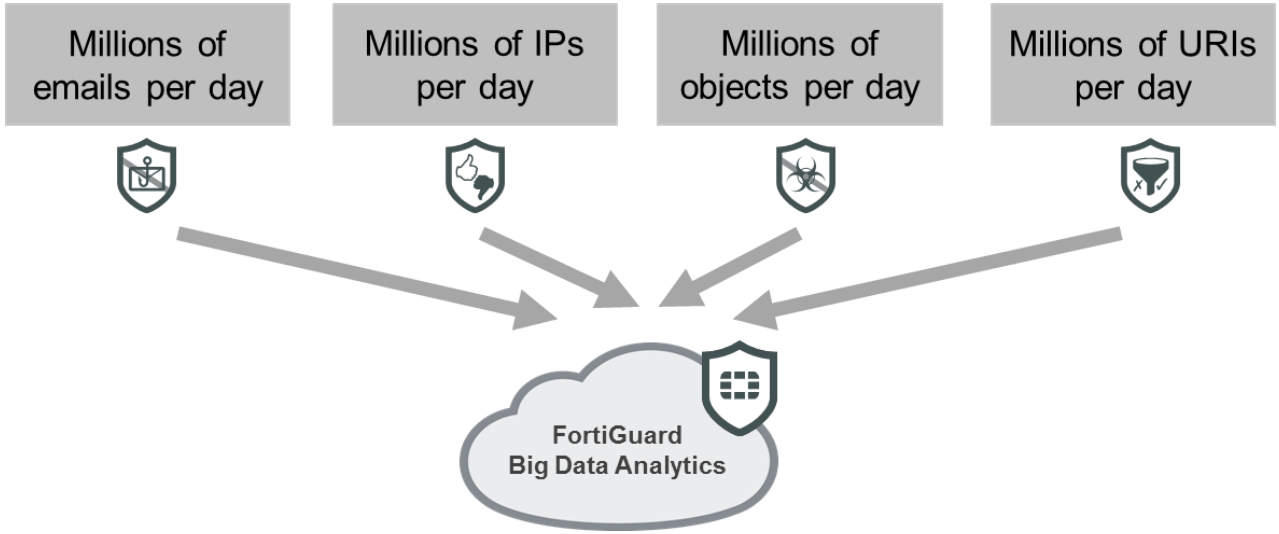
Table 2: Execution sequence of antispam techniques

Sender reputation	Client IP address	If the client IP is in the sender reputation database, check the score and enable any appropriate restrictions, if any.	Add the IP address to the sender reputation database and keep a reputation score based on the email received. Proceed to the next check.
FortiGuard block IP check	Client IP address	If the “Check FortiGuard Block IP at connection phase” is enabled in a session profile, FortiMail will check the client IP address against the FortiGuard block IP list. If positive, FortiMail rejects the email.	Proceed to the next check.
Endpoint reputation	Client endpoint ID	If the client endpoint ID is in the sender reputation database, check the score and enable any appropriate restrictions, if any.	Add the IP address to the endpoint reputation database and keep a reputation score based on the email received. Proceed to the next check.
Sender rate control per connection	Client IP address	Apply any connection limitations specified in the session profile. Proceed to the next check.	In there are no connection limitations, or if no session profile applies, proceed to the next check.

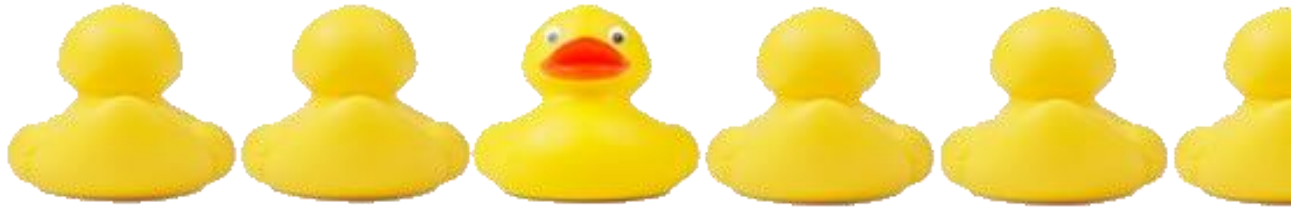
Адаптивная защита от новых кампаний

Защита от новых кампаний по рассылке спама и ВПО

- **Outbreak Protection**
  - **Спам:** подозрительные вложения выявляемые в известном спаме, могут быть заблокированы по репутации
  - **ВПО:** обмен данными о новом ВПО в Cyber Threat Alliance, облачная база репутации FortiSandbox, репутационный антивирус

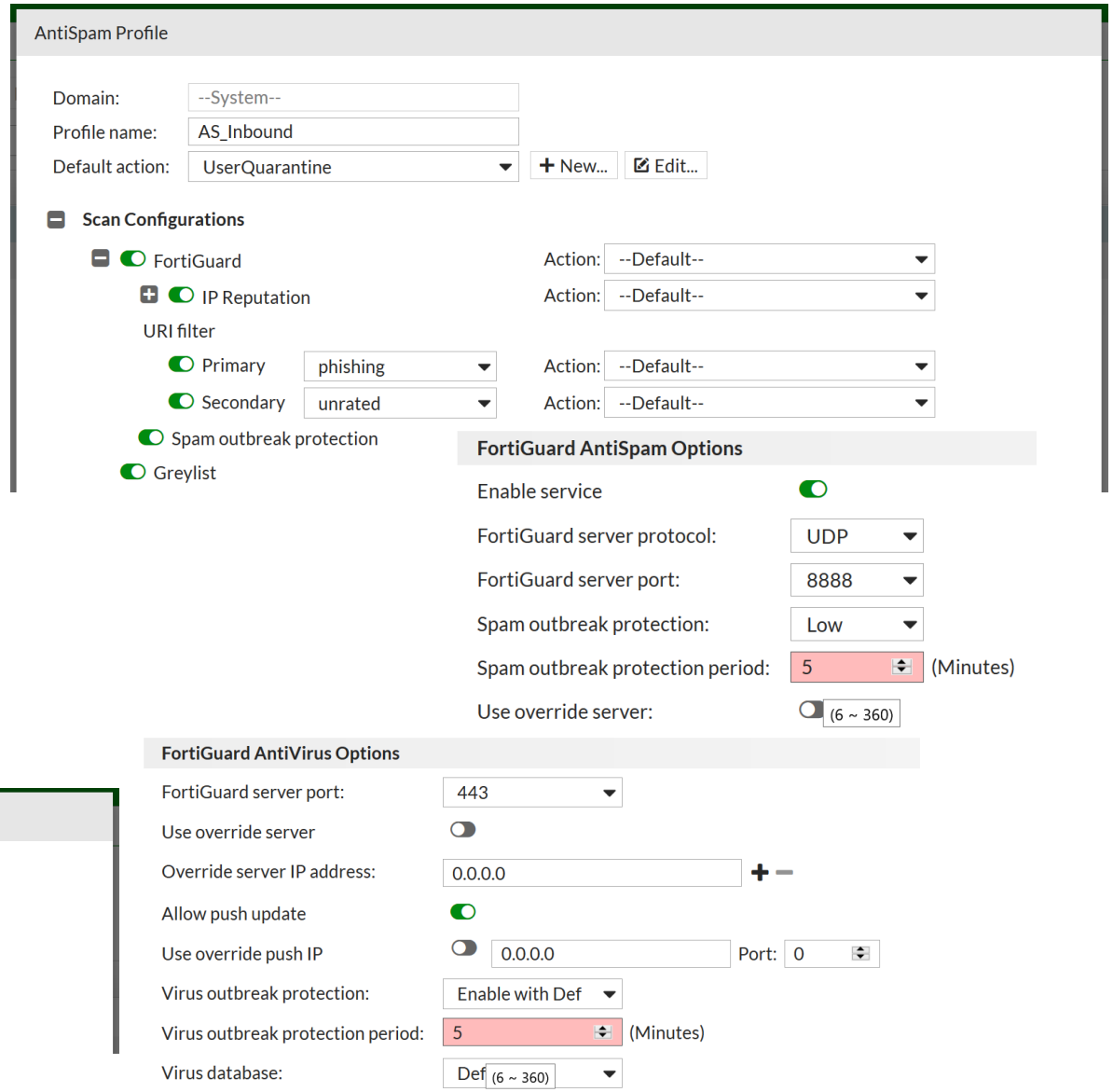


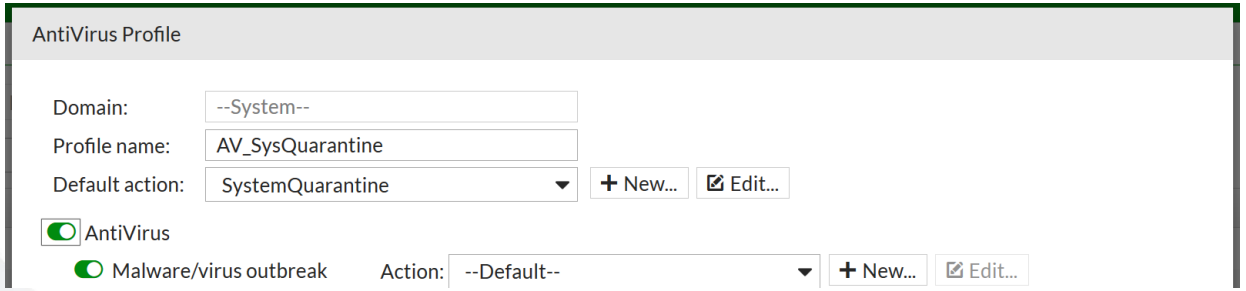
- **Поведенческий анализ**
  - Машинное обучение на основе предыдущих срабатываний
  - Похожи ли поведение отправителя и признаки письма на предыдущие срабатывания? "Если нечто выглядит как утка, плавает как утка и крякает как утка, ..."



