

Технические аспекты защиты от спама

Павел Нагаев

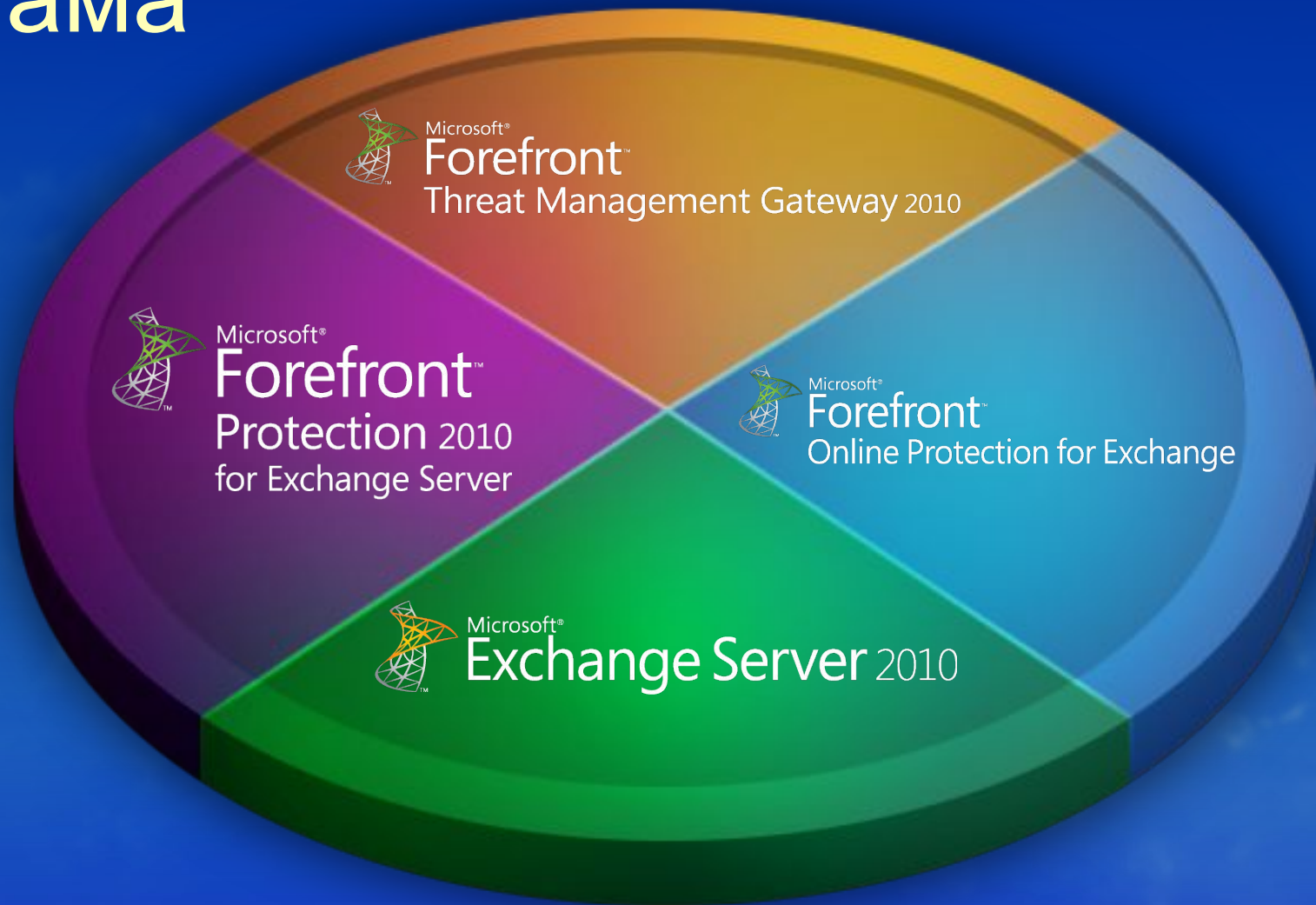
MCSE, MCITP, MVP Exchange

КТК-Р

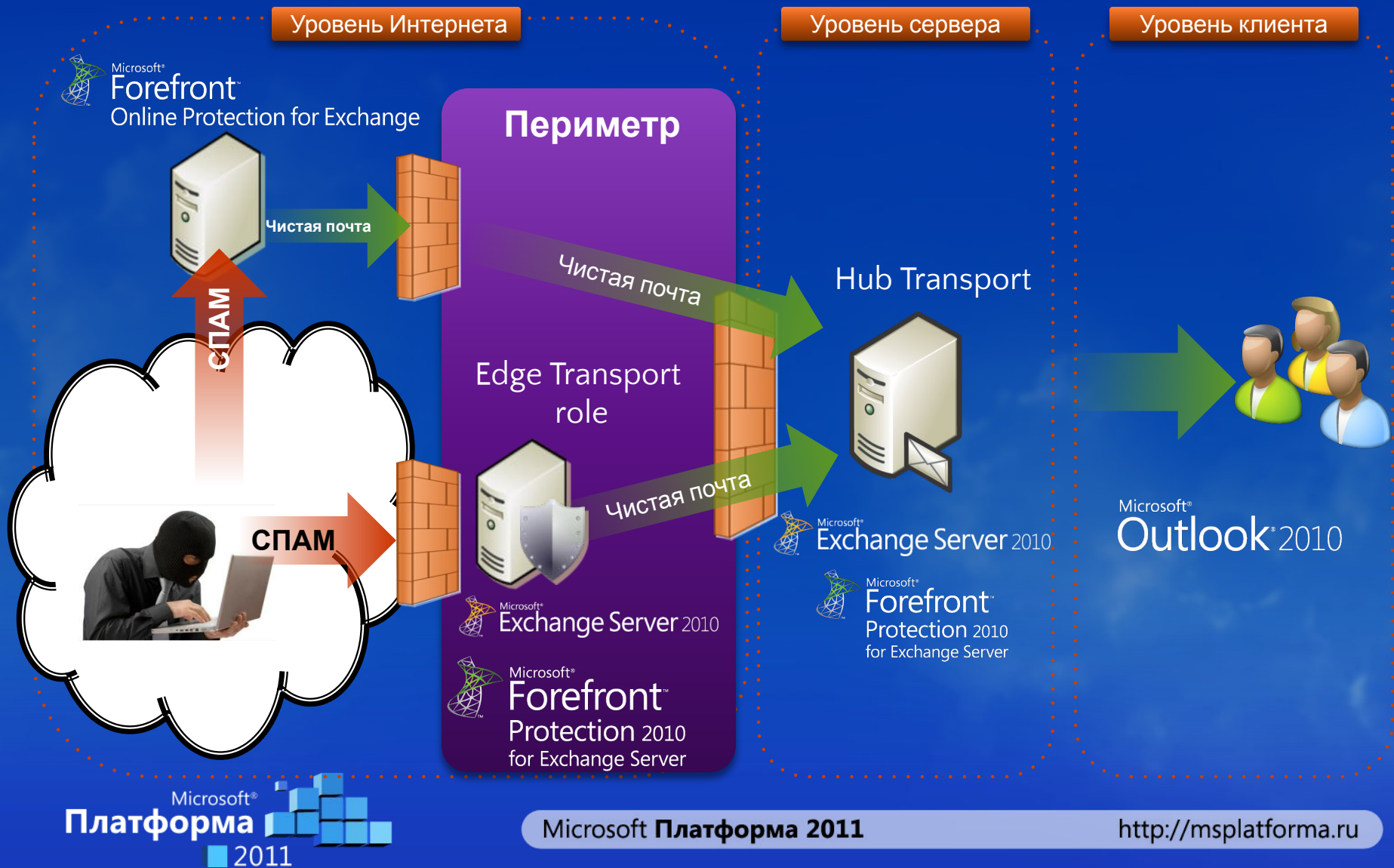
Содержание

- Краткий обзор продуктов защиты от спама
- Архитектура защиты
- Обзор Forefront Protection 2010 for Exchange Server
- Алгоритм работы спам-фильтров
- Общие рекомендации по настройке
- Итоги
- Вопросы (теле-мост)

Интегрированная защита от спама



Архитектура защиты от спама



Forefront Protection 2010 for Exchange Server

Exchange
2010

+ Forefront
Protection 2010

Преимущества



Microsoft®
Forefront
Protection 2010
for Exchange Server

Уровень
источника

Forefront DNS Block
List

- Собирает данные о DNS с нескольких провайдеров (Spamhaus.org, Forefront Online Protection for Exchange, Hotmail и т.д.)
- Не требует конфигурирования. «Включил, работает»

Уп
р
а
в

Уровень
протокола

Общее управление

- Фильтры отправителя/получателя/SenderID управляются из одной консоли

л
е

Anti-Backscatter

- Блокирует спам в NDR

н
и

Фильтр Cloudmark

- Альтернативный контент-фильтр от стороннего производителя
- Блокирует 99% спама; ложные срабатывания 0.004%
- Не требует конфигурирования. «Включил, работает»

е
F

Фильтрация файлов

- Проверяет тип файла по сигнатуре, а не по расширению
- Может помечать и удалять файлы внутри ZIP/RAR

or

Глобальный список
исключений

- Единая точка управления списком исключений для отправителей и получателей

ef

ro

nt

и

з
о

Консоль управления

Централизованное управление серверами Exchange 2010 Hub и Edge, FPE 2010 и FOPE

Отчеты о спаме

Управление настройками антивируса и спам-фильтра

Antispam - Configure

Connection Filter

- ☒ Enable Connection filtering
- Note: The Microsoft Exchange Transport service must be restarted for changes to this setting to take effect.
- ☐ Enable Forefront DNSBL checking
- ☒ Enable IP block list evaluation
- ☐ Enable IP allow list evaluation
