Cisco Email Security:
Лучшие практики и тонкая настройка

Pavel Rodionov
CSE Security, Cisco GSSO Ukraine
5 июня 2018

Программа

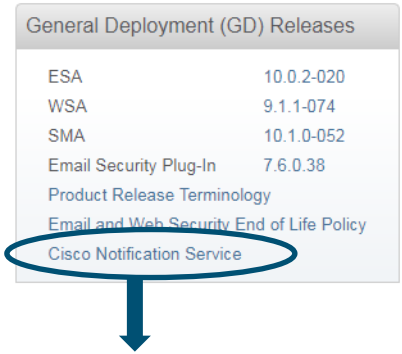
- Введение
- Понимание процесса Email Pipeline
- Настройка Anti-Spam
- Обнаружение спуфинга и фишинга
- Контроль и защита присоединенных файлов
- Мониторинг и инструменты
- Подведение итогов

Введение...

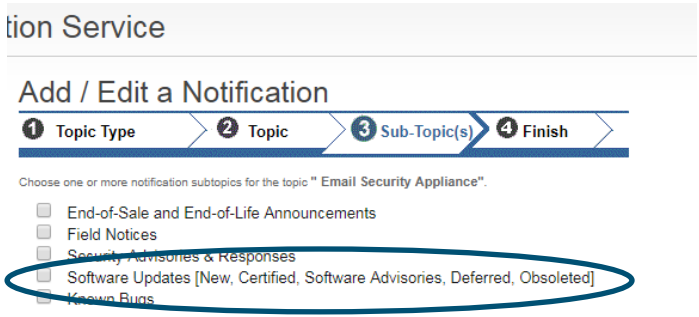
Pavel Rodionov

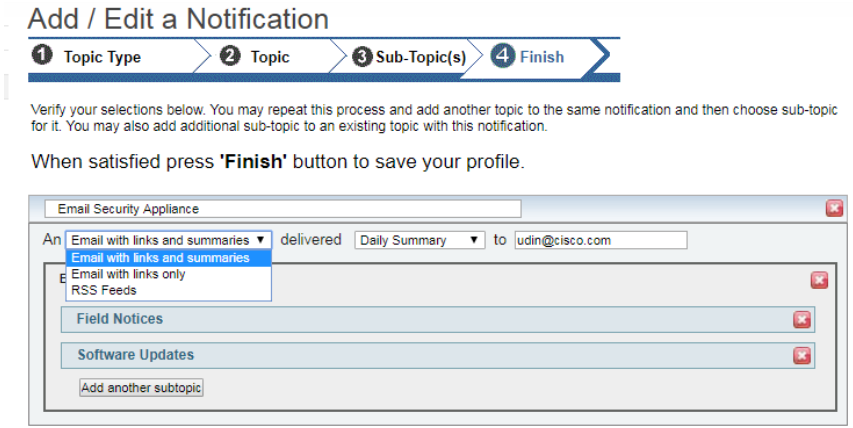
- Consulting Systems Engineer, Cisco Security
- Joined Cisco February, 2008
- Раньше работал в Ironport
- Over 20+ years industry experience in Networking and Security
- CCIE# 11155 (Routing and Switching)
- Based out of Ukraine, cover CIS region

Перед тем, как мы начнем, какая у вас версия?



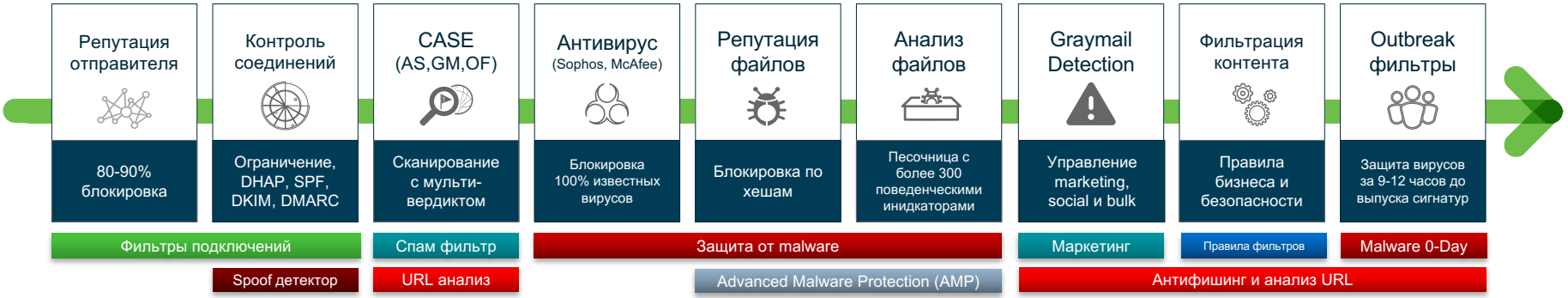
- Существующая версия GA 11.1.0-135
- Не получаете уведомлений о новых версиях? https://supportforums.cisco.com/community/5756/email-security



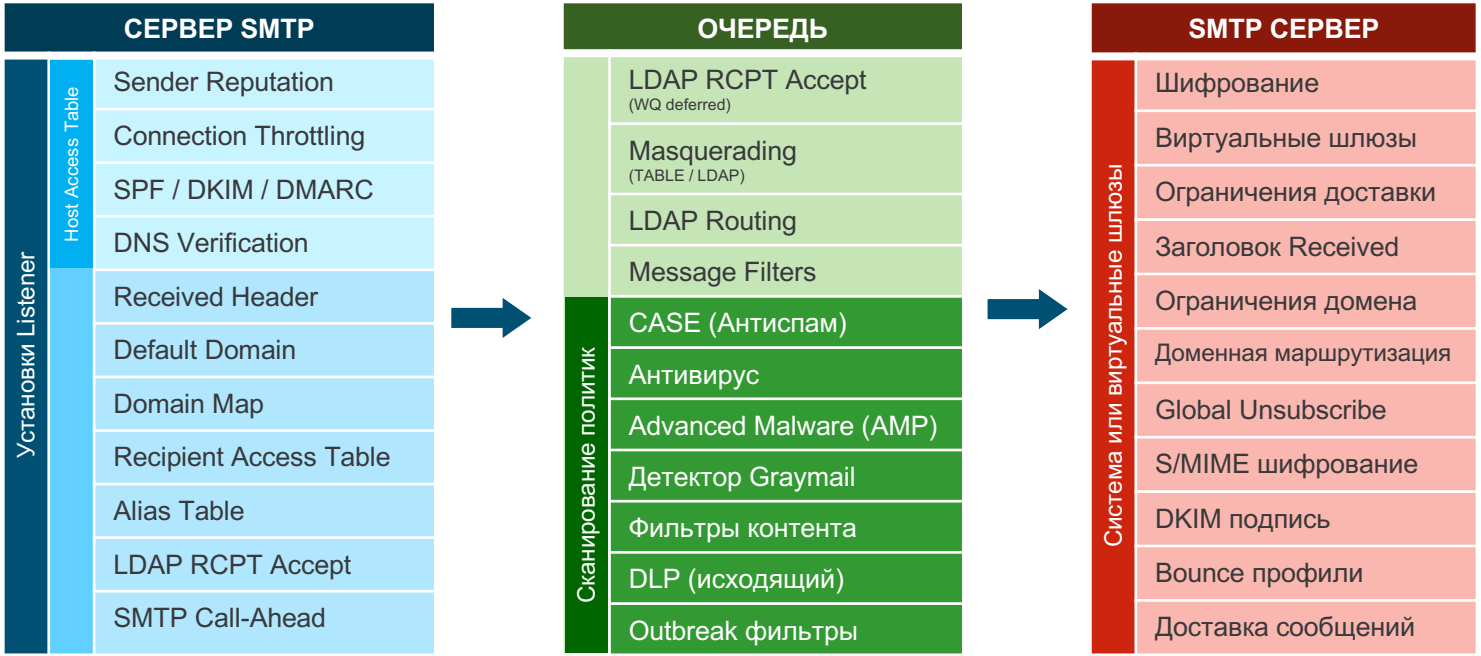


Процесс обработки Email Pipeline

Привязка функций к безопасности



Процесс обработки Email



Заметка о лучших практиках…

- В материале сессии мы будем представлять различные наборы опций для настройки вашей среды
- Они предназначены как пример использования. Поскольку каждая инсталляция уникальна, обязательно проверяйте и тестируйте эти настройки.
- После определенного времени проанализируйте результаты, донастройте правила для достижения желательного результата

Настройка антиспам системы

Мы все там были….

Цель: Злой босс

FBI Headquarters, Washington, D.C.

LC Larry Cooper <[redacted]>
Thu 4/21/2016, 8:33 PM
[redacted]

Reply all

Anti-Terrorist and Monetary Crimes Division
FBI Headquarters, Washington, D.C.
Federal Bureau of Investigation
J.Edgar Hoover Building 935 Pennsylvania Avenue,
NW Washington, D.C

Attn: Fund Beneficiary!!!

This e-mail has been issued to you in order to officially inform you that we have completed an investigation on an International Payment in which was issued to you by an International Lottery Company. With the help of our newly developed technology (International Monitoring Network System), we discovered that your e- mail address was automatically selected by an Online Balloting System, this has legally won you the sum of $2.4million USD from a Lottery Company outside the United States of America. During our investigation, we discovered that your e- mail won the money from an Online Balloting System and we have authorized this winning to be paid to you via INTERNATIONAL CERTIFIED BANK DRAFT.

Normally, it will take up to five business days for an INTERNATIONAL CERTIFIED BANK DRAFT by your local bank.
We have successfully notified this company on your behalf that funds are to be drawn from a registered bank within the world winded, to enable you cash the check instantly without any delay, henceforth the stated amount of $2.4million USD has been deposited with IMF.

We have completed this investigation and you are hereby approved to receive the winning prize as we have verified the entire transaction

Давайте взглянем ближе…

```
Sat Jun 17 05:29:48 2018 Info: New SMTP ICID 188036 interface Data 1 (216.71.129.13) address 98.137.70.150 reverse dns host sonic318-
24.consmr.mail.gq1.yahoo.com verified yes
Sat Jun 17 05:29:48 2018 Info: ICID 188036 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0] SBRS -0.7 country United States
Sat Jun 17 05:29:48 2018 Info: ICID 188036 TLS success protocol TLSv1.2 cipher AES128-SHA
Sat Jun 17 05:29:49 2018 Info: Start MID 94399 ICID 188036
Sat Jun 17 05:29:49 2018 Info: MID 94399 ICID 188036 From: <larrycooper02@yahoo.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 ICID 188036 RID 0 To: <angrybossman@dinconsulting.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 Message-ID '<267641597.11879217.1497447892063@mail.yahoo.com>'
Sat Jun 17 05:29:49 2018 Info: MID 94399 Subject 'FBI Headquarters, Washington, D.C.'
Sat Jun 17 05:29:49 2018 Info: MID 94399 ready 10951010 bytes from <larrycooper02@yahoo.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 matched all recipients for per-recipient policy DINCONSULTING in the inbound table
Sat Jun 17 05:29:49 2018 Info: ICID 188036 close
Sat Jun 17 05:29:51 2018 Info: MID 94399 was too big (10951010/1097152) for scanning by CASE
Sat Jun 17 05:29:51 2018 Info: MID 94399 interim AV verdict using Sophos CLEAN
Sat Jun 17 05:29:51 2018 Info: MID 94399 antivirus negative
Sat Jun 17 05:29:51 2018 Info: MID 94399 queued for delivery
Sat Jun 17 05:29:52 2018 Info: New SMTP DCID 1496 interface 216.71.129.13 address 23.103.157.42 port 25
```