Адаптивная защита от новых кампаний Лучшая практика

- Применение мер защиты от новых кампаний по рассылке спама и ВПО могут приводить к задержке в доставке почты пользователям.
- Antispam: Spam Outbreak, Greylisting
- Antivirus: Virus Outbreak
- FortiGuard: Spam Outbreak, Malware Outbreak

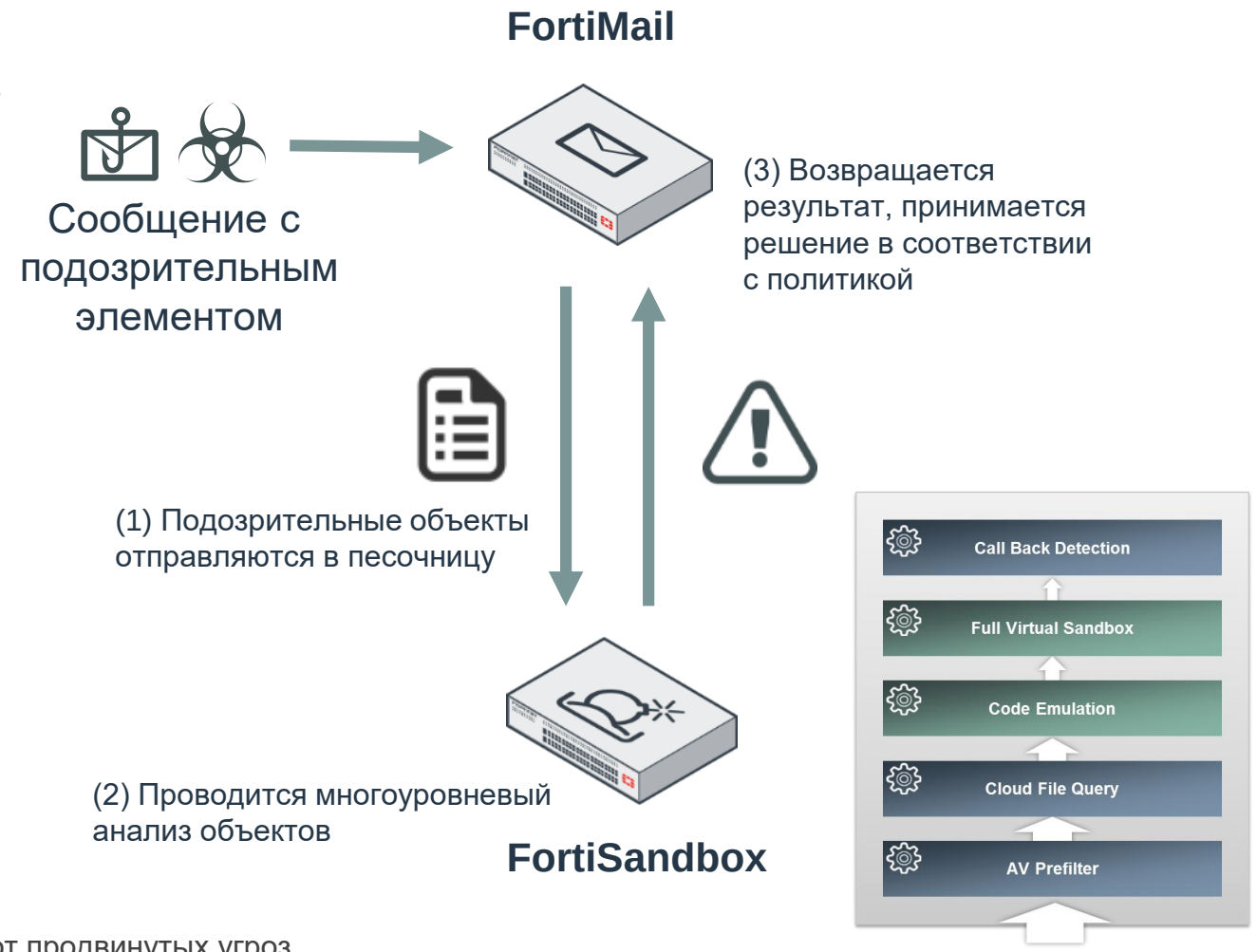




Сетевая песочница: защита от ВПО "нулевого дня"

Эффективное предотвращение ВПО "нулевого дня"

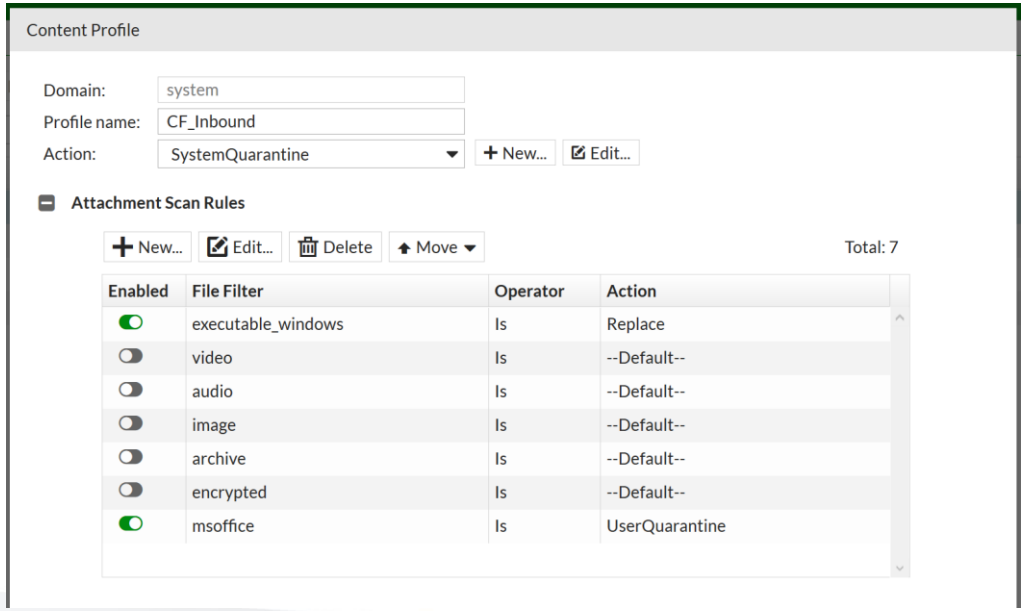
- **FortiMail помещает письмо в очередь и отправляет файлы и ссылки на проверку в FortiSandbox для анализа**
  - Статический сигнатурный и эвристический анализ
  - Запрос репутации в облаке FortiSandbox
  - Динамический анализ в виртуальной среде
  - Выявление попыток связи с C&C
  - Определение результата по шкале доверия и возврат результата
  - Многоуровневое кеширование результатов для максимальной эффективности

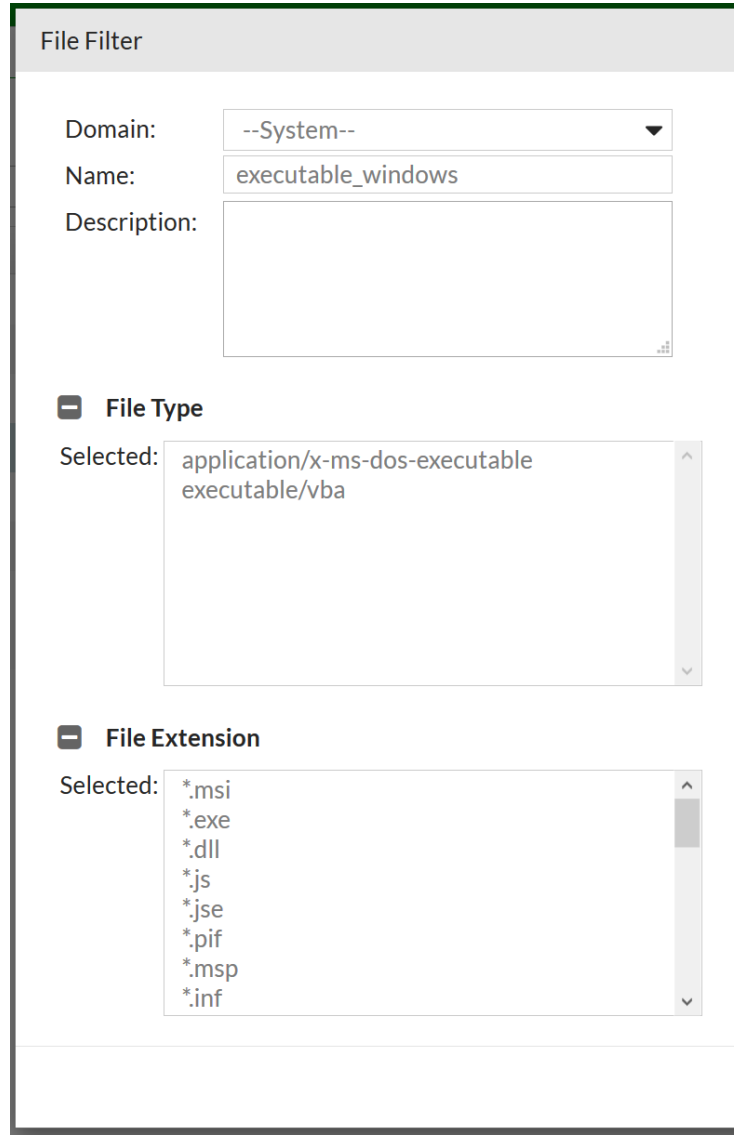


* Опциональная интеграция, входит в состав комплексного решения по защите от продвинутых угроз