- [Configure Allow/Block Lists...](#)

Sender ID Filter

- ☒ Enable SenderID filtering
- Upon failed Sender ID verification:
 - ☒ Reject message
 - ☐ Stamp header and continue processing
 - ☐ Delete message

Sender Filter

- ☐ Enable sender filtering
- ☐ Block messages with an empty sender address
- [Configure Sender Lists...](#)

Recipient Filter

- ☐ Enable recipient filtering
- ☐ Only accept messages to valid recipients from the Global Address List
- [Configure Recipient Lists...](#)

Backscatter Filter

- ☐ Enable backscatter filtering
- Note: The Microsoft Exchange Transport service must be restarted for changes to this setting to take effect.
- [Configure Backscatter Lists...](#)
- Backscatter Keys last generated: No date available
- [Generate](#) [Import Keys...](#) [Export Keys...](#)

Content Filter

- ☒ Enable content filtering
- Note: The Microsoft Exchange Transport service must be restarted for changes to this setting to take effect.
- ☐ Report statistical data to third-party engine provider

Server Security Views - Spam Details

View detailed spam detection statistics by antispam component.

Connection Filtering

Action	Count
Messages processed by connection filtering	3752
Messages blocked by IP block list	2
Messages blocked by DNS block list	2958

SMTP Filtering

Action	Count
Messages processed by SMTP filtering	792
Messages blocked by sender filtering	0
Messages blocked by sender ID filtering	0
Messages blocked by recipient filtering	474

Content Filtering

Action	Count
Messages processed by content filtering	318
Messages rejected by content filtering	74
Messages deleted by content filtering	0
Messages quarantined by content filtering	0

Backscatter Filtering

Action	Count
Messages processed by backscatter filtering	8
Messages blocked by domain rejection list	0
Messages allowed by domain exclusion list	0
Messages blocked by backscatter agent	4