Давайте взглянем ближе…

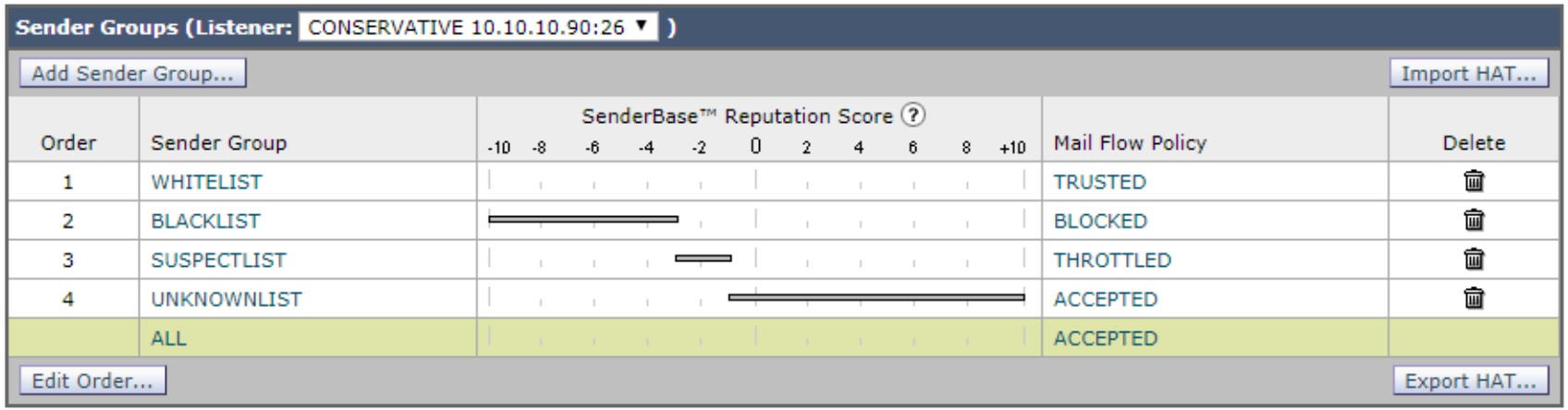
```
Sat Jun 17 05:29:48 2018 Info: New SMTP ICID 188036 interface Data 1 (216.71.129.13) address 98.137.70.150 reverse dns host sonic318-
24.consmr.mail.gq1.yahoo.com verified yes
Sat Jun 17 05:29:48 2018 Info: ICID 188036 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0] SBRS -0.7 country United States
Sat Jun 17 05:29:48 2018 Info: ICID 188036 TLS success protocol TLSv1.2 cipher AES128-SHA
Sat Jun 17 05:29:49 2018 Info: Start MID 94399 ICID 188036
Sat Jun 17 05:29:49 2018 Info: MID 94399 ICID 188036 From: <larrycooper02@yahoo.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 ICID 188036 RID 0 To: <angrybossman@dinconsulting.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 Message-ID '<267641597.11879217.1497447892063@mail.yahoo.com>'
Sat Jun 17 05:29:49 2018 Info: MID 94399 Subject 'FBI Headquarters, Washington, D.C.'
Sat Jun 17 05:29:49 2018 Info: MID 94399 ready 10951010 bytes from <larrycooper02@yahoo.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 matched all recipients for per-recipient policy DINCONSULTING in the inbound table
Sat Jun 17 05:29:49 2018 Info: ICID 188036 close
Sat Jun 17 05:29:51 2018 Info: MID 94399 was too big (10951010/1097152) for scanning by CASE
Sat Jun 17 05:29:51 2018 Info: MID 94399 interim AV verdict using Sophos CLEAN
Sat Jun 17 05:29:51 2018 Info: MID 94399 antivirus negative
Sat Jun 17 05:29:51 2018 Info: MID 94399 queued for delivery
Sat Jun 17 05:29:52 2018 Info: New SMTP DCID 1496 interface 216.71.129.13 address 23.103.157.42 port 25
```

3 области внимания

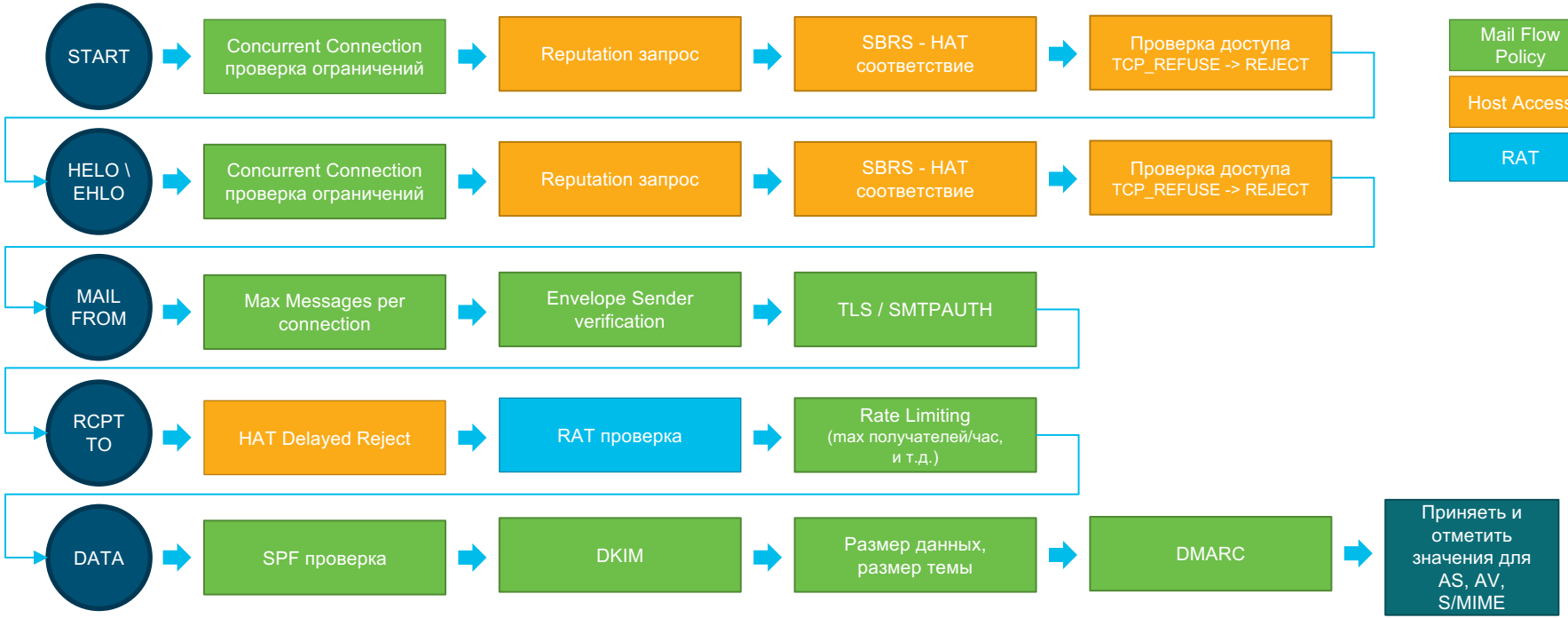
1. **Репутация и настройки Mail Flow Policy**
2. **CASE механизмы и граничные размеры**
3. **Настройки фильтров Spam, Graymail и Outbreak Engine**

Структура Host Access Table

- HAT привязывается к listener, определенному как Public или Private. После того, как Listener создан, его тип не может быть изменен.
- IP и хосты оцениваются в HAT сверху вниз до первого срабатывания
- SenderGroups – это контейнеры, которые определяют соответствие политик при совпадении
- Включение в SenderGroup определяется Reputation Score (по умолчанию), DNS, или явными указаниями IP

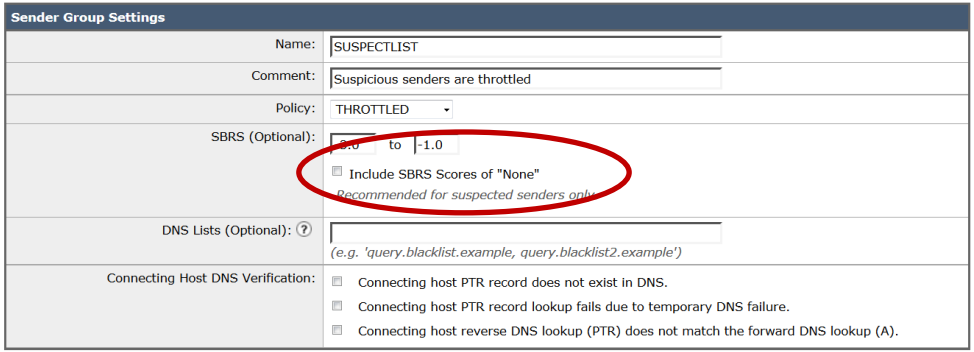


Reputation + Sender Groups + Mail Flow Policies



Опции SenderGroup

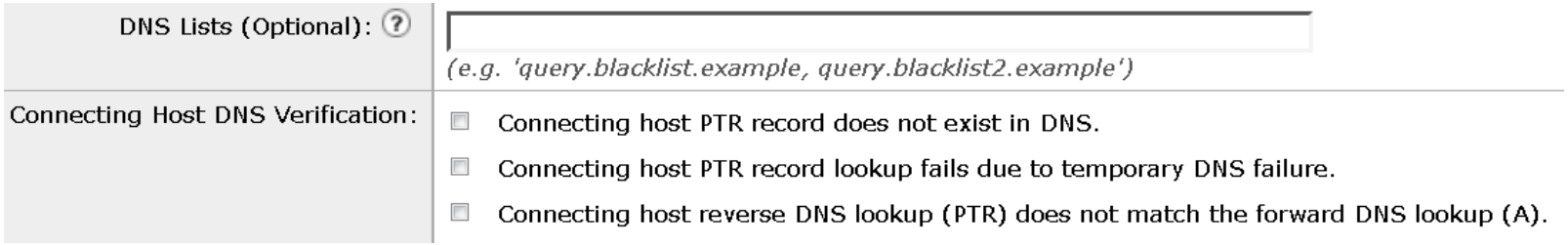
- Репутация SenderBase может назначаться SenderGroups, включая нейтральную репутацию и узлы без репутации
- В настройках вы определяете Name, Mail Flow Policy
- Номенклатура важна, она отображается в логах и отчетах!
- Могут использоваться RBL.




```
Thu Jun  9 13:40:34 2016 Info: New SMTP ICID 8 interface Management (10.10.10.90) address 94.46.249.12
Thu Jun  9 13:40:34 2016 Info: ICID 8 ACCEPT SG SUSPECTLIST match sbrs[-3.0:-1.0] SBRS -2.1
Thu Jun  9 13:40:34 2016 Info: Start MID 410 ICID 8
```

Опции SenderGroup

- Connecting host PTR record does not exist in DNS.
- Connecting host PTR record lookup fails due to temporary DNS failure.
- Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).



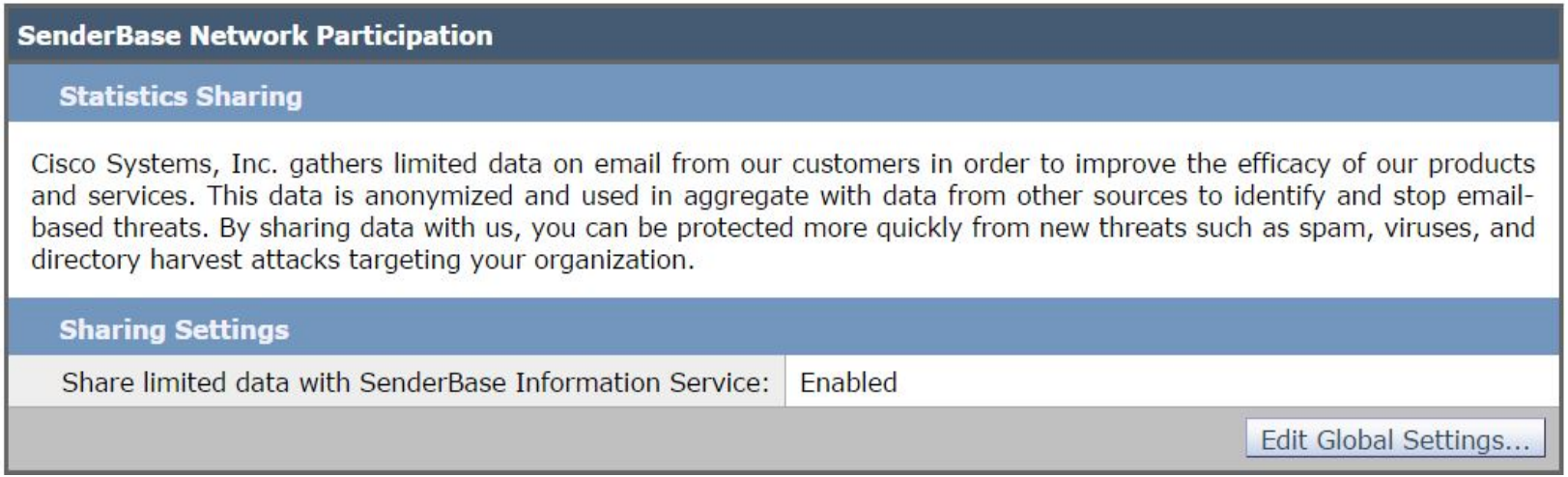
Понимание репутации Email

Spam Traps	Отчеты о жзалобах	Черные и белые списки IP	Данные о геолокации
Состав сообщения	Список скомпроме-тированных узлов	Данные о вебсайтах	Данные о хостах
Данные о глобальных объемах email	Доменные Blacklist и Safelists	Другие данные	DNS данные

- Основное отличие – это охват и качество данных
- Обработка данных в реальном времени позволяет нам видеть угрозы перед тем, как кто-то еще их увидит и защитит клиентов

Почему важна телеметрия

- Предоставляет Talos возможность понять целевые атаки
- Если хотите поделиться деталями, используйте скрытую CLI команду: "fullsenderbaseconfig"



Что отправляется?