Сетевая песочница: защита от ВПО "нулевого дня“ Лучшая практика

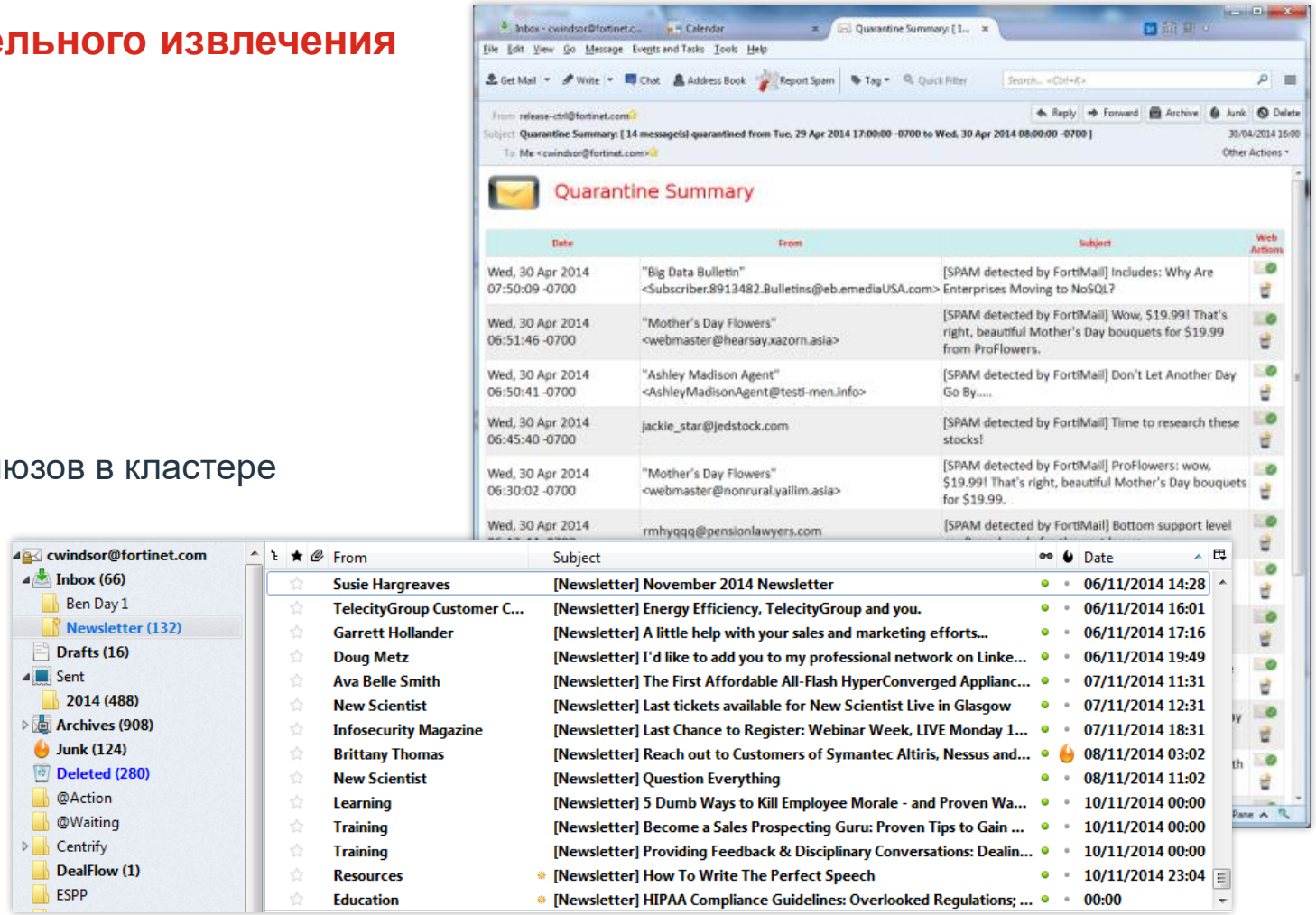
- Подозрительные и нежелательные вложения лучше отфильтровать, чем доставить пользователям.
- Отфильтруйте нежелательные вложения и ссылки до их попадания пользователю
- Пример - исполняемые файлы: exe, js, vbs, ps1.
- Content Profile -> File Filter





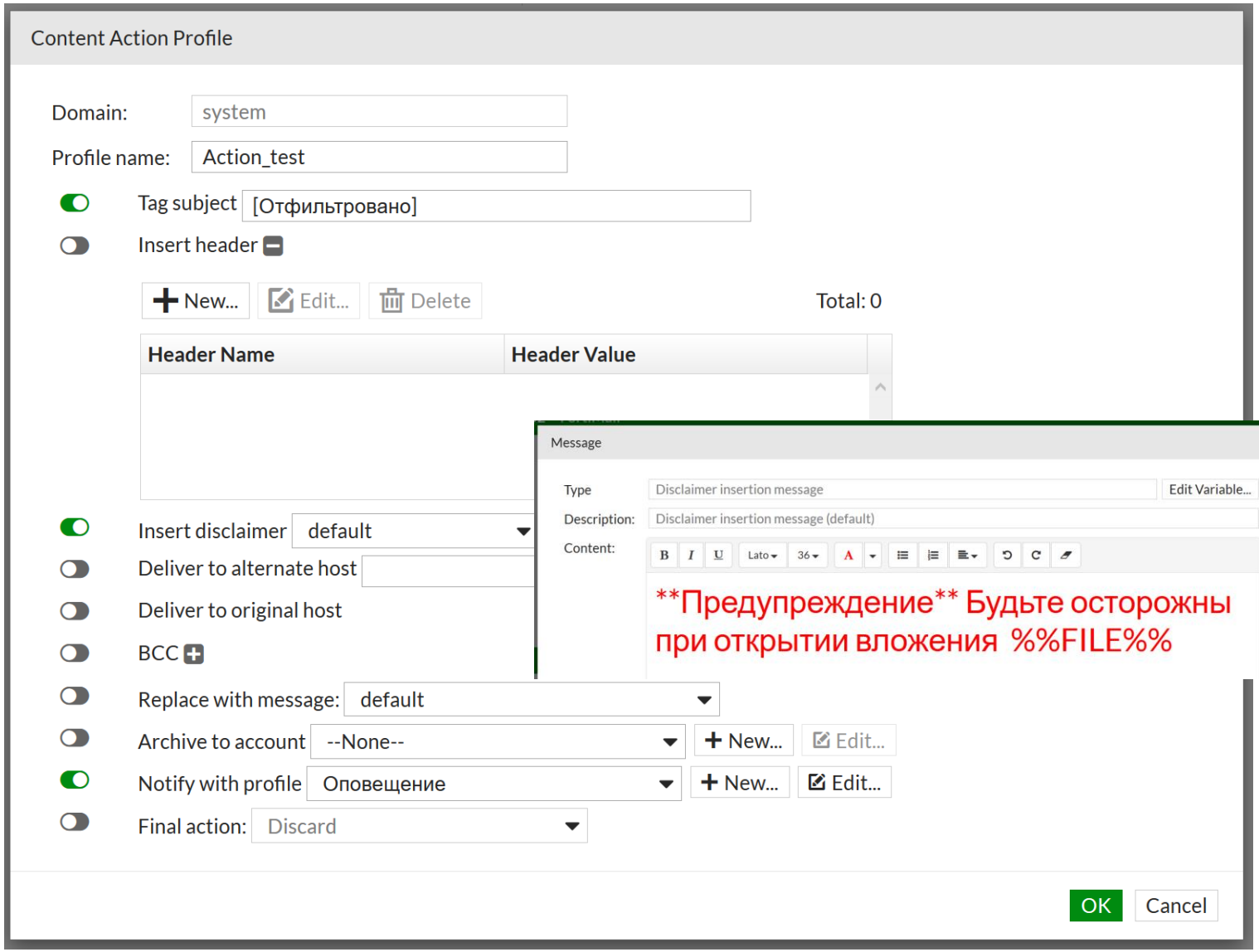
Пользовательский карантин и оповещения о срабатывании

- **Дайджест с возможностью самостоятельного извлечения письма из карантина**
  - Отправитель и тема
  - Ссылки на выпуск или удаление
  - Извлечение по web и электронной почте
- **Централизованный карантин**
  - Лёгкое администрирование
  - Может быть консолидирован для всех шлюзов в кластере
- **Выявление новостных рассылок**
- **Оповещение пользователей**
  - Автоматическая маркировка и доставка
  - Вставка заголовков
  - Блокирование и оповещение