Transport Spam Blocking Summary

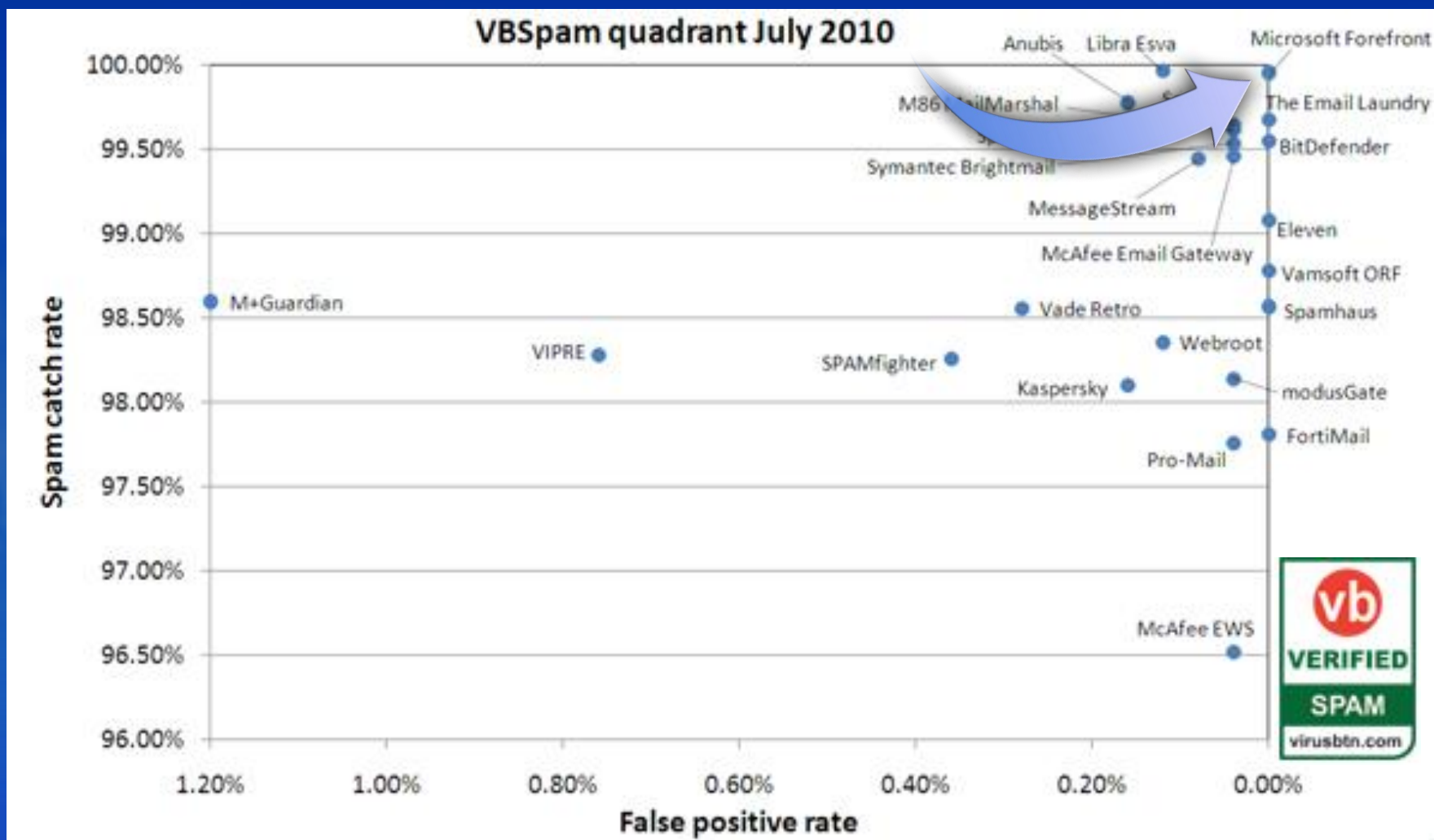
Last updated: 15.11.2010 15:40:55
Total blocked messages: 3514

Legend:

- Connection: 2962
- SMTP: 474
- Content: 74
- Backscatter: 4

Total: 3514

Virus Bulletin (Июль 2010)



Транспортные агенты FPE 2010

```
Machine: TMG-SITE-A | Scope:

[PS] C:\Windows\system32>Get-TransportAgent

Identity                                     Enabled      Priority
-----
FSE Batv Receive Agent                     True         1
Connection Filtering Agent                 True         2
Address Rewriting Inbound Agent            True         3
Edge Rule Agent                           True         4
Content Filter Agent                      False        5
Protocol Analysis Agent                   True         6
Attachment Filtering Agent                True         7
Address Rewriting Outbound Agent           True         8
FSE Routing Agent                         True         9
Sender Id Agent                          True        10
Sender Filter Agent                      True        11
Recipient Filter Agent                   True        12
FSE Connection Filtering Agent            True        13
FSE Content Filter Agent                 True        14
FSE Batv Routing Agent                   True        15

[PS] C:\Windows\system32>
```