- Когда включено, Context Adaptive Scanning Engine (CASE) используется для сбора и отправки данных (вне зависимости от того, включен или выключен антиспам)
- Данные – это суммарная информация об атрибутах сообщения и информация о том, как разные сообщения обрабатываются Cisco устройством. Мы не отправляем сообщения целиком!

Item	Sample Data
Message count at various stages within the appliance	Seen by Anti-Virus engine: 100 Seen by Anti-Spam engine: 80
Sum of Anti-Spam and Anti-Virus scores and verdicts	2,000 (sum of anti-spam scores for all messages seen)
Number of messages hitting different Anti-Spam and Anti-Virus rule combinations	100 messages hit rules A and B 50 messages hit rule A only
Number of Connections	20 SMTP Connections
Number of Total and Invalid Recipients	50 total recipients 10 invalid recipients
Hashed Filename(s): (a)	A file <one-way-hash>.pif was found inside an archive attachment called <one-way-hash>.zip.
Obfuscated Filename(s): (b)	A file aaaaaaa0.aaa.pif was found inside a file aaaaaaa.zip.
URL Hostname (c)	There was a link found inside a message to www.domain.com
Obfuscated URL Path (d)	There was a link found inside a message to hostname www.domain.com, and had path aaa000aa/aa00aaa.
Number of Messages by Spam and Virus Scanning Results	10 Spam Positive 10 Spam Negative 5 Spam Suspect 4 Virus Positive 16 Virus Negative 5 Virus Unscannable
Number of messages by different Anti-Spam and Anti-Virus verdicts	500 spam, 300 ham
Count of Messages in Size Ranges	125 in 30K-35K range
Count of different extension types	300 “.exe” attachments
Correlation of attachment types, true file type, and container type	100 attachments that have a “.doc” extension but are actually “.exe” 50 attachments are “.exe” extensions within a zip
Correlation of extension and true file type with attachment size	30 attachments were “.exe” within the 50-55K range
Number of attached files uploaded to the file reputation service (AMP cloud)	1110 files were uploaded to the file reputation service
Verdicts on files uploaded to the file reputation service (AMP cloud)	10 files were found to be malicious 100 files were found to be clean 1000 files were unknown to the reputation service
Reputation score of files uploaded to the file reputation service (AMP cloud)	50 files had a reputation score of 37 50 files had a reputation score of 57 1 file had a reputation score of 61 9 files had a reputation score of 99
Names of files uploaded to the file reputation service (AMP cloud)	example.pdf testfile.doc
Names of malware threats detected by the file reputation service (AMP cloud)	Trojan-Test

Настройка репутации на ESA

Default Settings: Moderate Blocking

Order	Sender Group	SenderBase™ Reputation Score -10 -8 -6 -4 -2 0 2 4 6 8 +10	Mail Flow Policy
1	RELAYLIST		RELAYED
2	WHITELIST		TRUSTED
3	BLACKLIST		BLOCKED
4	SUSPECTLIST		THROTTLED
5	UNKNOWNLIST		ACCEPTED
	ALL		ACCEPTED

Custom Settings: Aggressive Throttling

Order	Sender Group	SenderBase™ Reputation Score -10 -8 -6 -4 -2 0 2 4 6 8 +10	Mail Flow Policy
1	RELAYLIST		RELAYED
2	WHITELIST		TRUSTED
3	BLACKLIST		BLOCKED
4	SUSPECTLIST		HEAVY_THROTTLE
5	GREYLIST		LIGHT_THROTTLE
6	UNKNOWNLIST		ACCEPTED
	ALL		ACCEPTED

Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	98.6%	756
Stopped as Invalid Recipients	1.4%	11

- Значение репутации определяется сразу после инициации подключения
- Sender Groups и действия определяются администратором
- Репутация может заблокировать 80-90%нежелательных подключений на ESA

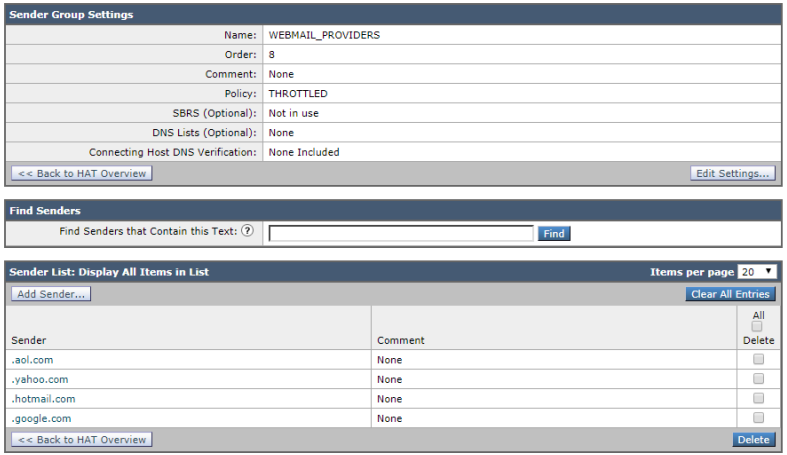
Репутация: DNS и кеширование

- DNS – это наиболее критический сервис для ESA
- По умолчанию на одно подключение выполняется 4 DNS запроса: Reverse DNS, 2 запроса SRBS и номер ASN (информационный)
- С SPF, DKIM и DMARC – 3 или больше запроса DNS TXT записей
- Возможно как минимум 7 DNS запросов на соединение (исключая кеширование)
- Плюс фактор DNS резолвинга для исходящей почты, LDAP, внутренние хосты, etc.
- Больше резолверов в высоконагруженных системах

```
Tue Dec 19 07:34:05 2017  Info: ICID 394968647 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS unable to retrieve

Tue Dec 19 07:34:05 2017 Warning: Received an invalid DNS Response: rcode=ServFail
data="'ev\\x81\\x82\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x01m\\x02ag\\x00\\x00\\x01\\x00\\x01'"
```

Выделение почты, не критической для бизнеса

Sender Group: WEBMAIL_PROVIDERS - IncomingMail 216.71.129.13:25



Sender Group Settings

Name:	WEBMAIL_PROVIDERS
Order:	8
Comment:	None
Policy:	THROTTLED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview | Edit Settings...

Find Senders

Find Senders that Contain this Text: | Find

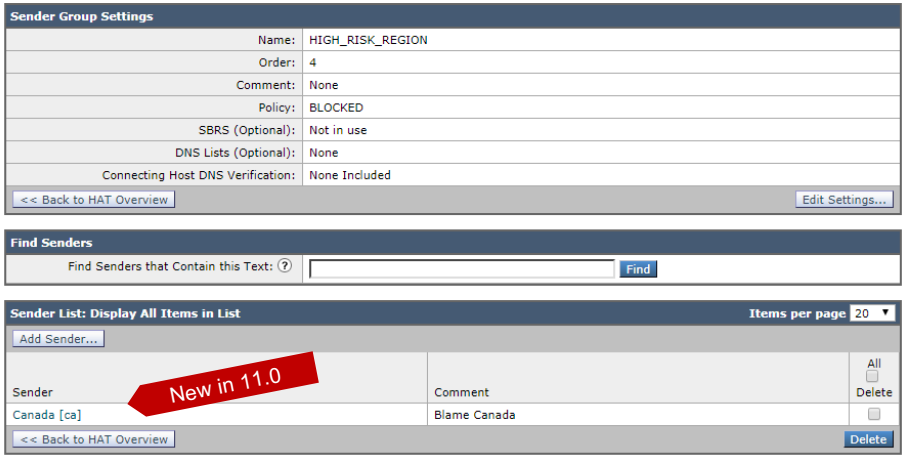
Sender List: Display All Items in List — Items per page 20

Add Sender... | Clear All Entries

Sender	Comment	All Delete
.aol.com	None	
.yahoo.com	None	
.hotmail.com	None	
.google.com	None	

<< Back to HAT Overview | Delete

Sender Group: HIGH_RISK_REGION - IncomingMail 216.71.129.13:25



Sender Group Settings

Name:	HIGH_RISK_REGION
Order:	4
Comment:	None
Policy:	BLOCKED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview | Edit Settings...

Find Senders

Find Senders that Contain this Text: | Find

Sender List: Display All Items in List — Items per page 20

Add Sender...

New in 11.0

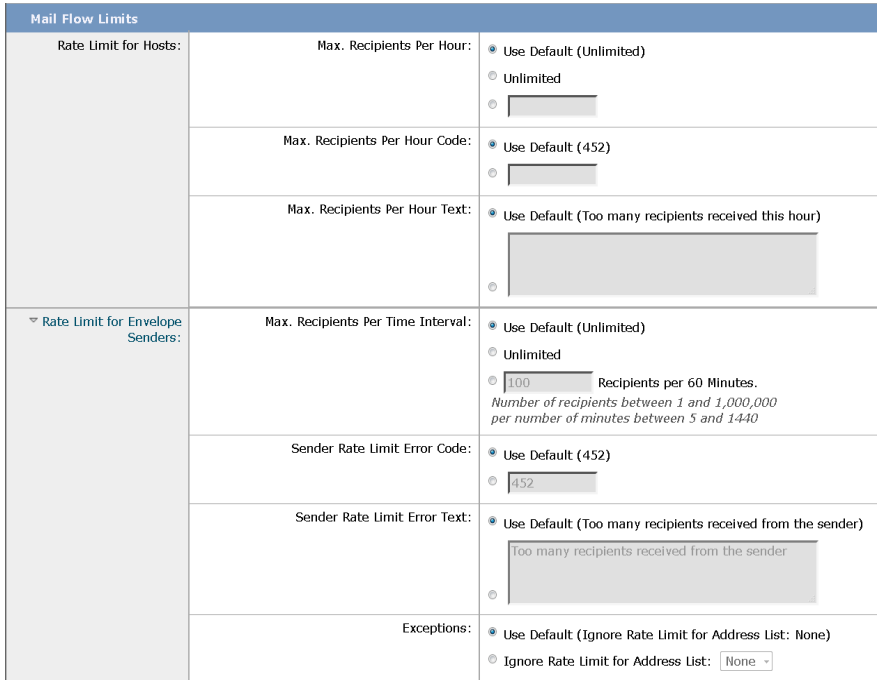
Sender	Comment	All Delete
Canada [ca]	Blame Canada	

<< Back to HAT Overview | Delete

- Явно добавляя хосты, IP и страны в SenderGroup вы можете определить желательное поведение подключений
- Основная идея – это ограничить возможности для атакующих путем ограничения на доставку не критических писем

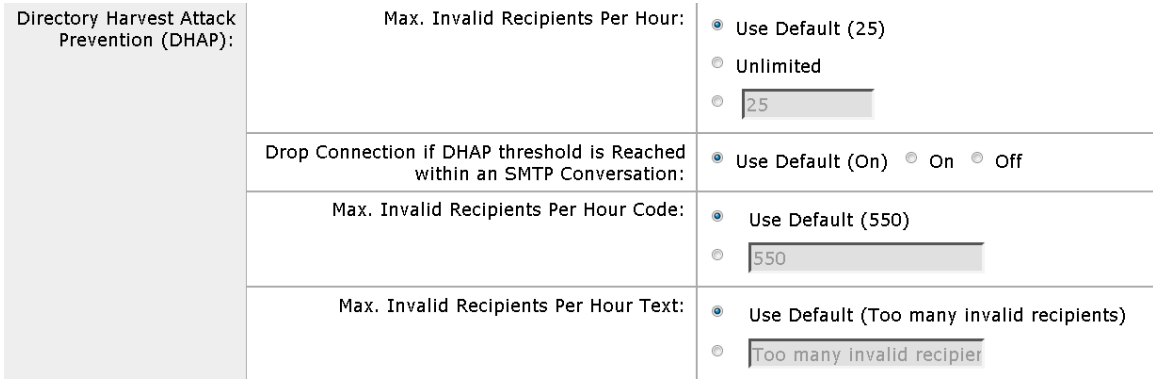
MailFlow политики: Ограничения Host vs Sender

- По умолчению ограничения накладываются именно на хост.
- По умолчанию ограничения Envelope Sender Limits на ESA выключены
- Рекомендуется использовать Sender Limits для подозрительных отправителей