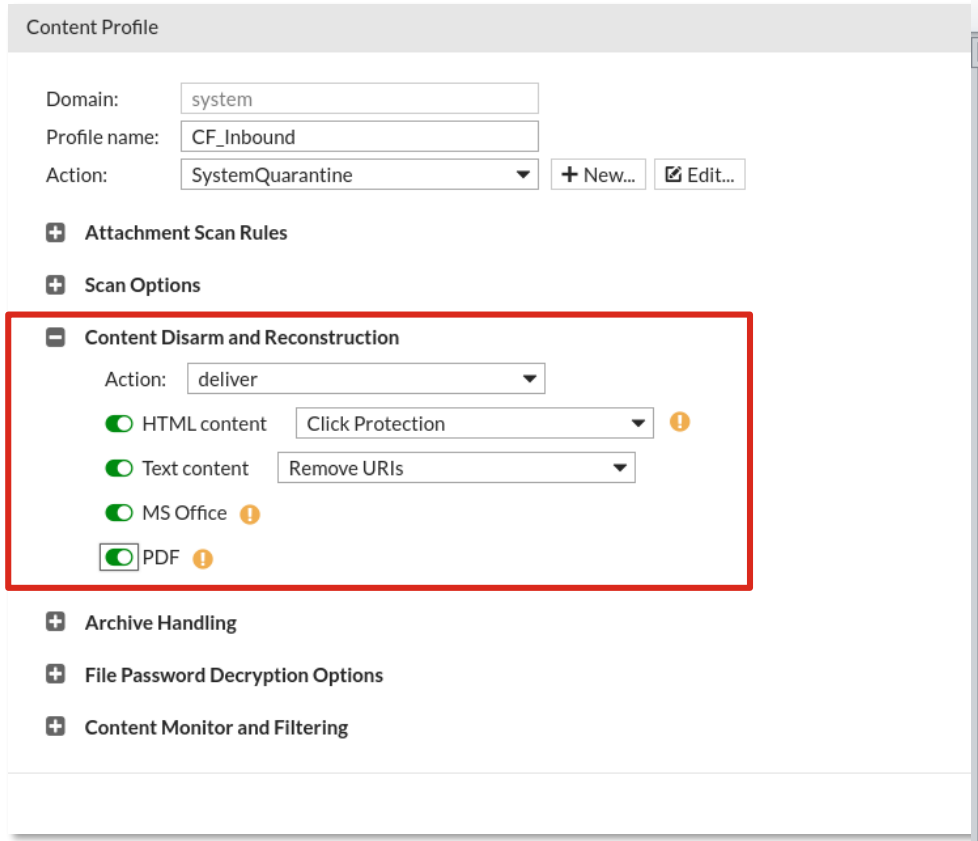


Оповещения о срабатывании Лучшая практика

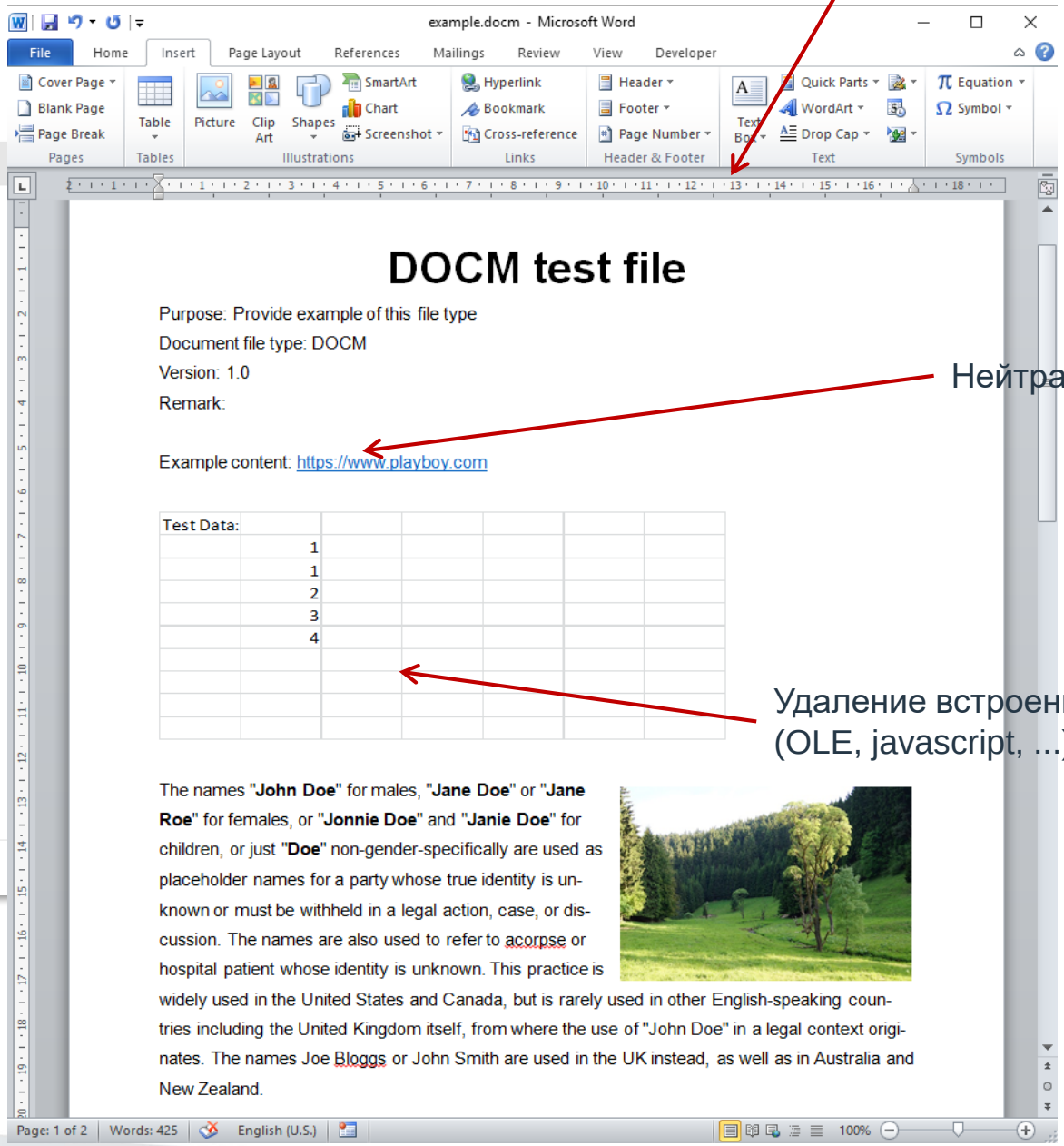
- Различные меры защиты имеют разные уровни точности и полноты фильтрации.
- Освойтесь с возможностями SEG по реагированию при срабатывании защитных мер
- Это позволит минимизировать блокировку сообщений из-за ложноположительных срабатываний.



Нейтрализация контента (Content Disarm and Reconstruction, CDR)