Спам-фильтры Forefront Protection 2010 for Exchange Server

1

Уровень соединения

- Списки IP Allow/Deny
- Блок-листы Forefront DNSBL/ 3-х фирм

2

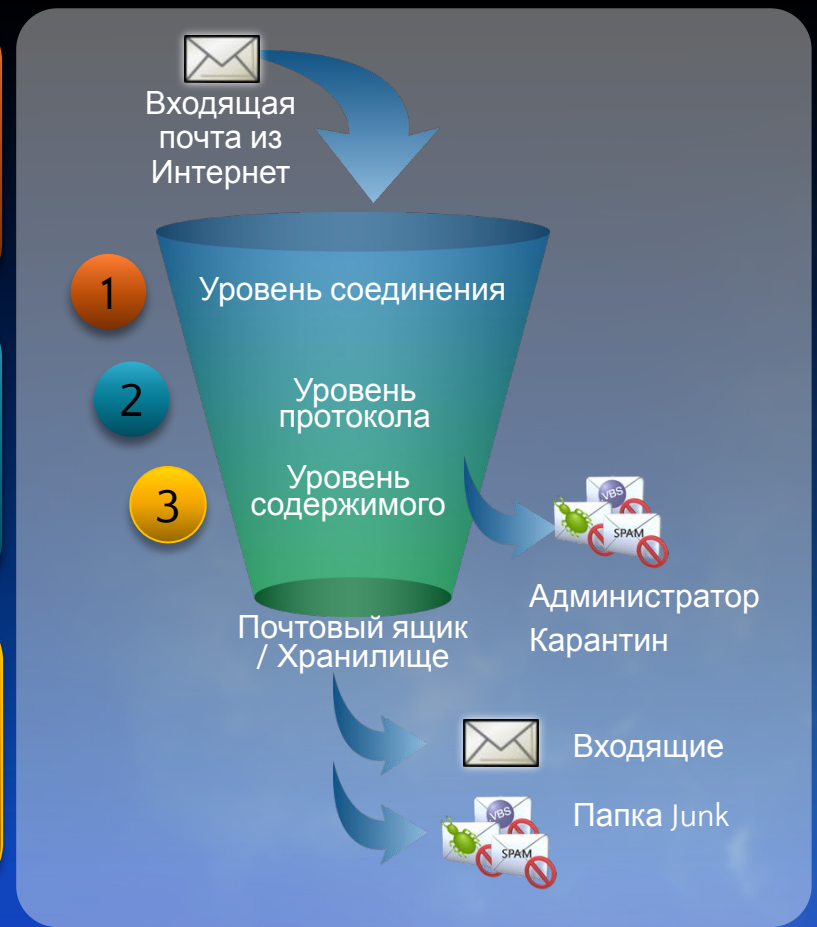
Уровень протокола

- Фильтры отправителя/получателя
- Sender ID
- Списки доверенных отправителей
- Фильтр Backscatter

3

Уровень содержимого

- Фильтр Cloudmark
- Анализ протокола
- Отпечатки
- SMTP Carving
- Анти-фальшинг Edge Synchronizer
- Message submission rate (per IP)



Фильтрация на уровне соединения



Как работает DNS Block List

IP спам-сервера: 109.195.41.161

```
C:\>nslookup 161.41.195.109.zen.spamhaus.org
Server:  dns.exchangerus.ru
Address:  10.10.10.10
```

```
Non-authoritative answer:
Name:      161.41.195.109.zen.spamhaus.org
Address:   127.0.0.11
```



```
C:\>nslookup 85.78.15.152.zen.spamhaus.org
Server:  dns.exchangerus.ru
Address:  10.10.10.10
```

```
*** dns.exchangerus.ru can't find
85.78.15.152.zen.spamhaus.org: Non-existent domain
```

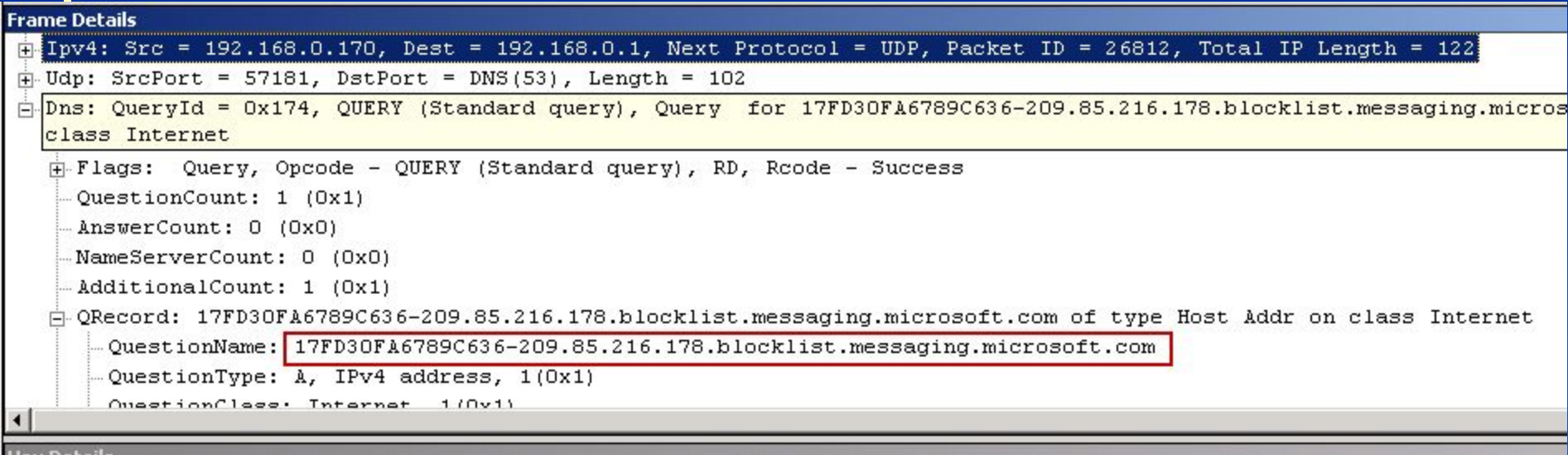
Ответы Forefront DNS Block List

550 5.7.1 :127.0.0.10:Client host 109.195.41.161 blocked using 87.blocklist.zap; Mail from IP banned. To request removal from this list please visit [http://www.spamhaus.org/query/bl?ip=\\$](http://www.spamhaus.org/query/bl?ip=$)

550 5.7.1 :127.0.0.5:Client host 113.160.112.120 blocked using 88.blocklist.zap; Mail from IP banned. To request removal from this list please forward this message to delist.forefront@messaging.microsoft.com

Возвращает	Код	Описание
127.0.0.2	SBL Spamhaus	SBL Data
127.0.0.3	SBL Spamhaus	SBL CSS Data
127.0.0.4	XBL CBL	Data
127.0.0.5	XBL Customized	NJABL Data
127.0.0.10	PBL ISP	Maintained
127.0.0.11	PBL Spamhaus	