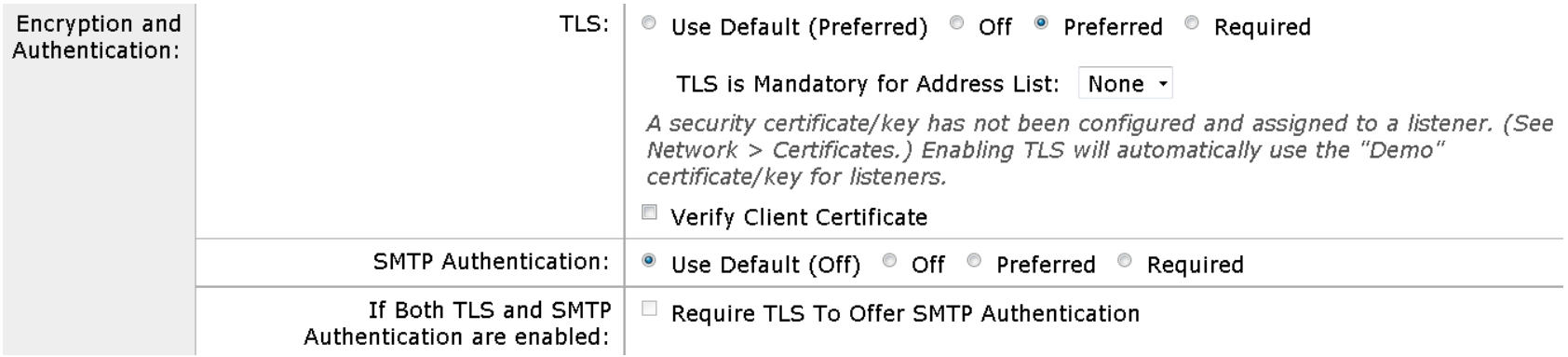
MailFlow политики: Настройки безопасности

- DHAP использует очень «мягкие» значения на ESA, рекомендуется настроить его на более низкие значения
- LDAP расширяет DHAP выполняя reject во время SMTP обмена



MailFlow политики: настройки безопасности

- TLS по умолчанию выключен для входящей и исходящей почты
- Три уровня проверки, рекомендуется поставить preferred по умолчанию
- "Mandatory” может устанавливаться для списка или для отдельной SenderGroup



Пример HAT шаблона

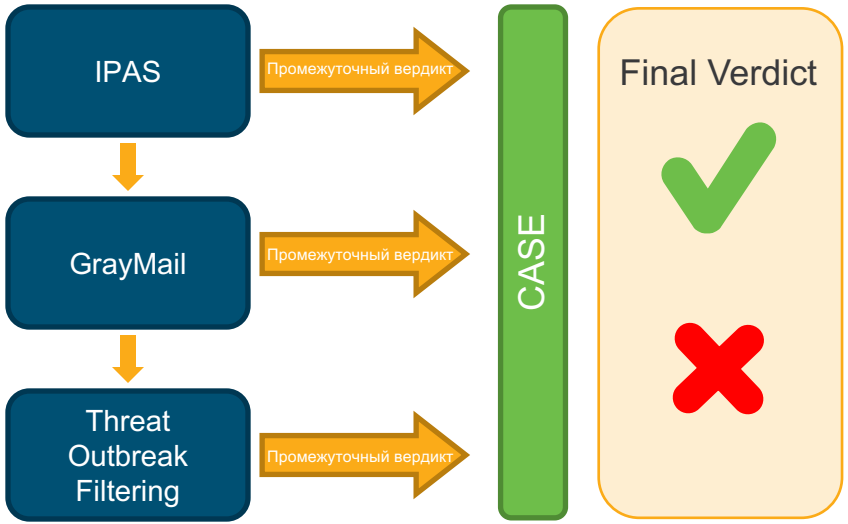
		Sender Group	RELAYLIST	TLSFORCED	WHITELIST	BLACKLIST	SUSPECTLIST	WEBMAIL	GREYLIST	ACCEPTLIST	ALL
		SenderBase Reputation Score				-10 to -2	-2 to 0 (+None)		0 to 4.0	4.0 to 10	
		Connecting Host DNS Verification					Not Exist, Not Match				
		Mail Flow Policy	RELAYED	TLSFORCED	TRUSTED	BLOCKED	HEAVY_THROTTLE	MEDIUM_THROTTLE	MEDIUM_THROTTLE	ACCEPTED	LIGHT_THROTTLE
Policy Settings											
Connection Behavior:		Default Policy Parameters	Relay	Accept	Accept	Reject	Accept	Accept	Accept	Accept	Accept
Connections:	Max. Messages Per Connection:	10	5000	100	1000		1	5	5	DEFAULT	10
	Max. Recipients Per Message:	50	5000		1000		20	25	25	DEFAULT	25
	Max. Message Size:	20M	DEFAULT	DEFAULT	DEFAULT		DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	Max. Concurrent Connections From a Single IP:	10	5000	100	100		1	5	5	DEFAULT	10
SMTP:	Custom SMTP Banner Code:	220	DEFAULT	DEFAULT	DEFAULT		DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	Custom SMTP Banner Text:	Use Default()	DEFAULT	DEFAULT	DEFAULT	Your account or this mail system has been rejected due to the poor sending HTTP(s) peer reputation. If you believe that this failure is in error, please contact the	DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	Override SMTP Banner Hostname:	Use Hostname from Interface	DEFAULT	DEFAULT	DEFAULT		DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
Mail Flow Limits											
Rate Limit for Hosts:	Max. Recipients Per Hour:	1000			UNLIMITED		5	15	15	DEFAULT	100
	Max. Recipients Per Hour Code:	452									
	Max. Recipients Per Hour Text:	Too many recipients received this hour									
Rate Limit for Envelope Senders:	Settings to define maximum recipients for envelo	1000			UNLIMITED		50	50	50	DEFAULT	100
	Sender Rate Limit Error Code:	452					DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	Sender Rate Limit Error Text:	Too many recipients received from the sender									
	Exceptions:	Ignore Rate Limit for Address List: None									
Flow Control:	Use SenderBase for Flow Control:	On	OFF	DEFAULT	DEFAULT		DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	Group by Similarity of IP Addresses:	Off									
Directory Harvest Attack Prevention (DHAP):	Max. Invalid Recipients Per Hour:	25	UNLIMITED	DEFAULT	UNLIMITED		5	10	10	DEFAULT	15
	Drop Connection if DHAP threshold is Reached v	On	Off				DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	Max. Invalid Recipients Per Hour Code:	550									
	Max. Invalid Recipients Per Hour Text:	Too many invalid recipients									
Security Features											
Spam Detection:		On	Off	DEFAULT	Off		DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
Virus Protection:		On	DEFAULT	DEFAULT	DEFAULT		DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
Encryption and Authentication:	TLS:	Preferred		REQUIRED			DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	SMTP Authentication:	Off									
	If Both TLS and SMTP Authentication are enable	Off									
Domain Key/DKIM Signing:											
DKIM Verification:	Use DKIM Verification Profile:	On									
SPF/SIDF Verification:	SPF Verification:	On					DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	Conformance Level:	SIDF Compatible									
	Downgrade PRA verification result if 'Resent-Ser	No									
	HELO Test:	On					DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
DMARC Verification		On					DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	Use DMARC Verification Profile:	Monitor					DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT
	DMARC Feedback Reports:	Send aggregate feedback reports									
Bounce Verification:	Consider Untagged Bounces to be Valid:	No					DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT

- Пример записи данных Host Access Table и Mail Flow policy для того, чтобы создать стратегию для управления подключениями
- Заполнено значениями, чтобы вы могли их использовать как пример

https://cisco.box.com/s/tgub07f1sfyc061o7xmay0p3c4iahg3h

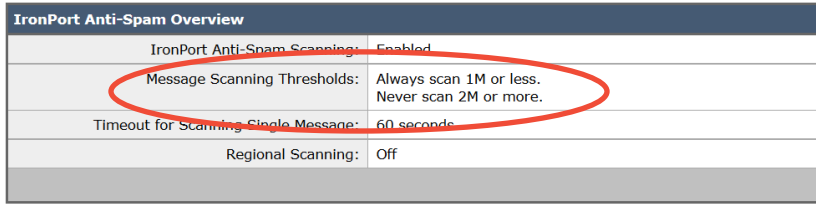
Понимание CASE

- CASE расшифровывается как Context Adaptive Scanning Engine
- CASE это комбинация механизмов Anti-Spam, Graymail and Outbreak
- Каждый механизм дает свой вердикт и в зависимости от действий механизм или пропустит, или сбросит сообщения
- **Не финальные** действия («карантин») отправляют сообщения для обработки дальше в рабочей очереди.
- Финальные действия («drop») вызываю состояние “**early exit**”
- Другие механизмы сканирования могут иметь приоритет если в других механизмах определяется позитивных вердикт



Включение и настройка CASE

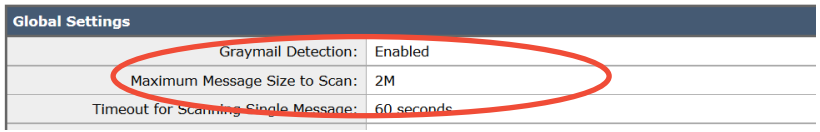
IronPort Anti-Spam



IronPort Anti-Spam Overview	
IronPort Anti-Spam Scanning:	Enabled
Message Scanning Thresholds:	Always scan 1M or less. Never scan 2M or more.
Timeout for Scanning Single Message:	60 seconds
Regional Scanning:	Off

Включите антиспам и увеличьте граничные значения сканирования до 1M Always scan и 2M Never scan or more

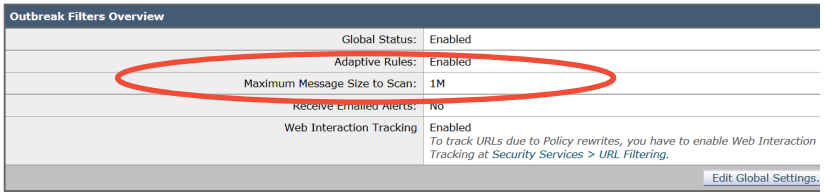
Graymail Detection and Safe Unsubscribing



Global Settings	
Graymail Detection:	Enabled
Maximum Message Size to Scan:	2M
Timeout for Scanning Single Message:	60 seconds

Включите Graymail – это беспланый механим, который увеличивает эффективность антиспама. Был анонсирован в версии 9.5

Outbreak Filters



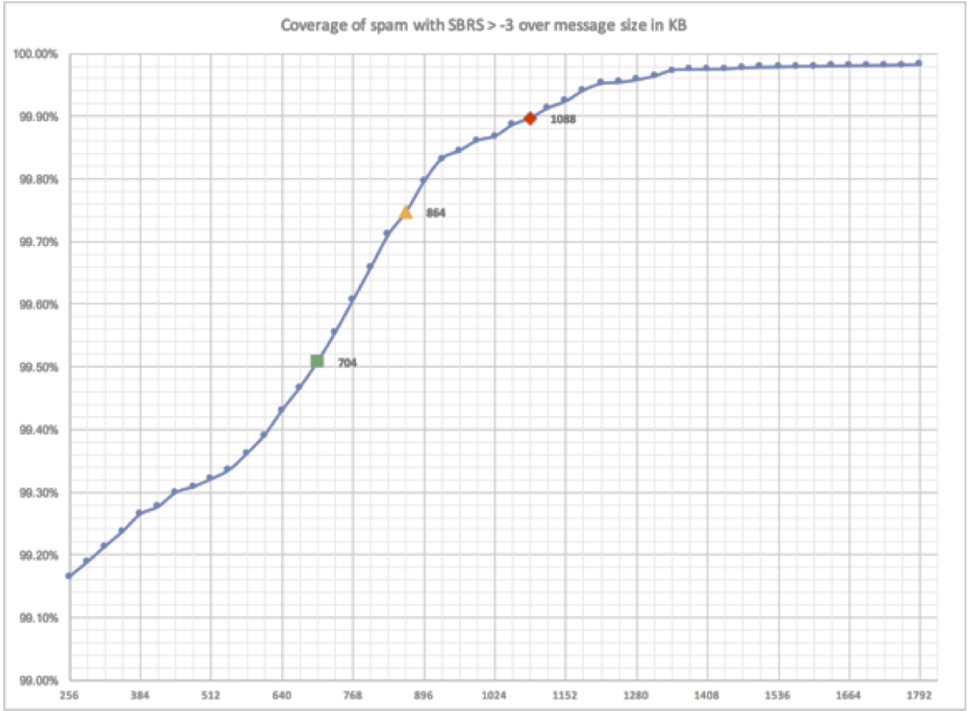
Outbreak Filters Overview	
Global Status:	Enabled
Adaptive Rules:	Enabled
Maximum Message Size to Scan:	1M
Receive Emailed Alerts:	No
Web Interaction Tracking	Enabled *To track URLs due to Policy rewrites, you have to enable Web Interaction Tracking at Security Services > URL Filtering.*

Edit Global Settings...