Удаление макросов

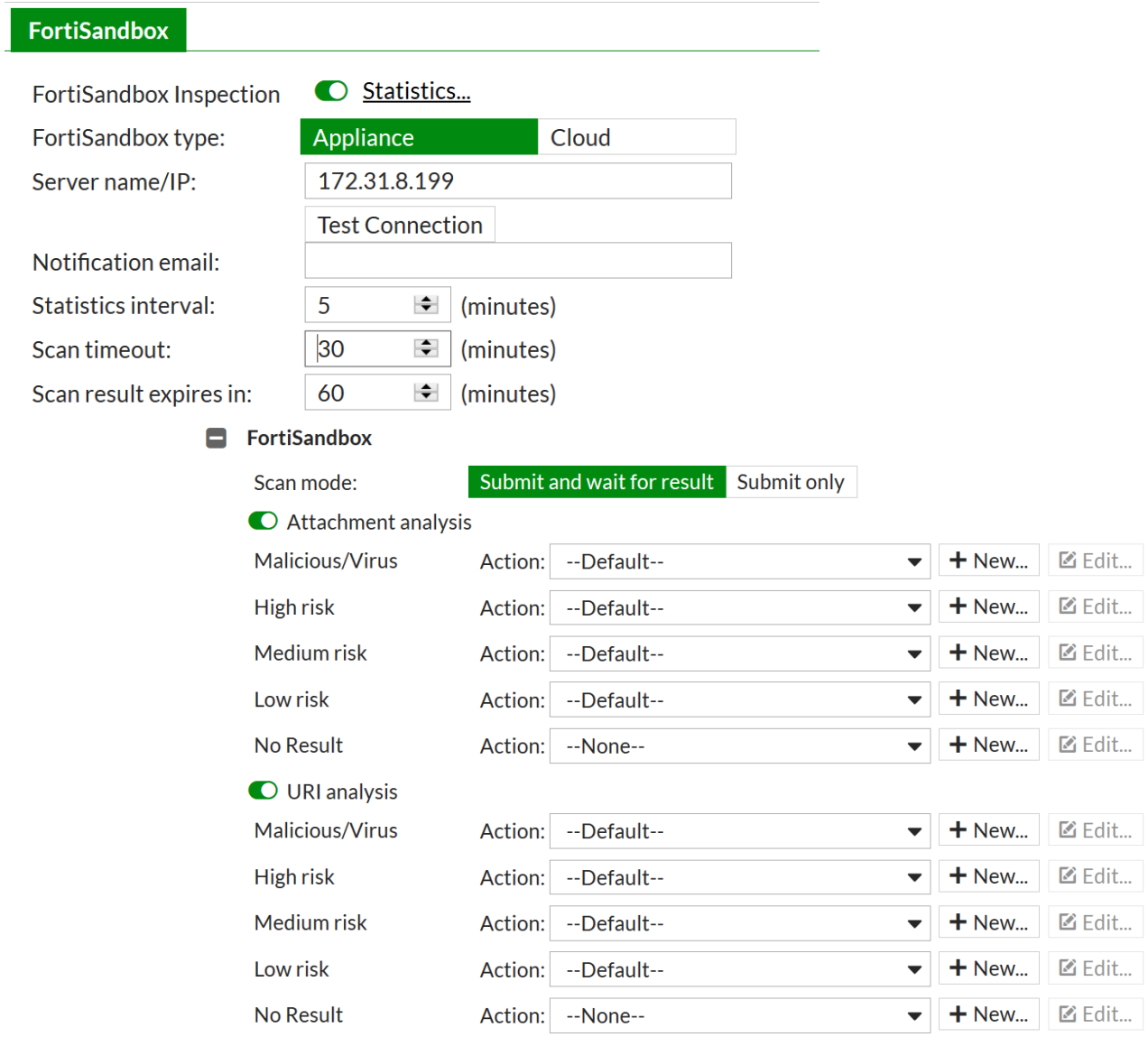


Нейтрализация ссылок

Удаление встроенного содержимого (OLE, javascript, ...)

Нейтрализация контента и анализ в песочнице Лучшая практика

- Анализ в сетевой песочнице занимает от нескольких секунд до нескольких минут
- В моменты пиковой нагрузки и накопления очереди время анализа может быть выше
- Определите допустимый предел задержки и реакцию при его превышении.
- Включите технологию CDR для мгновенной доставки сообщений с нейтрализованными вложениями.



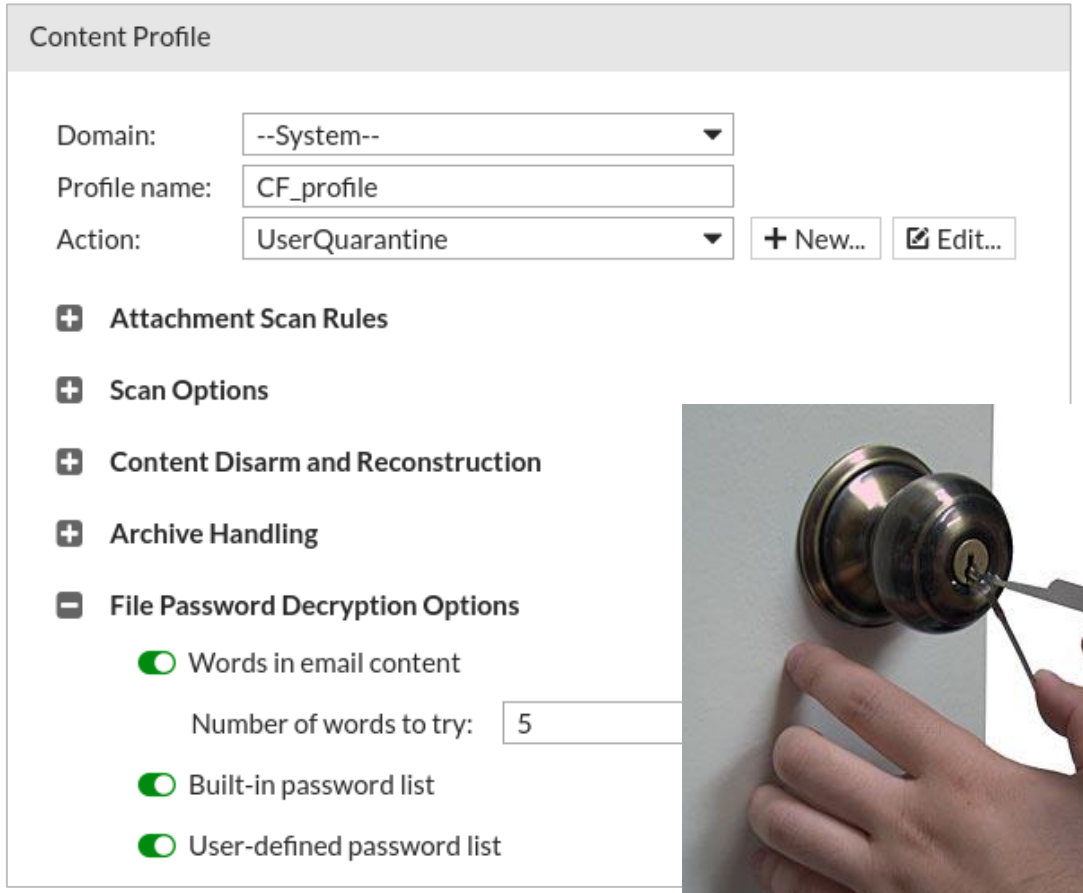
Работа с зашифрованными вложениями

Позволяет раскрыть и проверить зашифрованные/запароленные вложения

- PDF
- Архив
- Офисный документ

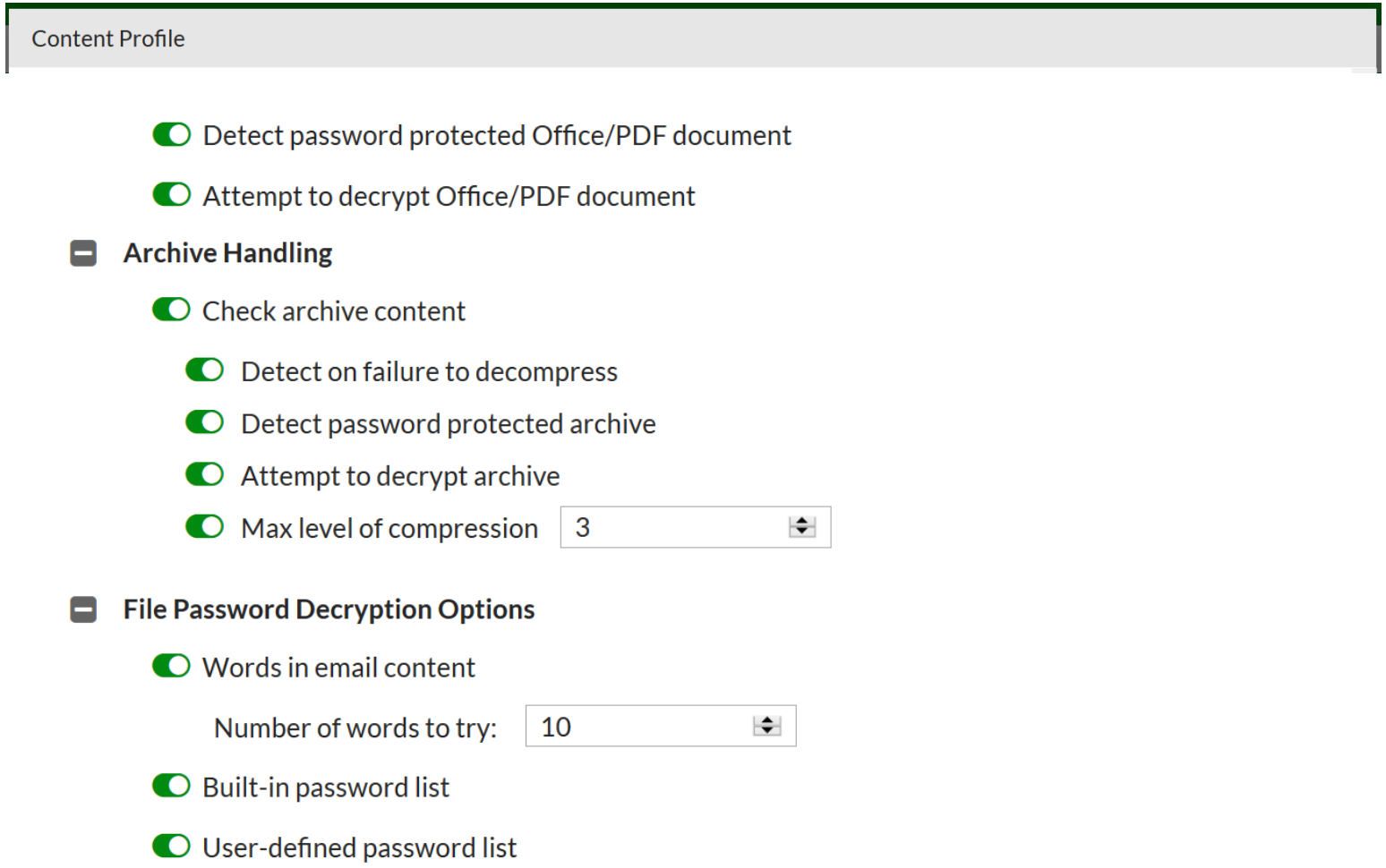
Используя ключевые слова из:

- тела письма
- встроенного списка паролей
- списка, определенного администратором