Запрос ForeFront DNS Block



IP адрес сервера: 209.85.216.178



Запрос в DNS: 17FD30FA6789C636-209.85.216.178.blocklist.messaging.microsoft.com

Хеш

IP

DNS имя сервера

Уровень соединения

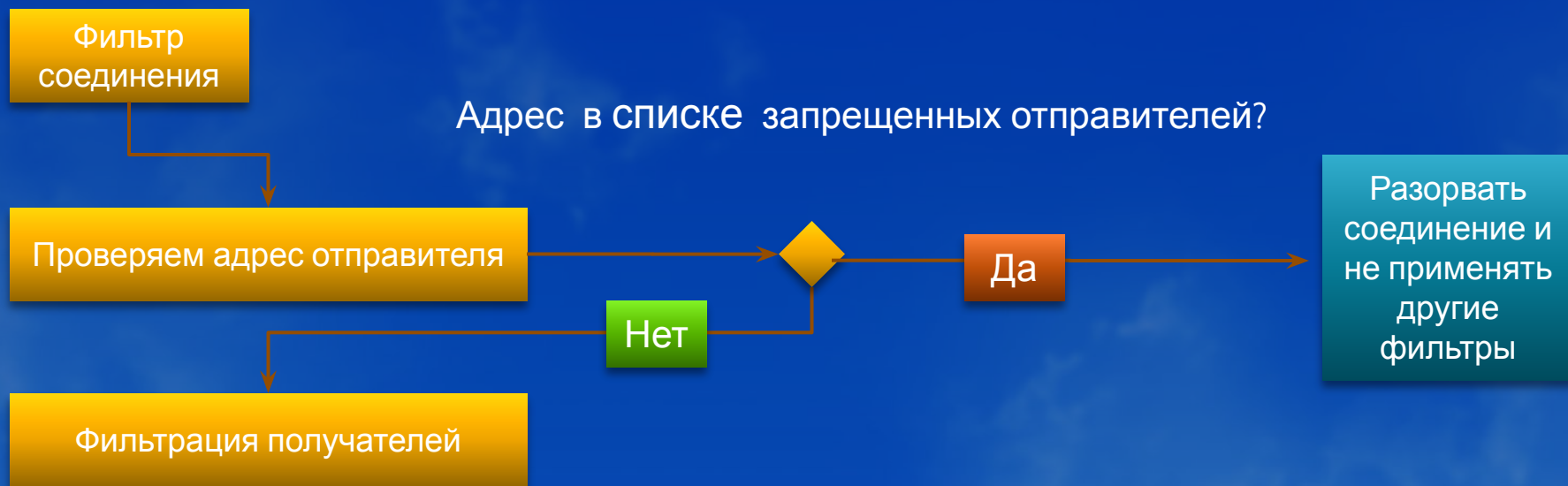
- Плюсы

- Экономия на трафике (*разрыв соединения на уровне SMTP*)
- Блокировка конкретного спам-сервера или сбойного сервера
- Комментарий и время жизни (EMS)
- Включение Forefront DNSBL одним нажатием

- Минусы

- Ручная настройка и разрастание списков
- Ошибочное попадание отправителей в списки спам серверов
- Неграмотность пользователей