Включите Threat Outbreak Filters и увеличьте максимальный размер до 1M

Почему так важен размер сканирования

- График от Talos показывает объем спама с большими размерами сообщений по сравнению с общим объемом спама
- На самом деле большинство спама имеет небольшой размер
- Но, если вы не увеличите граничные значения, вы будете пропускать спам-письма
- Большая часть «объемоного» спама находится в диапазоне от 512KB и 896KB, максимальное значение 1.3MB



Сканирование по политикам

- Используйте политики с возможностью message splintering для применения правил сканирования
- Обработка сверху вниз до первого срабатывания, очень важен порядок сообщений!

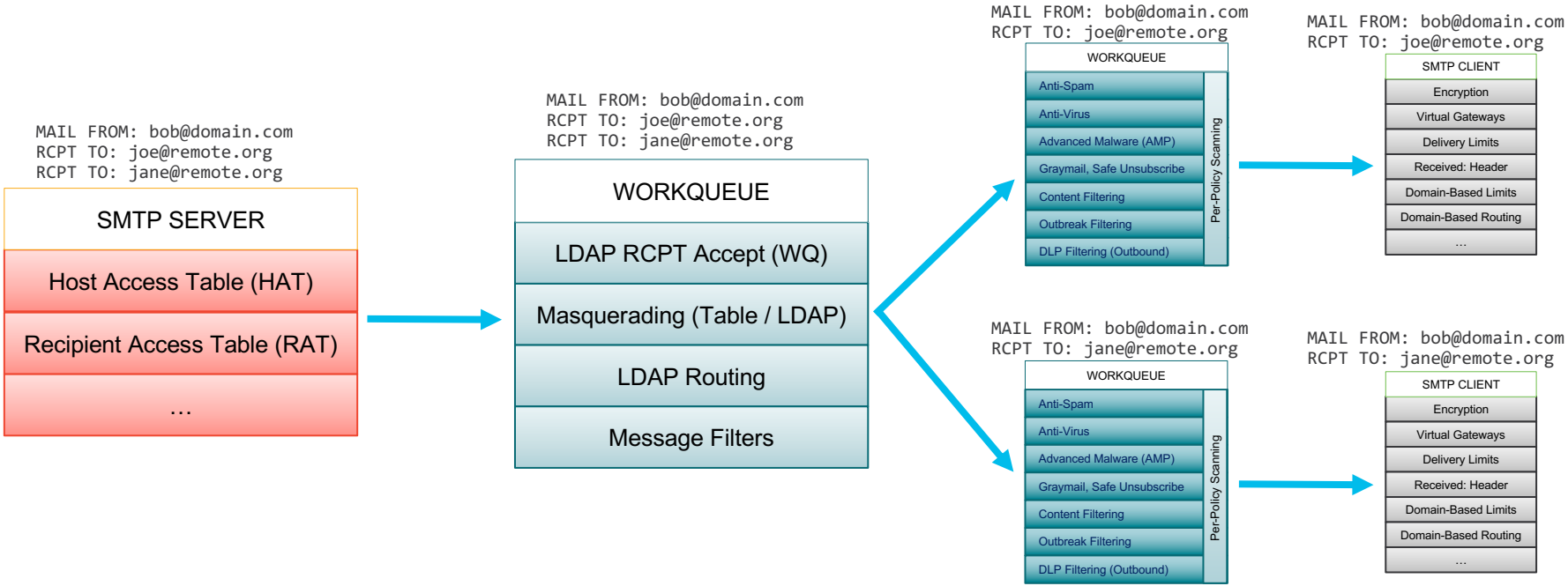
Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	IMP.CISCOSECURITYGURU	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	
2	IMP.INTERNETSINKHOLE	Disabled	Disabled	Disabled	Disabled	Disclaimer-not-filter Bypass-relay-internetsinkhole	Disabled	
3	IMP.ENCORE	IronPort Anti-Spam Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Deliver	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Quarantine	(use default)	(use default)	(use default)	
4	IMP.CSEDEMO	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	(use default)	(use default)	(use default)	Enabled (no filters)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Drop	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Quarantine	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Deliver	BLOCK_URL REWRITE_URL WARN_NO_SCORE LOG_ALL_URLs ...	Retention Time: Virus: 1 day Other: 4 hours	

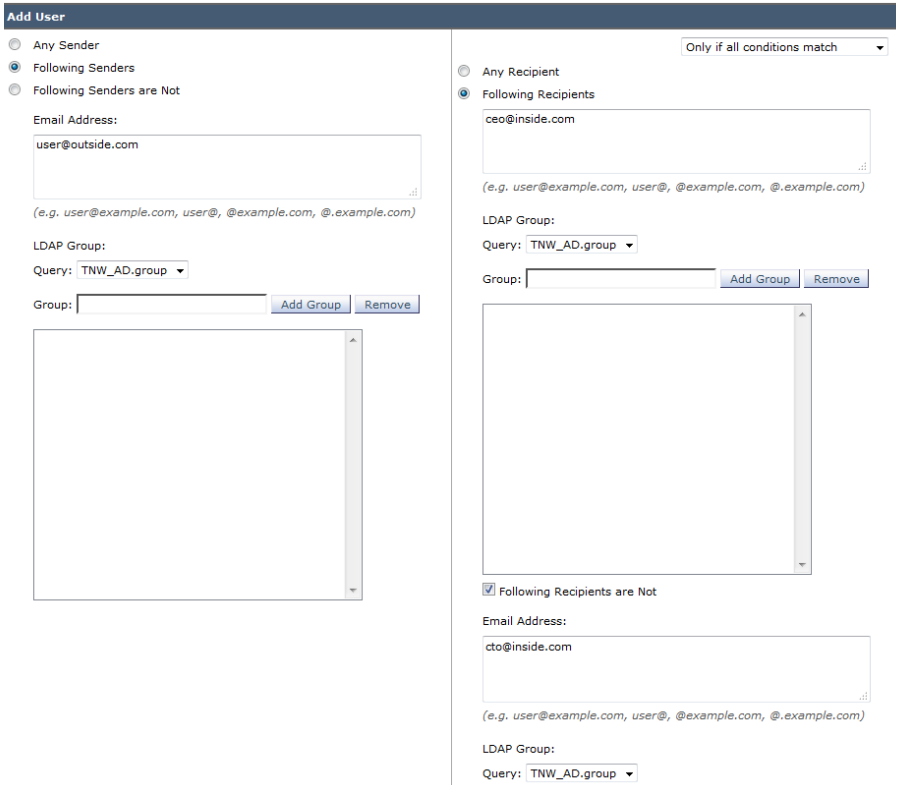
Policy Engine и Splintering

- Если одно сообщение соответствует нескольким политикам, оно будет разделено (splintered)
- Разделение происходит **только, если есть соответствие нескольким политикам**!



Условия соответствия политикам

- В политике используются сложные условия с AND/OR/NOT
- В одной политике может использоваться несколько условий
- Для снижения нагрузки стоит сдвинуть логику из фильтров к политиками



Приоритет соответствия политикам (10.x, 11.1)

- После апгрейда до 10.0 , когда ищется поиск соответствия политике envelope sender и envelope recipient имеют более высокий приоритет перед Sender Header
- В 11.1 есть опция, позволяющая выбрать приоритет данных, которые будут использоваться для поиска соответствия политике.

Mail Policy Settings

Match Priority

Add Priority...

Priority	Headers	Delete
P1	Envelope Sender	
P2	Header "From"	
P3	Header "Sender"	
P4	Header "Reply-To"	

Политики и словари (Dictionaries)

- Клиенты часто используют Dictionaries для поиска соответствия в BlockLists / Allow Lists
- Когда вы блокируете через content filter + dictionary это сканирует все сообщения, таки образом занимая ресурсы
- Используйте политики для быстрого разделения правил между собой
- Помните про порядок политик

Edit Policy

Policy Name:	BLOCKLIST *(e.g. my IT policy)*
Editable by (Roles):	Cloud Operator
Insert Before Policy:	1 (BLOCKLIST)

Users

Add User...

Sender	Recipients	Edit	Delete
user@gmail.com	ANY	Edit	
anotheruser@gmail.com	ceo@company.com	Edit	

Edit Policy

Policy Name:	ALLOWLIST *(e.g. my IT policy)*
Editable by (Roles):	Cloud Operator
Insert Before Policy:	2 (ALLOWLIST)

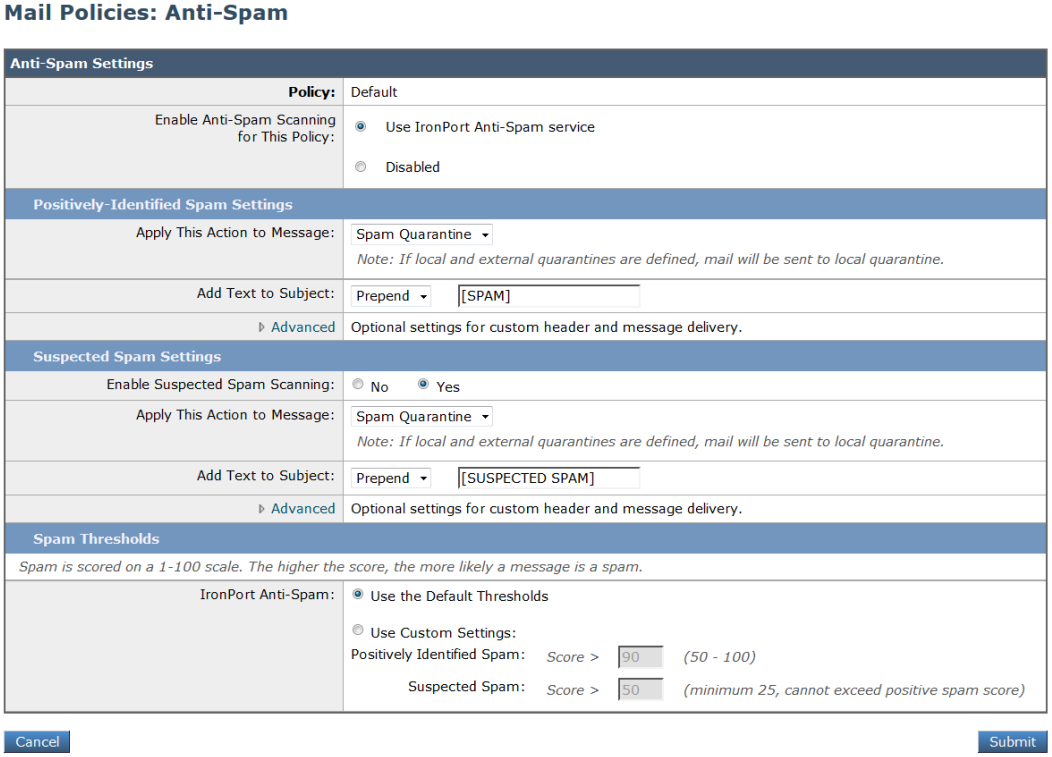
Users

Add User...

Sender	Recipients	Edit	Delete
user@gooddomain.com	ANY	Edit	

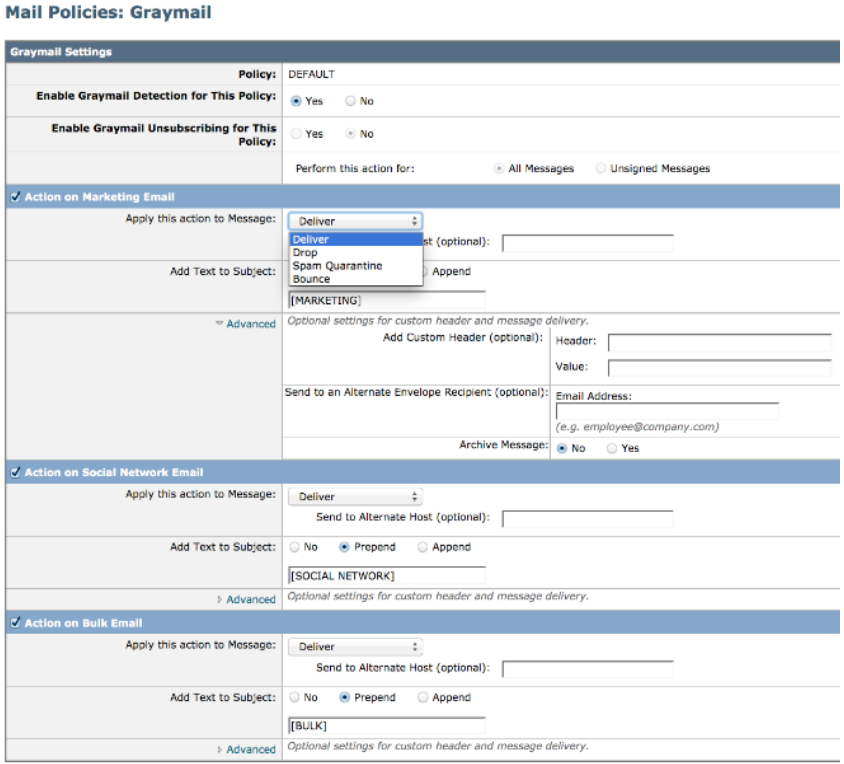
Anti-Spam сканирование

- Вы можете изменить граничные значения для Suspect / Positive spam чтобы увеличить или уменьшить чувствительность
- Не делайте этого, кроме тех случаев, когда это действительно необходимо
- Когда мы настраиваем правила антиспам, мы используем значения по умолчанию как базис, поэтому изменения могут приветси к нежелательным результатам.