Работа с зашифрованными вложениями Лучшая практика

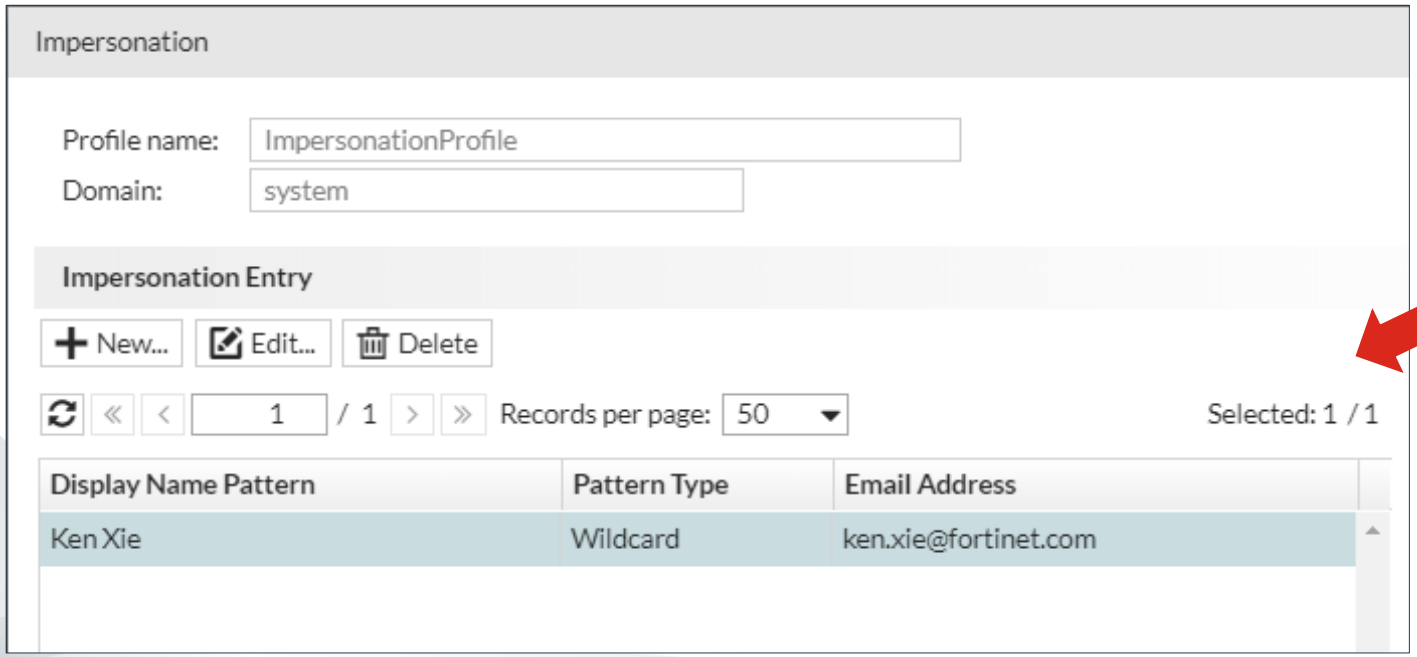
- Архивы и зашифрованные документы могут представлять особую угрозу из-за сложностей с их анализом.
- Определите допустимые правила формата архивов.
- Используйте функциональность подбора пароля к зашифрованным архивам и документам.

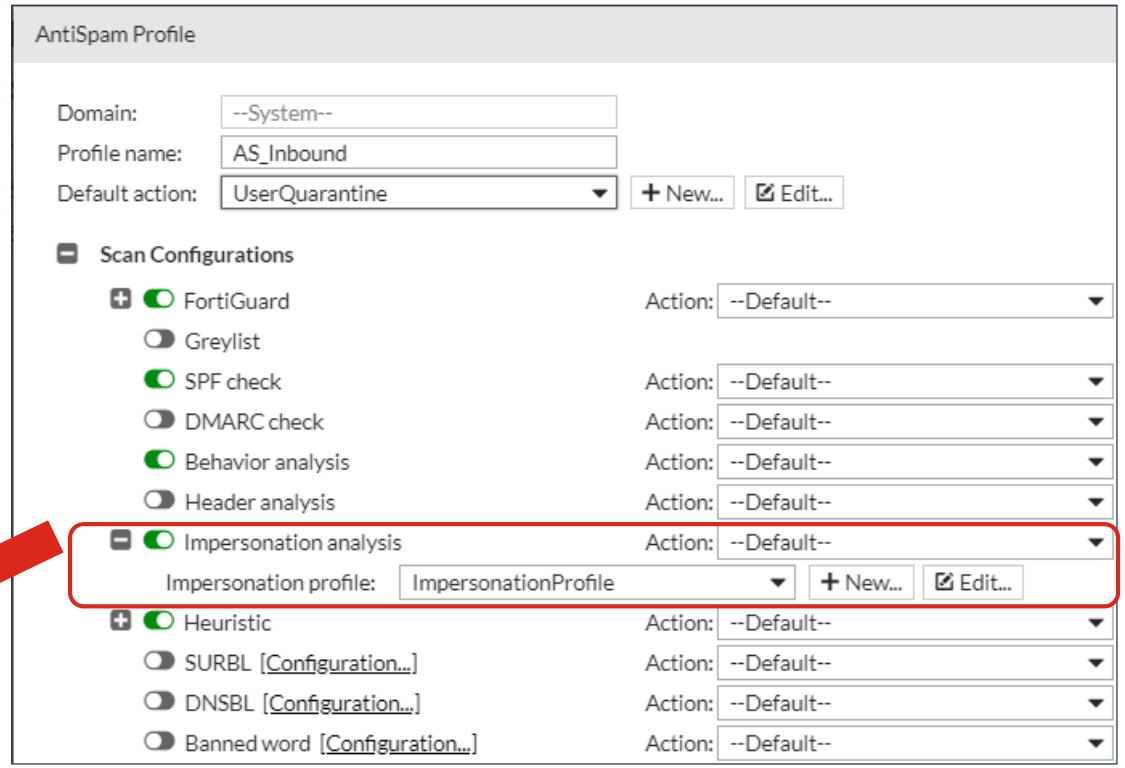


Защита от подмены отправителя

Impersonation analysis

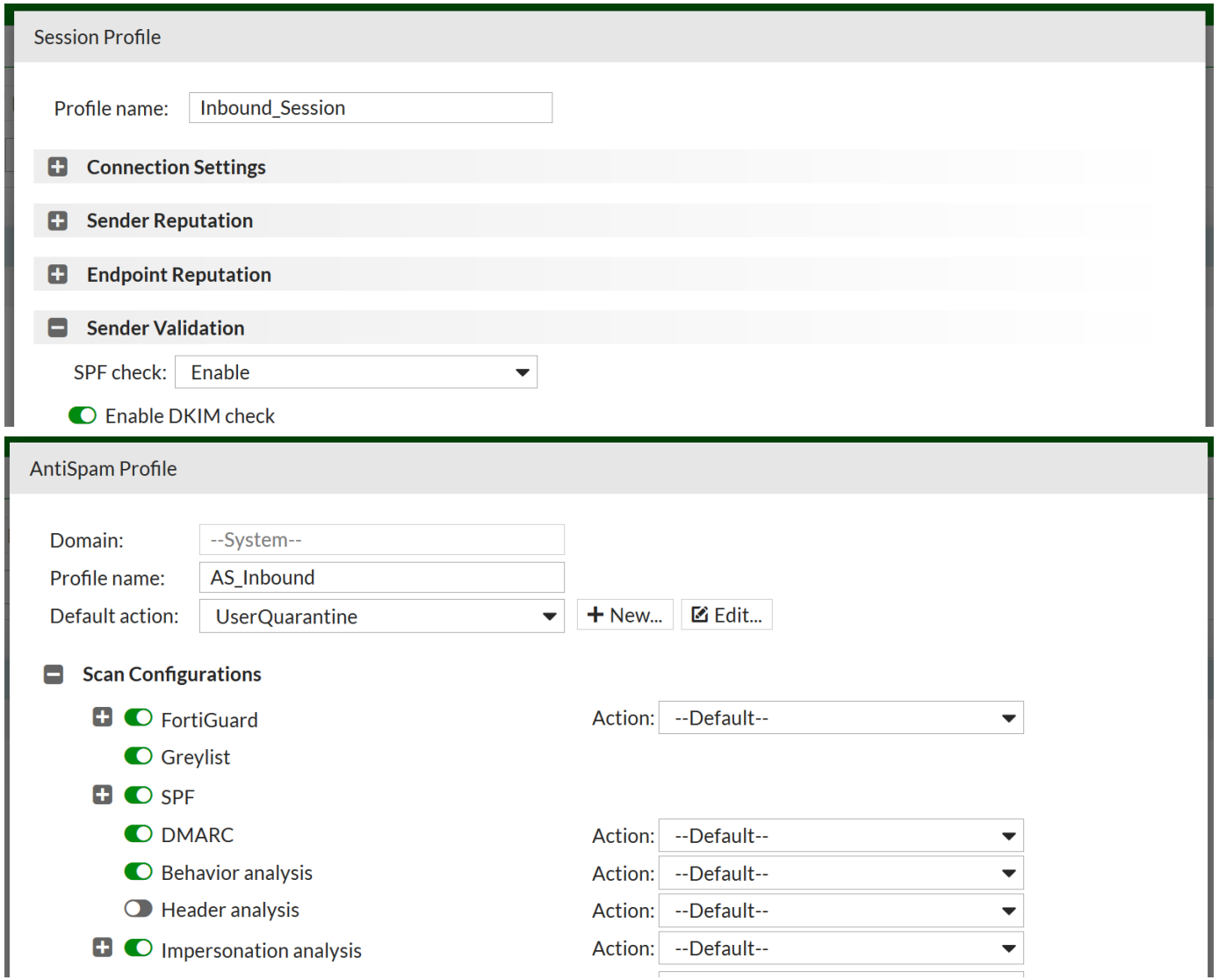
- Выявление маскировки отправителя под топ-менеджмент
  - » Идентификация нормальных соответствий имени и адреса в заголовке
  - » Выявление спуфинга во входящей почте
  - » Предупреждение получателя