Схема фильтрации отправителей



Синхронизация EdgeSync

E2007:
Safe
Senders List
+
E2010:
Blocked
Senders List



E2010: Автоматическое обновление = 30 секунд

E2007: Ручное обновление = до 4 часов



Mailbox role



Domain Controller

E2010: EDGE SYNCH = 30 сек

E2007: Полная AD синхронизация на Edge = до 4 часов



Edge Server

Белые и черные списки отправителей синхронизируются на Edge сервер за секунды

Фильтрация отправителей

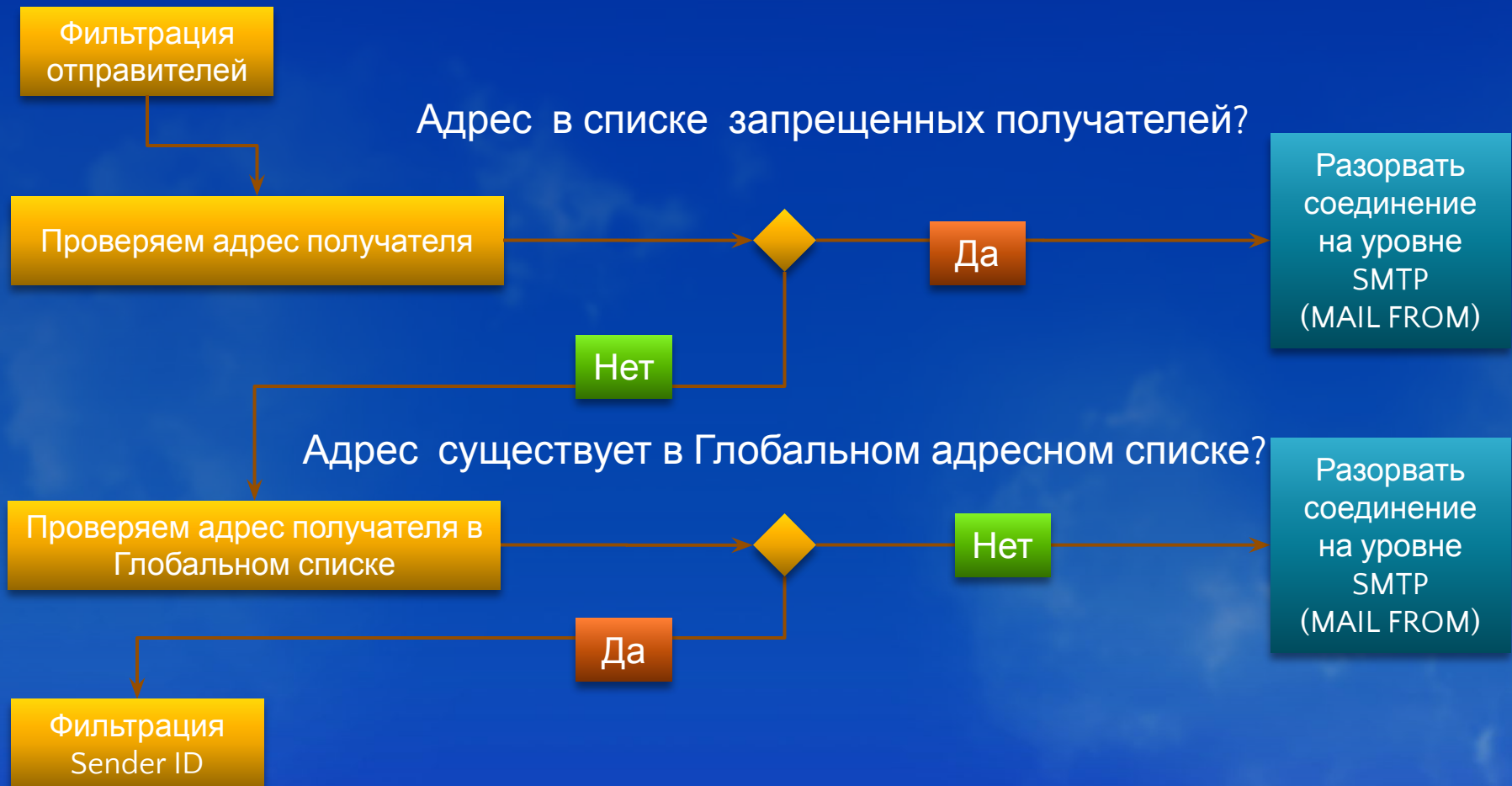
- Плюсы

- Возможность заблокировать рассылки или «настойчивых» пользователей

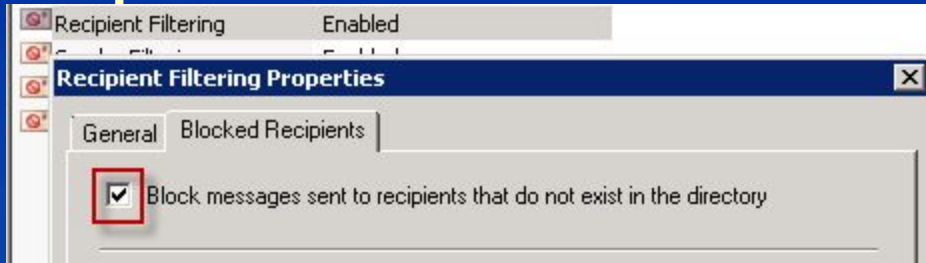
- Минусы

- Легко подделать отправителя
 - Нет возможности добавить комментариев
 - Ограничение по количеству записей

Фильтрация получателей



Режим замедления ответов SMTP (Tarpit)



```
1 Client: MAIL FROM: spammer@anydomain.com
2 Server: 250 2.1.0 spammer@anydomain.com....Sender OK
3 Client: RCPT TO: pavel.nagaev@exchangerus.ru
4 Server: 250 2.1.5 pavel.nagaev@exchangerus.ru
5 Client: RCPT TO: pavel.nagaev001@exchangerus.ru
6 Server: 550 5.5.1 User Unknown
```

- Предотвращает Directory Harvesting Attack (DHA) – подбор «живых» адресов
- Tarpit интервал равен 5 секундам по умолчанию

Фильтрация получателей

- Плюсы

- Запрет приема сообщений для определенных пользователей
- Принимать сообщения для существующих получателей

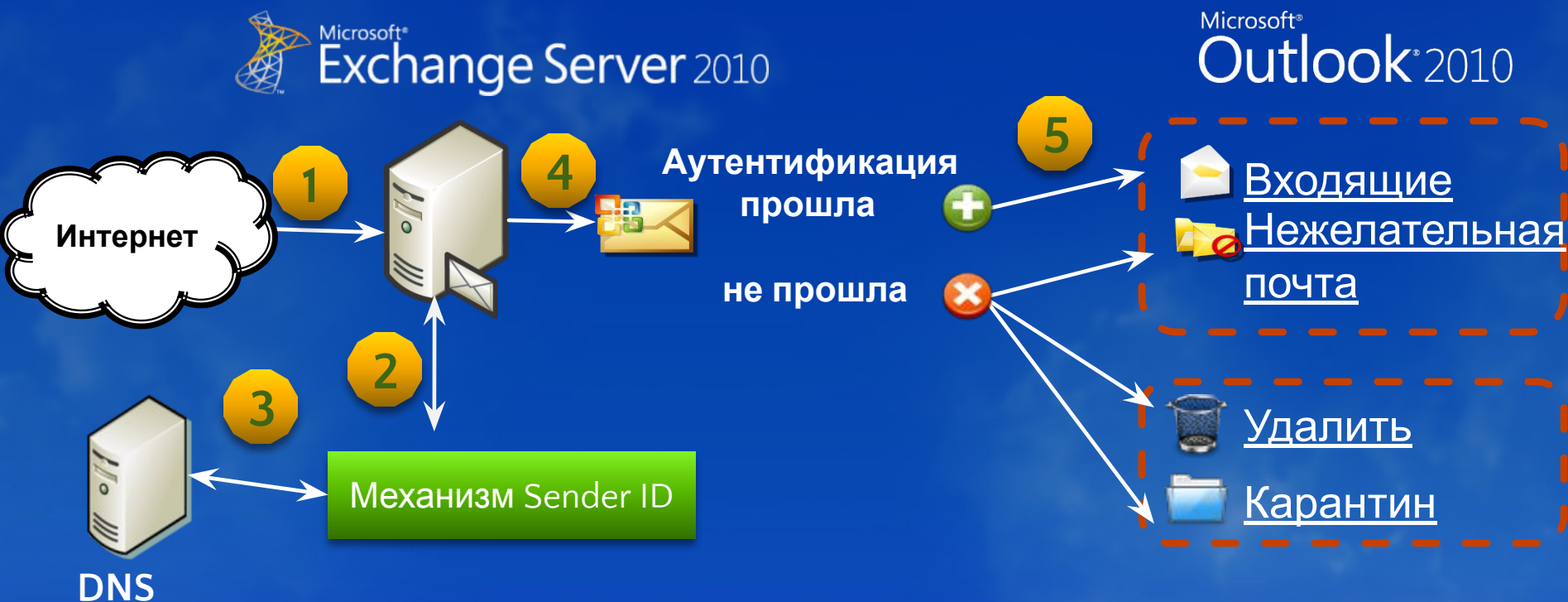


- Минусы

- Подбор адресов электронной почты

Уровень протокола. Код отправителя

exchangerus.ru. IN TXT "v=spf1 ip4:85.111.10.40 +a:smtp.exchangerus.ru -all"



Код отправителя (Sender ID)

- Плюсы
 - Идентификация сервера отправителя
 - Не нужно проверять MX
 - FPE действует только наверняка
- Минусы
 - Пересылка почты на другой адрес (механизм forward)
 - Прием получателем почты через резервный почтовый сервер (backup MX)

Что такое Backscatter?