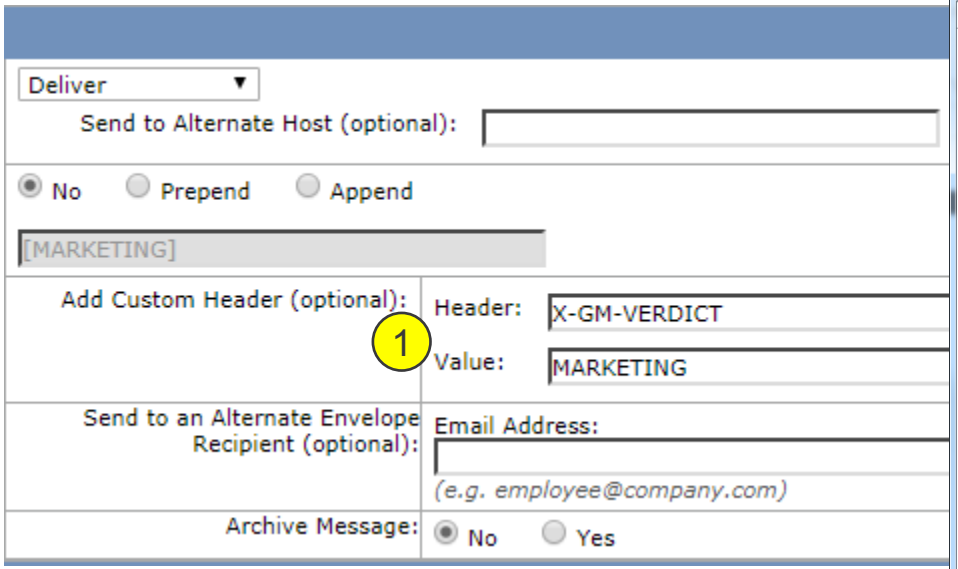
Включение сканирования Graymail

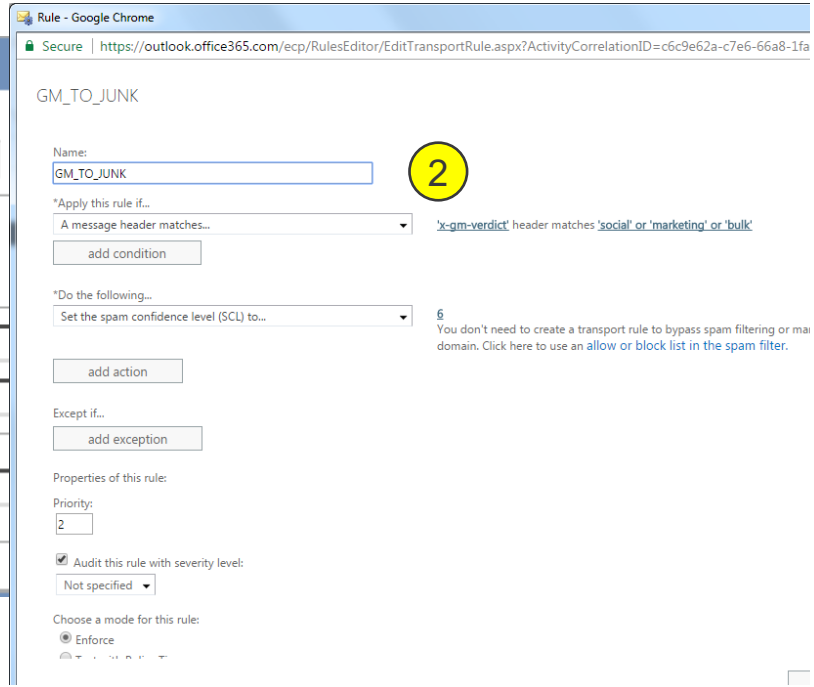
- Graymail имеет 2 компоненты: Detection и Unsubscribe
- Graymail Detection включено, и работает как часть базовой подписки антиспам
- Механизм graymail предоставляет вердикт IPAS (окончательное решение), что обеспечивает более высокую общую эффективность



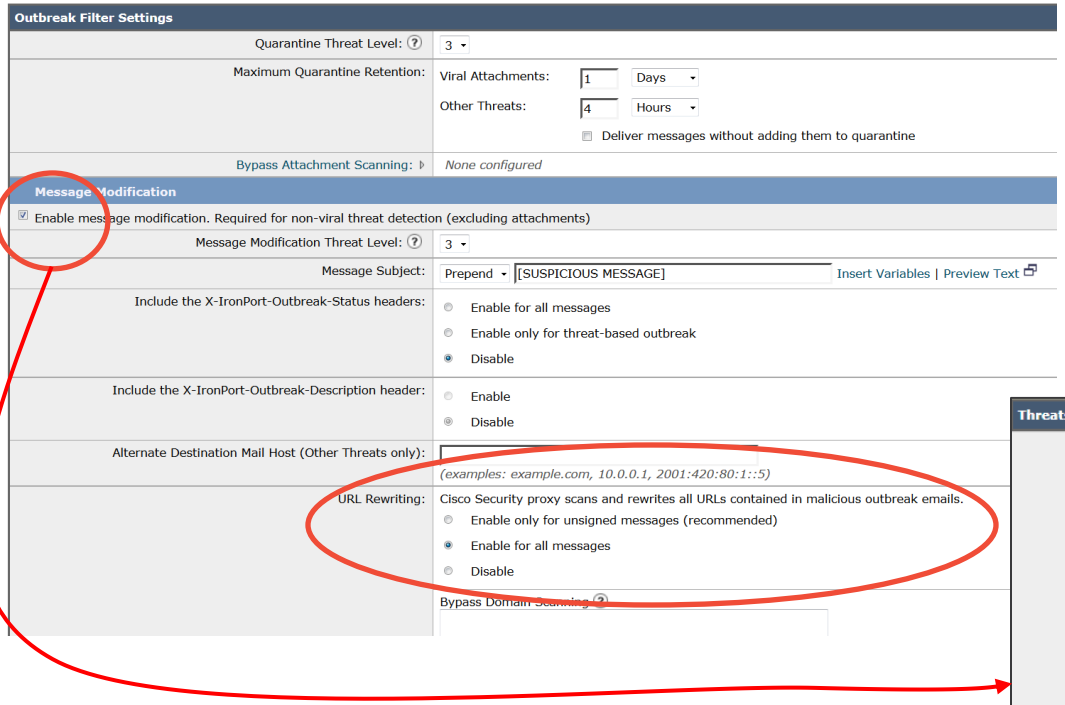
Использование Graymail и папок Outlook Junk

- 2 шага: Создайте x-header в Graymail, фильтруйте в Exchange чтобы установить значение SCL

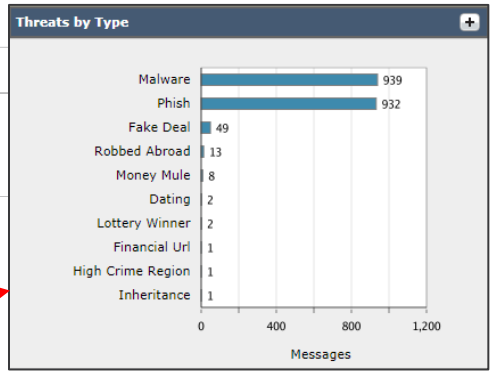




Включение Threat Outbreak Filters



- По умолчанию сключены только Virus Outbreak Filters
- Включением Threat Outbreak (модификация сообщений) вы добавляете информацию, которая отправляется в CASE
- Чтобы использовать URL функционал (позже) Outbreak Filters должны быть включены и настроены



На что это похоже!

```
Sat Jun 17 05:29:48 2018 Info: New SMTP ICID 188036 interface Data 1 (216.71.129.13) address 98.137.70.150 reverse dns host
sonic318-24.consmr.mail.gq1.yahoo.com verified yes
Sat Jun 17 05:29:48 2018 Info: ICID 188036 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0] SBRS -0.7 country United States
Sat Jun 17 05:29:48 2018 Info: ICID 188036 TLS success protocol TLSv1.2 cipher AES128-SHA
Sat Jun 17 05:29:49 2018 Info: Start MID 94399 ICID 188036
Sat Jun 17 05:29:49 2018 Info: MID 94399 ICID 188036 From: <larrycooper2@yahoo.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 ICID 188036 RID 0 To: <angrybossman@dinconsulting.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 Message-ID '<267641597.11879217.1497447892063@mail.yahoo.com>'
Sat Jun 17 05:29:49 2018 Info: MID 94399 Subject 'FBI Headquarters, Washington, D.C.'
Sat Jun 17 05:29:49 2018 Info: MID 94399 ready 10951010 bytes from <larrycooper02@yahoo.com>
Sat Jun 17 05:29:49 2018 Info: MID 94399 matched all recipients for per-recipient policy DINCONSULTING in the inbound table
Sat Jun 17 05:26:49 2018 Info: MID 94398 interim verdict using engine: CASE spam positive
Sat Jun 17 05:26:49 2018 Info: MID 94398 using engine: CASE spam positive
Sat Jun 17 05:26:49 2018 Info: MID 94398 interim AV verdict using Sophos CLEAN
Sat Jun 17 05:26:49 2018 Info: MID 94398 antivirus negative
Sat Jun 17 05:26:49 2018 Info: MID 94398 AMP file reputation verdict : SKIPPED (no attachment in message)
Sat Jun 17 05:26:49 2018 Info: MID 94398 using engine: GRAYMAIL negative
Sat Jun 17 05:26:49 2018 Info: MID 94398 Outbreak Filters: verdict positive
Sat Jun 17 05:26:49 2018 Info: MID 94398 Threat Level=5 Category=Scam Type=Fake Deal
Sat Jun 17 05:26:49 2018 Info: MID 94398 Virus Threat Level=5
Sat Jun 17 05:26:49 2018 Info: MID 94398 quarantined to "Outbreak" (Outbreak rule:Scam: Fake Deal)
Sat Jun 17 05:26:49 2018 Info: Message finished MID 94398 done
```

Подумайте: где это сообщение находится и почему?

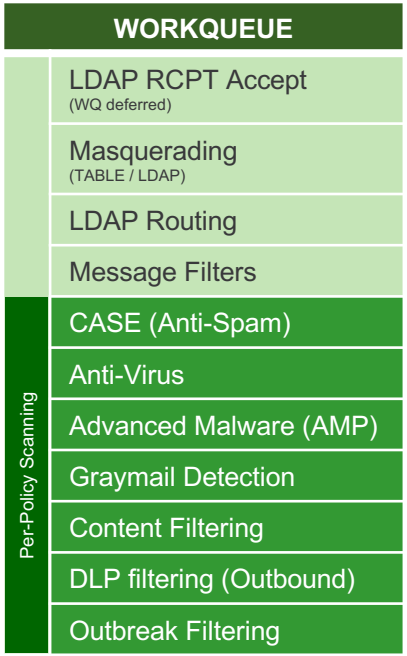
Проверка настройка антспам системы

- Проверьте Host Access Table – все еще используете старые значения? Время их изменить
- Создайте больше SenderGroups и постепенно измените настройки
- Проверьте WhiteLists – объекты могут устареть, ip изменены etc. Используйте комментарии для отслеживания и регулярно обновляйте данные
- Проверьте Mail Flow Policies и включите Sender limits, Sender Verification, etc.
- Используйте новые детальные политики для создания улучшенных Incoming Mail Policies
- Сместите логику из фильтров в политики для создания более эффективных настроек.
- Включите Graymail и Threat Outbreak Filtering для получения информации и улучшенной эффективности
- Проверьте граничные размеры файлов: Значения по умолчанию низкие и могут потенциально пропустить подозрительные сообщения
- Upgrade, Upgrade, Upgrade!