Защита от подмены отправителя
Лучшая практика

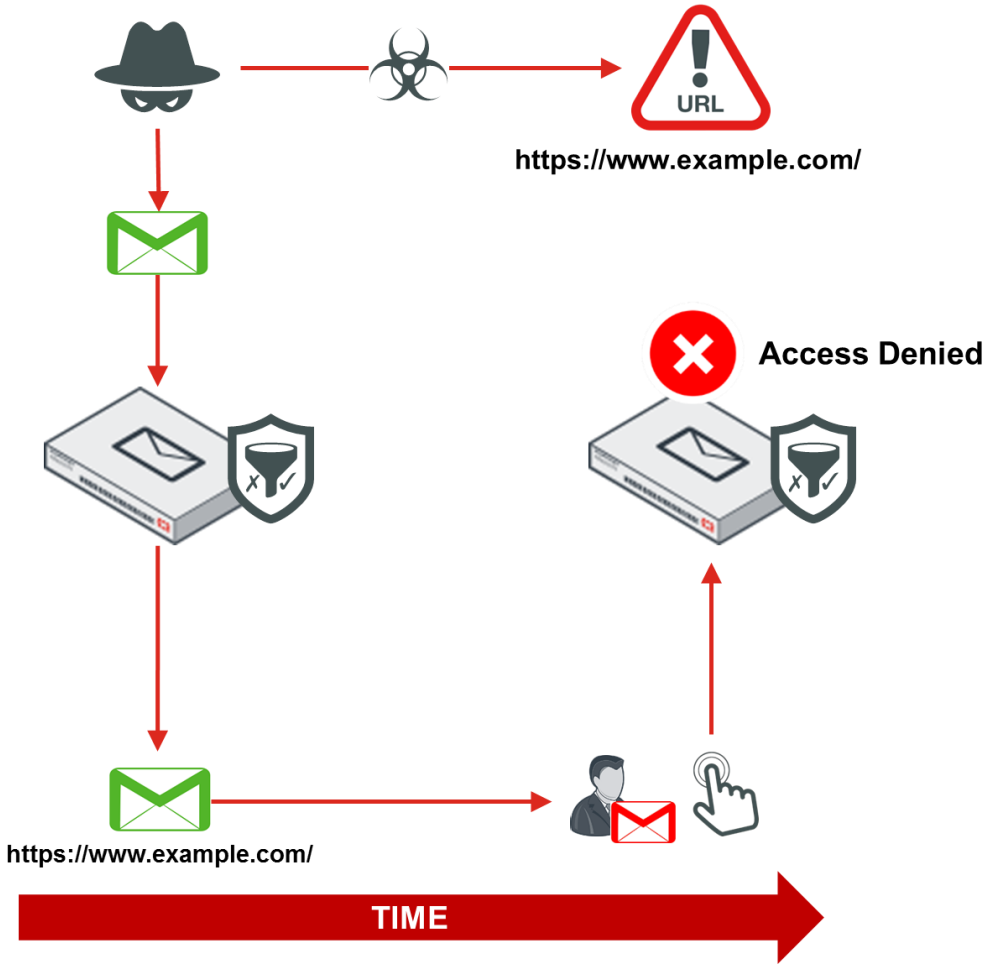
- Антиспуфинг - необходимая мера защиты от поддельных писем, в т.ч. от атак Business Email Compromise.
- Используйте SPF и другие доступные меры антиспуфинга.
- Session Profile: SPF, DKIM
- Antispam Profile: SPF, DMARC, Impersonation



FortiMail – обзор перспективных функций

Защита в момент клика

- Переписывание ссылки в момент анализа письма в FortiMail
- Ссылки ведут на специальный сервис на FortiMail, перенаправляющий пользователя по исходному адресу только если он не является подозрительным



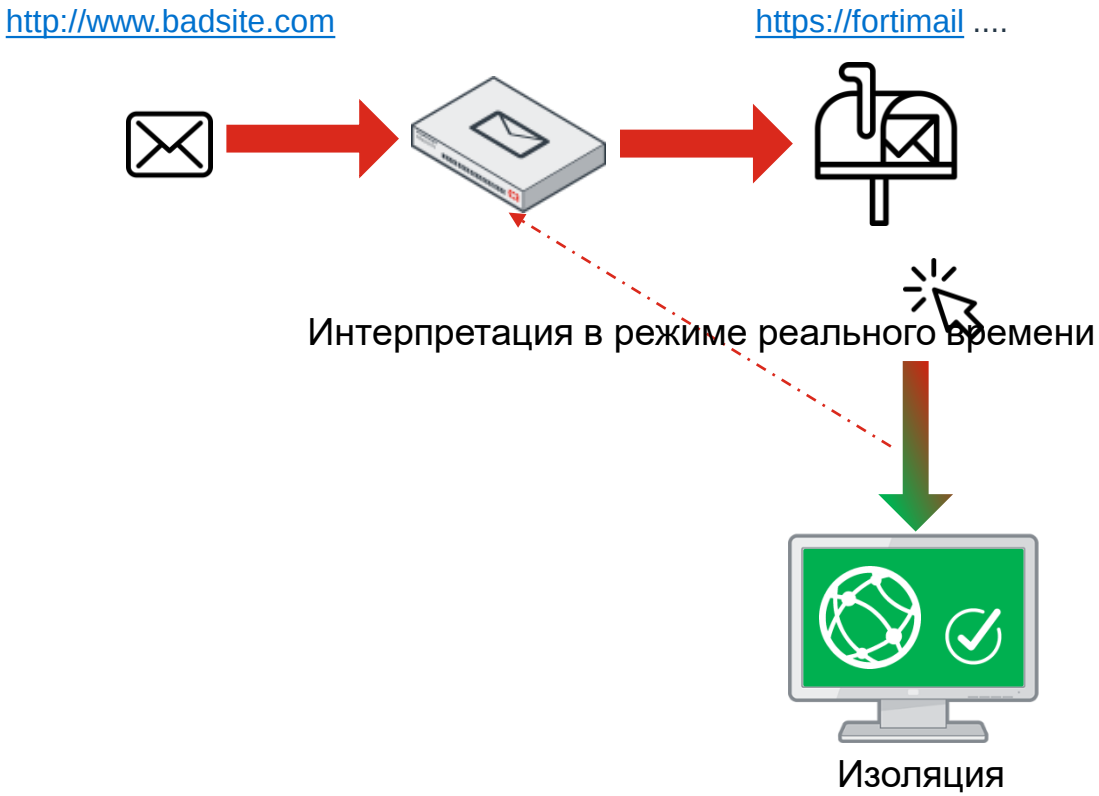
Защита в момент клика: регистрация кликов

Log Type	Date	Time ▲	Classifier	Dispositi...	From	Header F...	To	Subject	Client IP	Client Na...	Source	Message
Mail Event	2018-10-01	11:50:31.854										from=<yourfriend@gmail.com>, size=861, class=0, nrcpts=1, msgid=...
AntiSpam	2018-10-01	11:50:32.190			yourfrien...		a@a.com	test Mon, ...	10.0.0.66			Detected by Attachment Filter. Content disarm
History	2018-10-01	11:50:32.191	Attachme...	Modify S...	yourfrien...	yourfrien...	a@a.com	test Mon, ...	10.0.0.66		External	
Mail Event	2018-10-01	11:50:32.226										STARTTLS=client, relay=a.com., version=TLSv1.2, verify=OK, cipher...
Mail Event	2018-10-01	11:50:32.568										to=<a@a.com>, delay=00:00:01, xdelay=00:00:00, mailer=esmtp, pri...
AntiSpam	2018-10-01	12:07:08.043					a@a.com			10.0.0.1		URI Protect Passed: received at Mon, 01 Oct 2018, received categor...
AntiSpam	2018-10-01	12:09:47.317					a@a.com			10.0.0.1		URI Protect Blocked: received at Mon, 01 Oct 2018, category: 37, cli...
AntiSpam	2018-10-01	12:10:01.653					a@a.com			10.0.0.1		URI Protect Passed: received at Mon, 01 Oct 2018, received categor...