- Backscatter — NDR спам с подделанным адресом отправителя
- Bounce Address Tag Validation (BATV) — технология по защите от NDR спама

you@example.com



$prvs=F_{\text{ключ}}(\text{время жизни, адрес})=you@example.com$

Пример: $prvs=12we34fnr=you@example.com$

Механизм работы Anti-Backscatter



Внутренний
пользователь
(you@example.com)



FPE 2010



Сервер
получателя

1. Внутренний пользователь отправляет сообщение на корпоративный сервер
2. FPE 2010 добавляет хешированную метку к P1.MailFrom
3. Получатель не может доставить сообщение и возвращает его обратно
4. FPE 2010 просматривает метку
5. Если метка существует, то NDR будет доставлен пользователю

`<prvs=12we34fnr=you@example.com>`

Backscatter. Атака спамера



Внутренний
пользователь
(you@example.com)



FPE 2010



Сервер
получателя



Spammer

1. Спамер генерирует сообщение с фальшивым адресом в MAIL FROM <you@example.com> и посылает его на сервер.
2. Получатель не может доставить и должен послать NDR
3. FPE 2010 ищет хешированную метку
4. Если метки нет, то сообщение признается backscatter spam

Технология backscatter в FPE

- Используется два транспортных агента для анализа хешированной метки
- Метка содержит отправителя и время
- Backscatter начинает работать через 24 часа
 - accepted: in phase out period, BATV tag was not validated
 - rejecting: BATV tag validation failed, returning 550 response.
- 550 5.7.1 Request action not taken: message refused

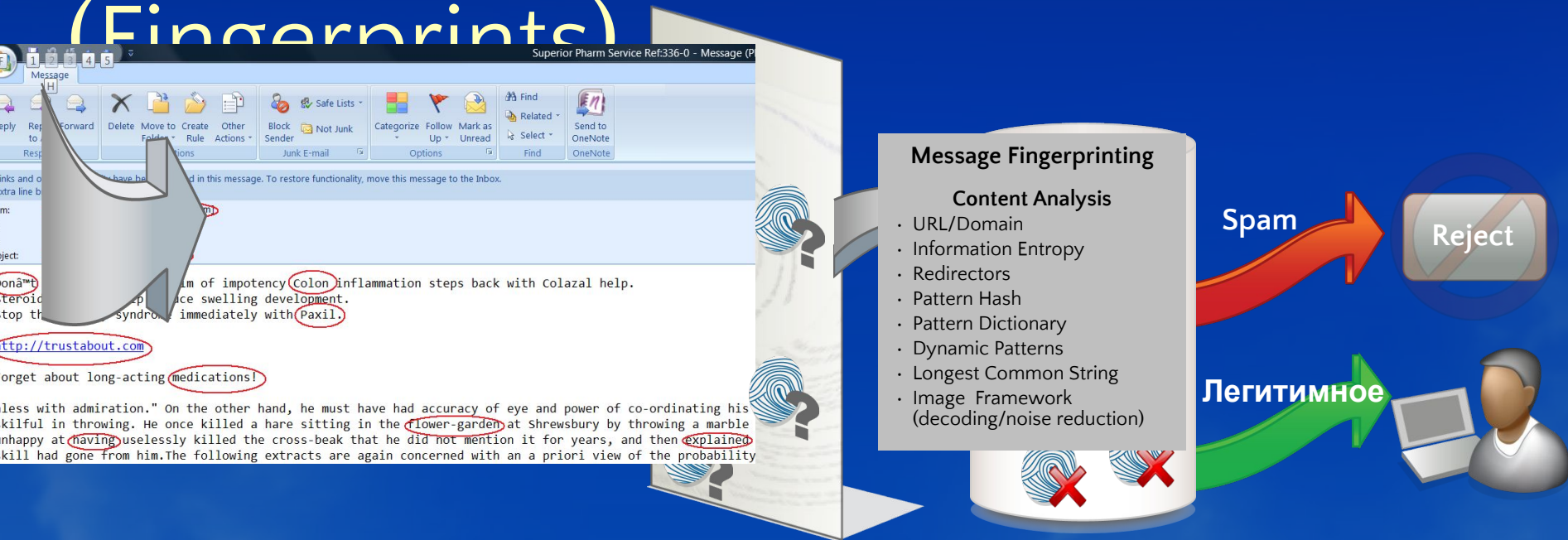
Фильтр содержимого



- Новый фильтр Cloudmark Authority Engine
- Изменены значений SCL

SCL	Определение
-1	Сообщения из доверенных источников или если в них спам не найден
0	Не используется, но можно включить
1- 4	Не используется
5 - 8	Менее 1% случаев
9	Однозначный спам, более 90% всех сообщений

Цифровые отпечатки (Fingerprints)



- Применяется к каждому входящему сообщению*
- Fingerprints не определяет относится письмо к спаму или нет
- Fingerprints сравниваются с локальным кэшем известных «спамовых» fingerprints

- Данные кэша обновляются каждые 45 секунд
- В случае совпадения письмо считается спамом
- В случае несовпадения запускается эвристика.
- Если не совпадает, то письмо считается

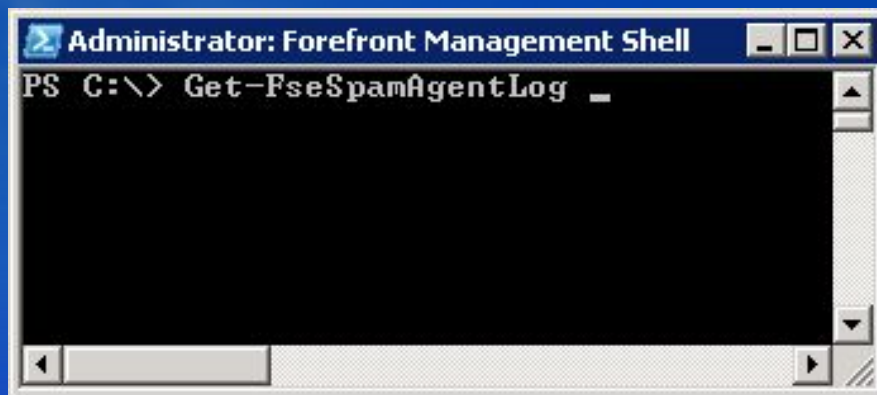
* Исключения: Safe Senders/Recipients/Safe Listed Ips и т.д.