Антифишинг

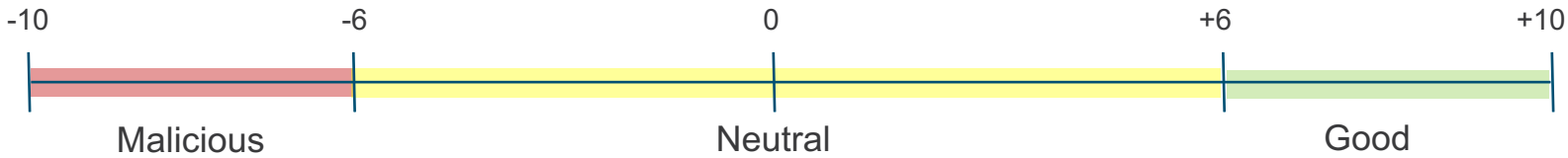
Фишинг: Понять, где сканируются URL

- Начиная с версии 8.5.6 ESA может оценивать URL в сообщении – репутация и категоризация
- URL фильтры по умолчанию выключены, вы должны включить сервис и иметь корректную лицензию Outbreak Filters
- После включения, URLs оцениваются с помощью трех механизмов
  1. Во время сканирования IPAS, а URL используется для оценки значений SPAM
  2. В Content Filter для Reputation и Category
  3. Как часть функции Threat Outbreak Filter URL Rewrite
- В 9.7 была анонсирована функция Web Interaction Tracking для Clicked URLs, которую надо включать после обновлений



Оценка URL и опции

- Web Reputation Score (WBRS) использует те же значения от -10 до +10, но есть небольшие отличия от SBRS
- На основе политики безопасности вы можете определить, как вести себя с URL, которые попадают в организацию.



Включение URL фильтров

1

URL Filtering Overview

URL Category and Reputation Filters:	Enabled
Cisco Web Security Services connection status:	Connected
URL Whitelist:	None
Web Interaction Tracking:	Enabled *To track URLs due to Outbreak Filter rewrites, you have to enable Web Interaction Tracking at Security Services > Outbreak Filters.*

Edit Global Settings...

Включите URL фильтры для URL DB в CASE

Включите для трекинга нажатых URL в фильтрах

2

Outbreak Filters Overview

Global Status:	Enabled
Adaptive Rules:	Enabled
Maximum Message Size to Scan:	1M
Receive Emailed Alerts:	No
Web Interaction Tracking	Enabled *To track URLs due to Policy rewrites, you have to enable Web Interaction Tracking at Security Services > URL Filtering.*

Edit Global Settings...

Включите для трекинга нажатых URL в Outbreak

Трекинг и логирование URL

- Логирование URLs появляется в логах только если:
  - Включено Message Tracking
  - Работают Outbreak фильтры и/или фильтры контента с URL репутацией или категориями
  - Дляoutbreak filters надо включить URL Rewriting
  - В CLI надо сключить URL логирование командой outbreakconfig

```
> outbreakconfig
Outbreak Filters: Enabled
Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[]> setup
...
Logging of URLs is currently disabled.
Do you wish to enable logging of URL's? [N]> y
Logging of URLs has been enabled.
...
```

Видимость URL

- С релизом 10.0, URL информация о URL записывается в Message Tracking

Tracking Privileges

User Roles	View information caught by Data Loss Prevention filters: ⓘ	View details for URLs caught by URL filter: ⓘ
Predefined		
Administrator	☑	☑
Operator	☑	☐
Read-Only Operator	☑	☐
Help Desk User	☑	☐
Custom Roles		
Cloud Help Desk	☑	☐
Cloud Operator	☑	☐

Processing Details

Summary | **URL Details**

13 Jun 2016 13:15:23 (GMT -04:00)	Message 740 rewritten URL u'http://tara.walletbest.info/jk/j/54/'.

```
Info: MID 3999805 antivirus negative
Info: MID 3999805 AMP file reputation verdict : CLEAN
Info: MID 3999805 using engine: GRAYMAIL negative
Info: MID 3999805 URL http://www.keyfuture.com/ has reputation -7.94499005274 matched url-reputation-rule
Info: Message aborted MID 3999805 Dropped by content filter 'BLOCK URL' in the inbound table
Info: Message finished MID 3999805 done
```

Включение обработки shortened URL (11.1)

- Эта функция позвляет «раскрыть» URL, которые использует сервис сокращения для определения реальных данных
- ESA запрашивает сервис напрямую для получения базового URL
- Уровень вложенности 10.
- Дожно быть включено через CLI

```
websecurityadvancedconfig >  Do you want to enable URL filtering for shortened URLs? [Y]> Y
```

Services supported (23):

- bit.ly
- tinyurl.com
- ow.ly
- tumblr.com
- formspring.me
- ff.im
- youtu.be
- chatter.com
- tl.gd
- plurk.com
- url4.eu
- j.mp
- goo.gl
- yfrog.com
- su.pr
- wp.me
- post.ly
- tiny.cc
- ustre.am
- tr.im
- ur.ly
- fb.me
- alturl.com

Оценка URL и опции для тела письма

- URL репутация оценивается CASE и используется как часть вердикта Anti-Spam
- Если письмо не остановлено AS, URL может оцениваться Content Filter на репутацию и категорию

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "")	

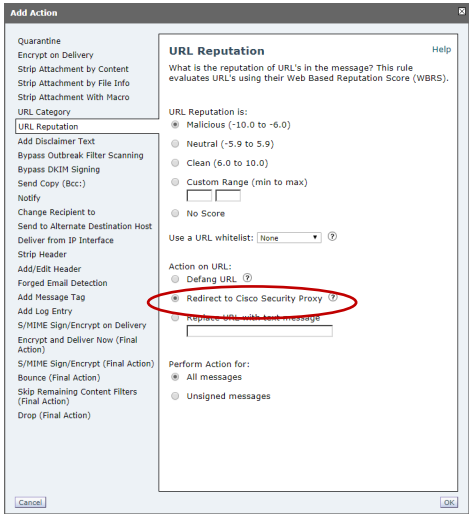
Actions

Add Action...

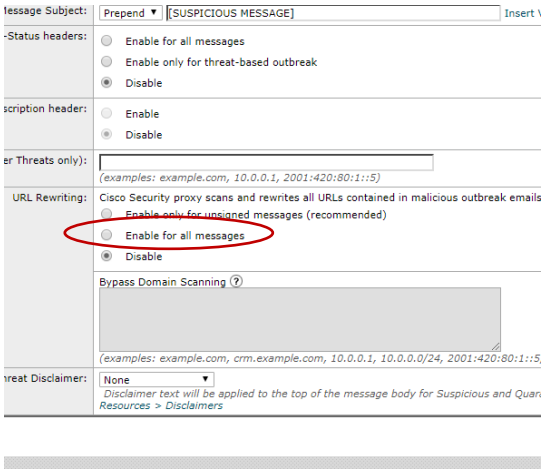
Order	Action	Rule	Delete
Final	Drop (Final Action)	drop()	

Понимание модификации URL

- URL может быть модифицирован в двух местах – в (Message или Content) или как часть вердикта Outbreak Filter
- URLs модифицированные фильтром с действием Re-Direct делает только проверку репутации во время клика
- URLs модифицированные Outbreak Filters проходит более глубокую инспекцию, включая сканирование Malware и AMP,



≠



«Чистая» перезапись URL

- В версии 9.7 мы анонсировали возможность делать “чистую” URL перезапись, при которой перезаписывается только тэг HREF, что позволяет письу выглядеть нормально
- Опция включается через CLI – Все URLs относится к href и тексту, при ответе N он будет перезаписывать только HREF

```
websecurityadvancedconfig >  Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
```

Перед «чистой» перезаписью:

Hi,

Click on the link below for your special offer!

https://secure-web.cisco.com/1adjW1InNsH83UFDjLDFTjer5nJId9J-HjqKlbAcaLQ74EH5ViYESt C5jPZqvg_weQJeocAQeEryL5b1JR6T0JgzXkjk1PUMCBb_eQApCXS6ZsoujzgNvwt9UqN27SN1zcMVjmIpWQN__ITmALmHdGMZ_PaFf9FTUvmMc7UjRZBhvHzDvGJ0Lm5uh9evj_C_OemBAy44xbXwmYuA3uRPqKrf7T6ZNepA0MlcszDFPwufWUB7bbmS8Ziqh_-CyjG8KI6fJU33qjnInxHsjOBq98VxQUT-vMf_2U_OlpguXStzGTlj3U__yBZlLZsS9W1xLZpcGUKpdUp8Q_SBBq9HknQ/http%3A%2F%randomofferurl.com

После «чистой» перезаписи:

Hi,

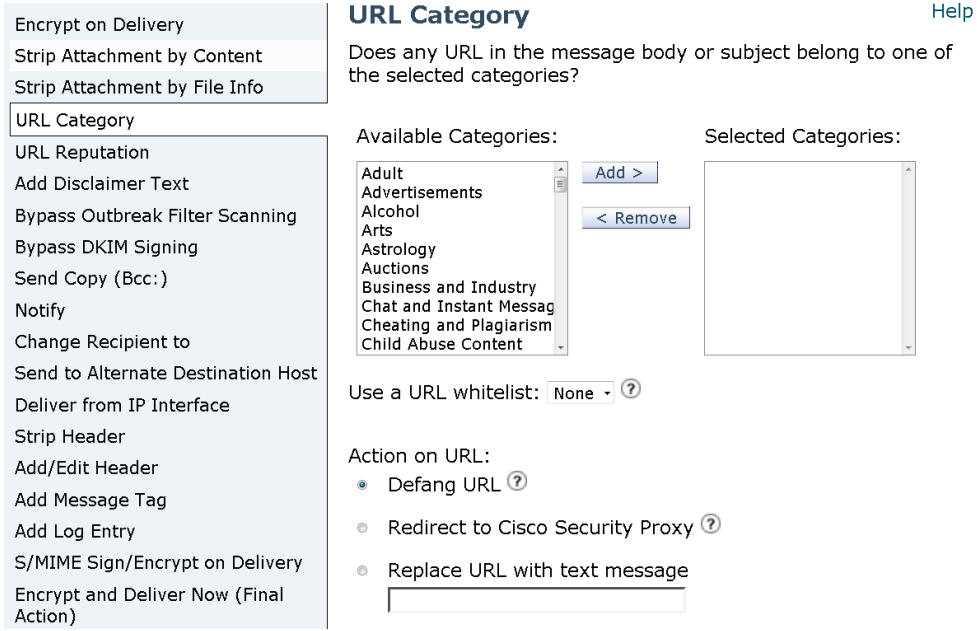
Click on the link below for your special offer!

http://randomofferurl.com

https://secure-web.cisco.com/1adjW1InNsH83UFDjLDFTjer5nJId9J-HjqKlbAcaLQ74EH5ViYESt C5jPZqvg_weQJeocAQeEryL5b1JR6T0JgzXkjk1PUMCBb_eQApCXS6ZsoujzgNvwt9UqN27SN1zcMVjmIpWQN__ITmALmHdGMZ_PaFf9FTUvmMc7UjRZBhvHzDvGJ0Lm5uh9evj_C_OemBAy44xbXwmYuA3uRPqKrf7T6ZNepA0MlcszDFPwufWUB7bbmS8Ziqh_-CyjG8KI6fJU33qjnInxHsjOBq98VxQUT-vMf_2U_OlpguXStzGTlj3U__yBZlLZsS9W1xLZpcGUKpdUp8Q_SBBq9HknQ/http%3A%2F%randomofferurl.com
Click or tap to follow