Date=2018-10-01
Time=12:10:01.653
To=a@a.com
Client Name=10.0.0.1
Message=URI Protect Passed: received at Mon, 01 Oct 2018, received category: 36, clicked category: 36, http://www.cnn.com
Session ID=w919oV12004663-w919oV13004663

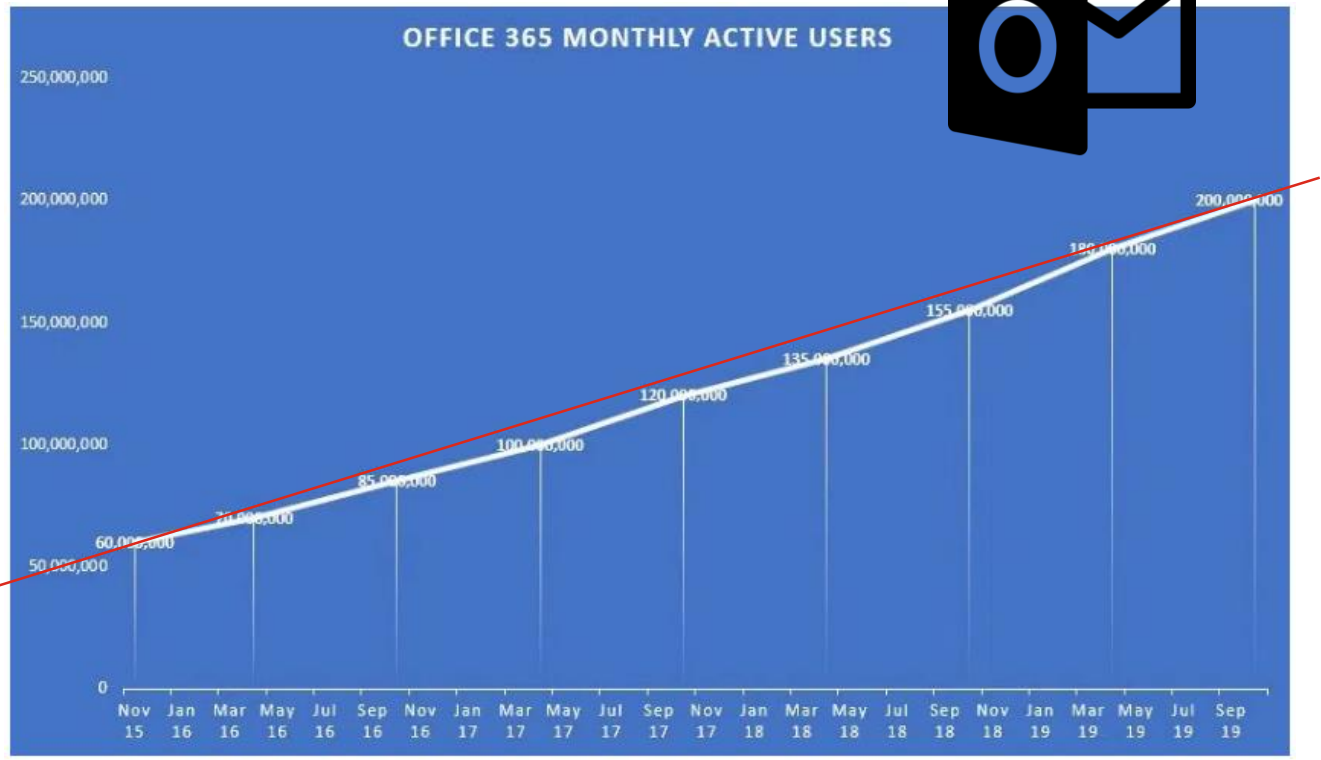
Защита от продвинутых угроз: интеграция с FortiIsolator

- FortiIsolator
  - Бесклиентский удаленный браузер
  - Сокрытие информации о пользователе от злоумышленников
- Может применяться совместно с защитой в момент клика
- Переписывание ссылок в теле письма для перенаправления на сервис



Office 365

- **Электронная почта - основной повод миграции пользователей офисного пакета в облако**
  - Применение продолжает расти
- **Специализированное средство защиты эффективнее встроенных в O365 защитных мер**
  - Более 50% организаций, использующих O365, применяют для защиты специализированный шлюз SEG (Gartner)
- **FortiMail для O365:**
  - Лучшая защита и видимость
  - Извлечение подозрительных писем



TOTAL ACCURACY RATINGS			
	Total Accuracy Rating	Total Accuracy (%)	Award
Symantec Email Security .cloud with ATP	2,932	98%	AAA
Proofpoint Essentials Advanced	2,926	98%	AAA
Fortinet FortiMail Cloud - Gateway Premium	2,804	93%	AAA
Microsoft Office 365 Advanced Threat Protection	1,050	35%	B
Microsoft Office 365	246	8%	

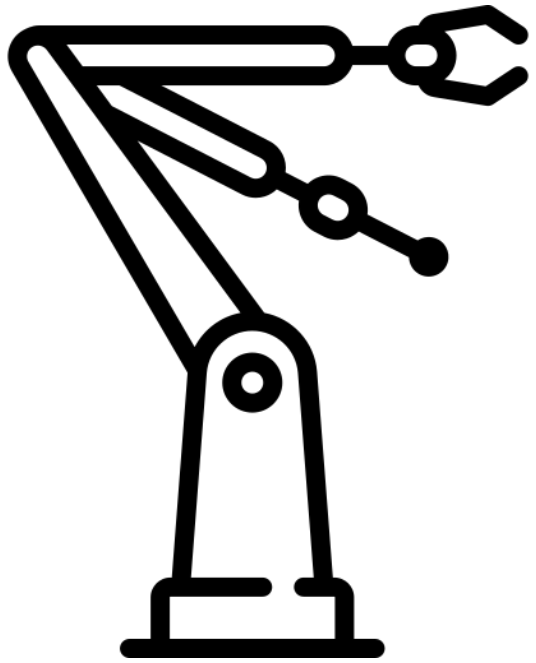
https://selabs.uk/en/reports/enterprise

Office 365

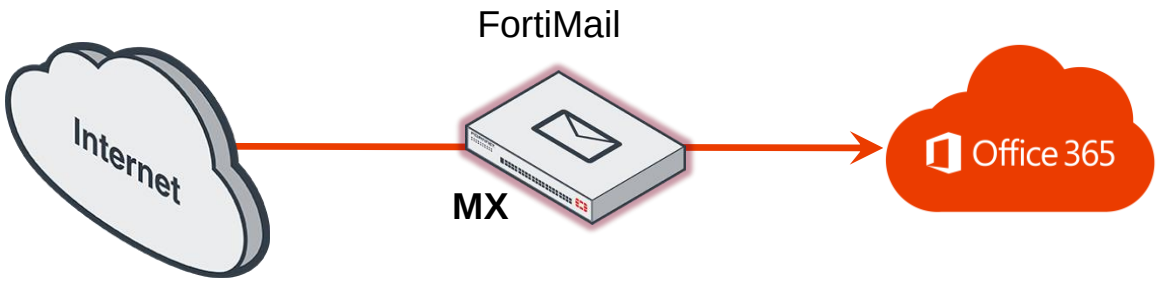
Интеграция по API

New

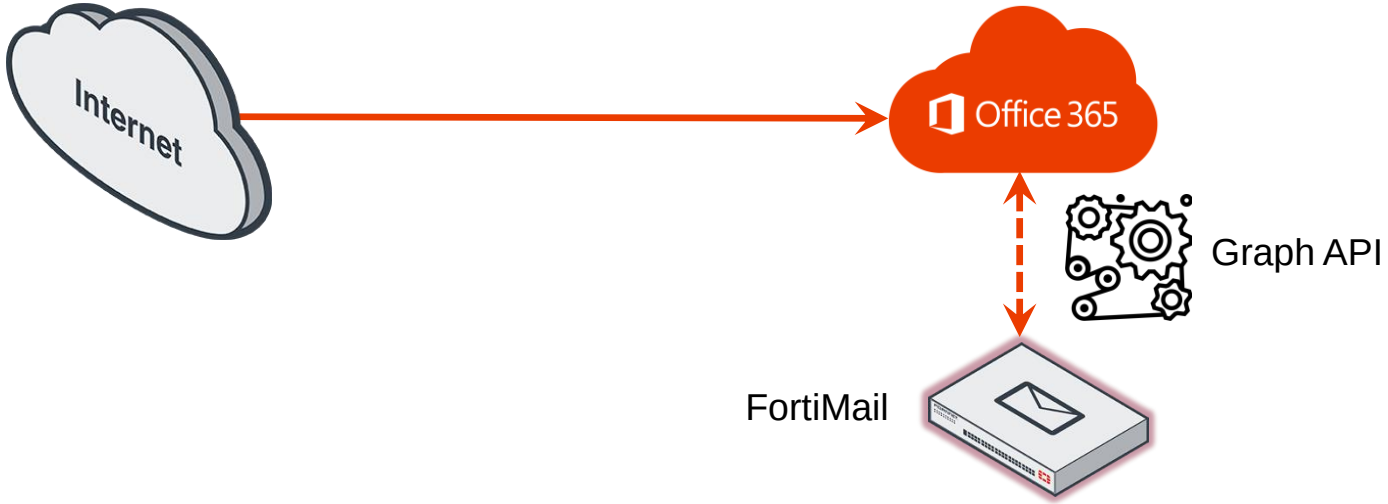
- **Специализированное средство защиты эффективнее встроенных в O365 защитных мер**
  - Более 50% организаций, использующих O365, применяют для защиты специализированный шлюз SEG (Gartner)
- **FortiMail для O365:**
  - Лучшая защита и видимость
  - Извлечение подозрительных писем
- Функция доступна в FML 400F/VM02 или выше



Архитектура интеграции с Office 365



В разрыв



Внеполосно

Остались вопросы?

email: cis_se@fortinet.com