Отчеты о работе спам-фильтров

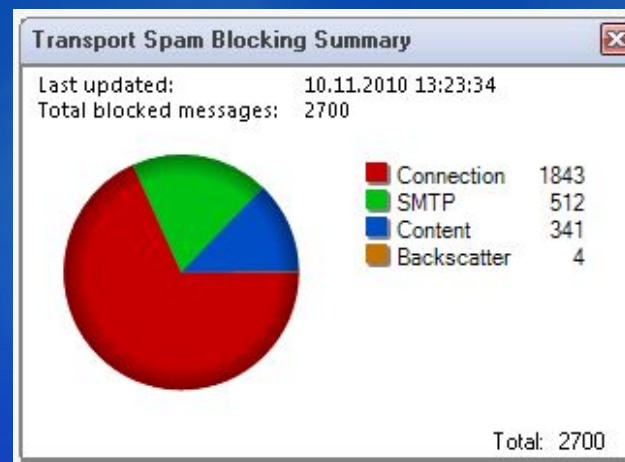
Заголовок письма

```
X-MS-Exchange-Organization-Antispam-Report: v=1.1  
cv=UmKbMGcK00DFGOVLbWSsnc4cSM78ciS0lL3oFpZVzQQ= c=1 sm=1  
a=gH2l33N09zgA:10  
a=xNkmr0qudcMA:10 a=jPJDAwAOAc8A:10 a=Fdkxr_5KmFUA:10  
a=ytB2GYGUEEAA:10  
a=ibi3b6Q5wLy8D8VTdfDbdA==:17 a=-OZdoqLpvXrLEne8aosA:9  
a=nb3xUh8hnMWWdIaeiJIBI77mBnsA:4 a=pvA44qeTxYYA:10  
a=ibi3b6Q5wLy8D8VTdfDbdA==:117;OrigIP:119.153.147.78;SCL:-1
```

PowerShell



Консоль Forefront



Рекомендации по защите от спама

- Правильная настройка почтовых серверов в DNS (A, PTR, MX, Sender ID)
- Проверка получателей в Active Directory
- Настройка интервала задержки (Tarpit)
- Запрет приема почты от «своего» домена
- Использование Forefront DNSBL
- Схема работы спам-фильтров
- Поиск заблокированных писем



Итоги

- Спам нельзя победить полностью, но с ним можно успешно бороться
- Защита должна быть многоуровневой
- Изменение психологии работы с почтой
- Борьба со спамом — соблюдение баланса
 - Эффективность или блокировка легитимных писем
 - Администратор или пользователь

Ресурсы

- Дополнительные сессии по теме
 - IS 303: Облачные технологии безопасности для компании (18/11, 13:00–14:00, Селигер)
 - СТ 304: Миграция на Exchange Server 2010: сценарии, рекомендации, практический опыт (18/11, 16:00–17:00, Зона интерактивных сессий)
- Блоги
 - <http://www.exchangerus.ru>
 - <http://blogs.technet.com/securityrus>

Официальные курсы и сертификация Microsoft

- Более 300 официальных курсов Microsoft доступно в России.
- Официальные курсы можно прослушать только в **авторизованных учебных центрах Microsoft**
 - под руководством опытного сертифицированного инструктора Microsoft
 - интенсивное обучение с акцентом на практику
 - более 80-и учебных центров более чем в 20-и городах России (+ дистанционные и выездные курсы)
- **Сертификат Microsoft** – показатель квалификации ИТ-специалиста для работодателя.
- Microsoft предлагает **гибкую систему сертификаций**.

40%

Доказательство № 75

сертифицированных специалистов считают, что сертификация помогла им получить работу или повышение

57%

Доказательство № 119

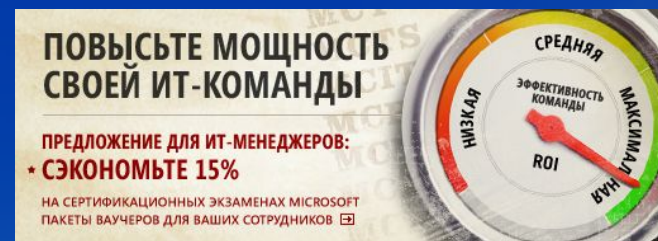
рекрутеров считают сертификацию сотрудников одним из критериев для повышения в должности

- Все курсы, учебные центры и центры тестирования:
www.microsoft.com/rus/learning



Специальные предложения

- **Сертификационный пакет со вторым шансом**
 - Пакеты экзаменационных ваучеров со скидкой от 15 до 20% и бесплатной пересдачей («вторым шансом»). Все экзамены сдаются одним человеком.
- **Сэкономьте 15% на сертификации вашей ИТ-команды**
 - Пакет из 10-и экзаменационных ваучеров со скидкой 15% для сотрудников ИТ-отдела. «Второй шанс» включен. Ваучеры можно произвольно распределять между сотрудниками.
- **Microsoft Certified Career Conference**
 - Первая 24-часовая глобальная виртуальная конференция с 18 ноября с 15.00 (моск. время) по 19 ноября 2010 г.
 - Сессии по технологиям и построению карьеры
 - Скидка 50% для сертифицированных специалистов Microsoft и студентов
- **Бесплатная подписка на TechNet для слушателей официальных курсов**
 - Некоторые курсы по SharePoint, Windows 7; Windows Server 2008; SQL Server 2008
- **Детали: www.microsoft.com/rus/learning**



**С 22 ноября 2010 г. –
подписка TechNet бесплатно
для слушателей курсов.
Количество ограничено!**

Обратная связь

Ваше мнение очень важно для нас.
Пожалуйста, оцените доклад, заполните
анкету и сдайте ее при выходе из зала

Спасибо!

Вопросы

- IS 302
- **Павел Нагаев**
 - Ведущий администратор системы электронной почты, КТК-Р
 - pan@exchangerus.ru
 - <http://www.exchangerus.ru>
- Вы сможете задать вопросы докладчику в зоне «Спроси эксперта» в течение часа после завершения этого доклада