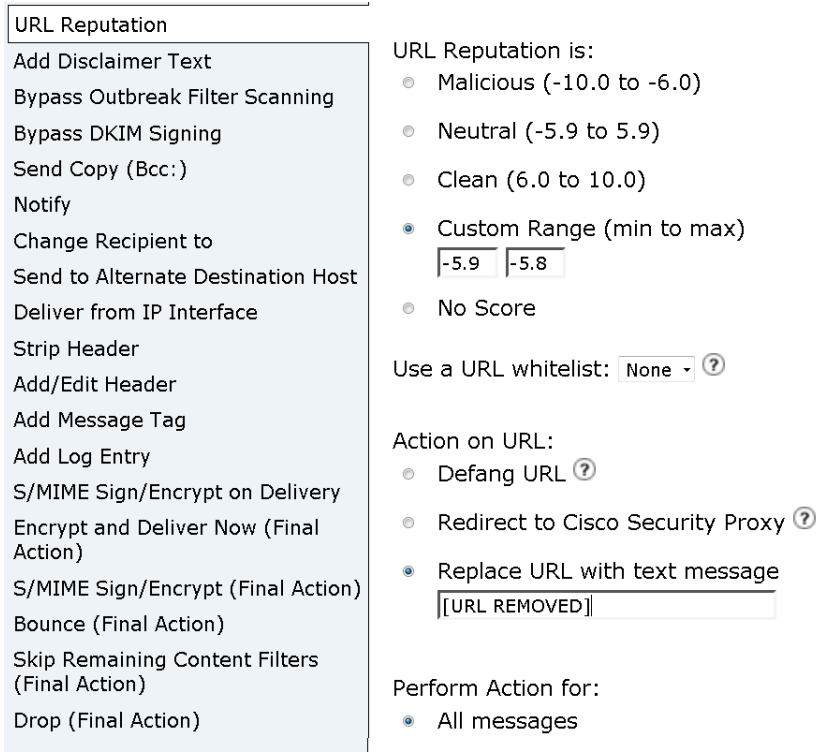
URL категоризация

- URL категоризация на ESA использует те же данные, что и Web Security Appliance (WSA)
- Используйте для дополнения политик использования, чтобы предотвратить нежелательные URL в почте



URL оценка и опции

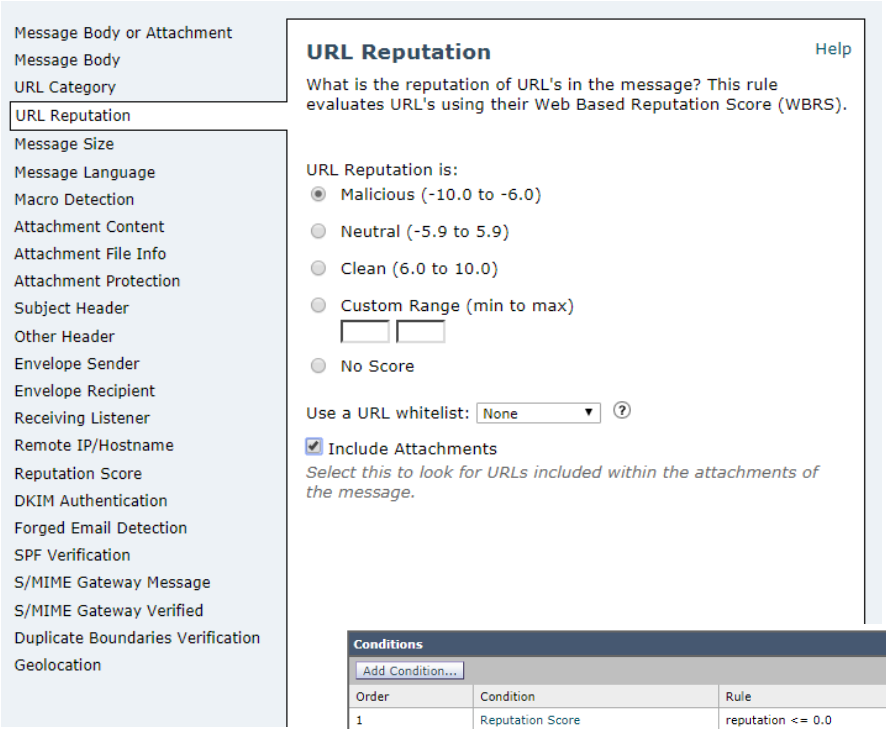
- Рекомендации:
  - Блок URL: -10 to -6
  - URL удаление: -5.9 to -5.8
  - Оставьте остальное для Outbreak Filters



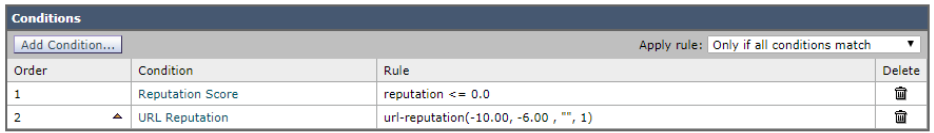
URLs в присоединенных файлах (11.1)

- Включите просмотр аттачей в Content или Message фильтрах для to perform URL reputation of links in documents
- Анализируются объекты Office / OLE (i.e doc, docx, xls, ppt, pdf)
- Если найдет вредоносный URL, предпринимается действие на все сообщение, а не на аттач.
- Ограничение на сканирование – 25, настраивается из CLI
- URLs в файле не перезаписывается

Структурирование эффективных правил для URLs в файлах

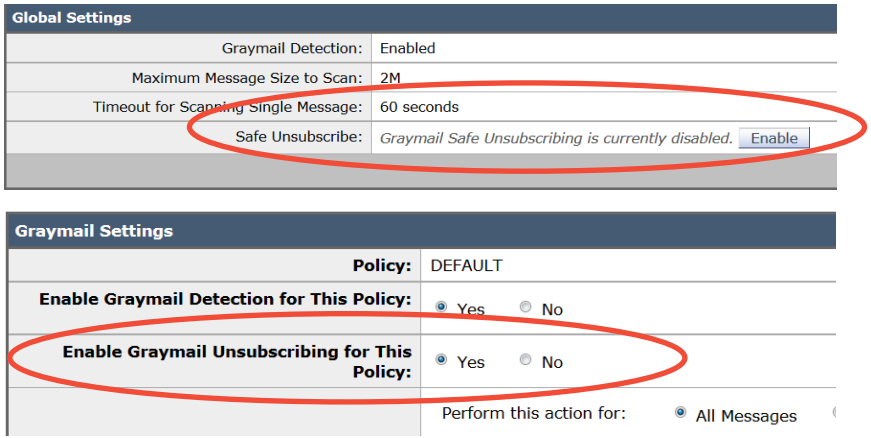


- Просмотр репутации не занимает много ресурсов, но тем не менее надо принимать это во внимание.
- Обрататывайте файли из недоверенных/неизвестных источников
- Используйте фильтры для того, чтобы избежать обработки глобально нежелательных или запрещенных файлов и уменьшить количество обрабатываемых



Graymail Unsubscribe

- Graymail Unsubscribe – это дополнительная лицензия
- Обеспечивает защиту от угроз, которые маскируются как ссылки unsubscribe
- Единый интерфейс для управления подписками для всех пользователей
- Лучшая видимость для email администраторов и пользователей для подобных писем



Graymail Unsubscribe

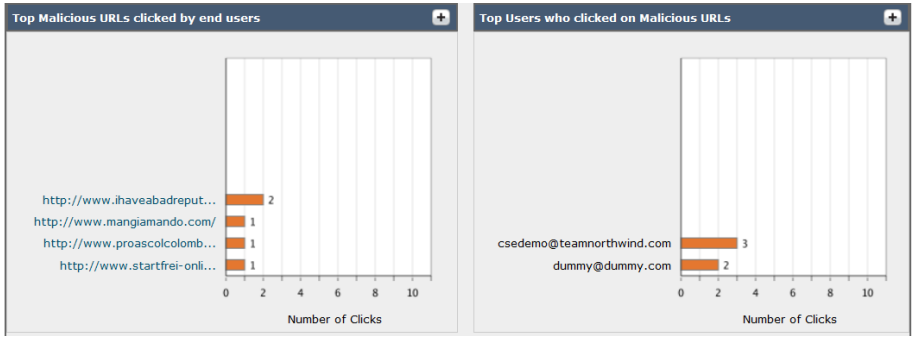
Пользователь кликает на перезаписанную ссылку Unsubscribe в письме

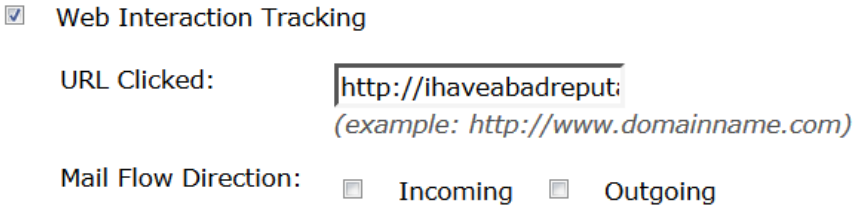
Проверка ссылки, если она безопасная, то переадресация на сервис Unsubscribe

Cisco выполняет отписывание от имени пользователя

Web Interaction Tracking & Reporting

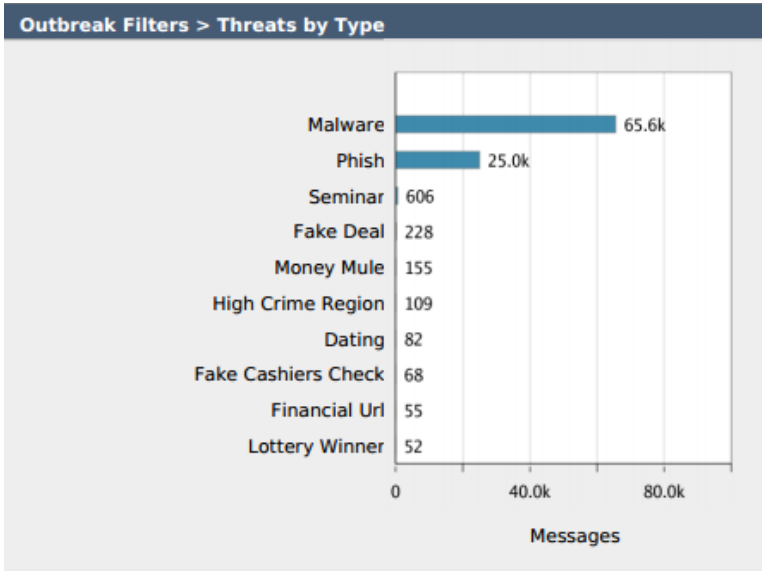
- Отчеты показывают важную информацию о том, кто кликнул на определенный URL
- Наибольшая ценность как инструмента обучения и понимания, кого могут атаковать в организации
- Страницы Reporting и Tracking покажут URLs (Tracking в 10.0 для деталей URL)



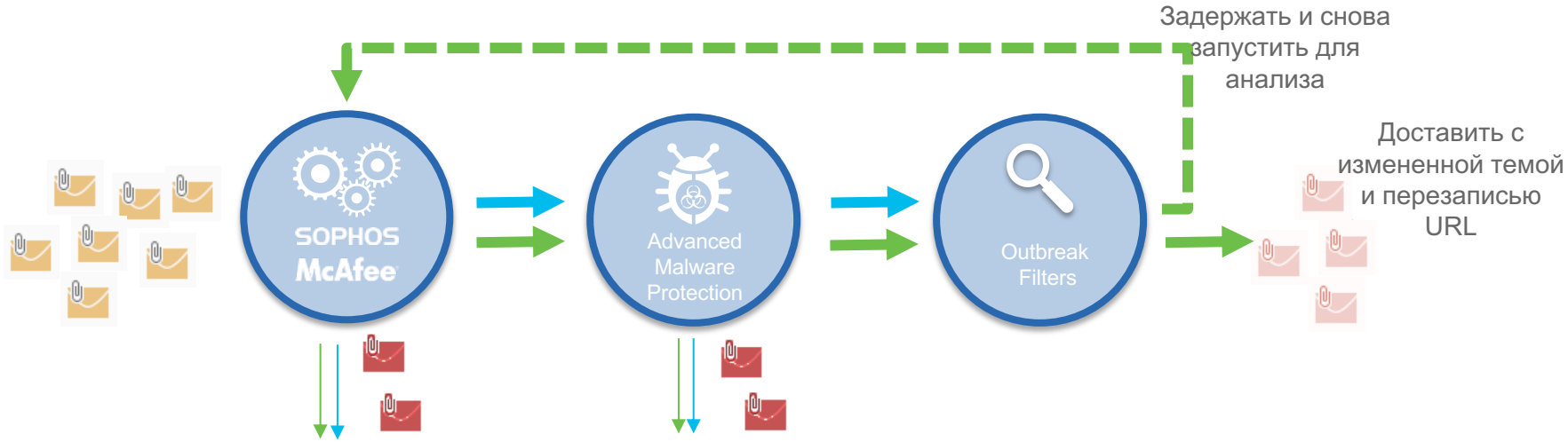


Фишинг – это не только URL

- Другие виды мошенничества -- банковское, отмывание денег, свидания, 419 и т.д. тоже используются для получения информации о целях.
- Смешанные угрозы комбинируют спуфинг и фишинг для того, чтобы выглядеть более легитимно в глазах цели
- Чтобы обнаружить и остановить подобные угрозы надо активировать Threat Outbreak Filters



Динамические карантины / задержка в карантине



Известные вредоносные файлы блокируются Sophos или McAfeee

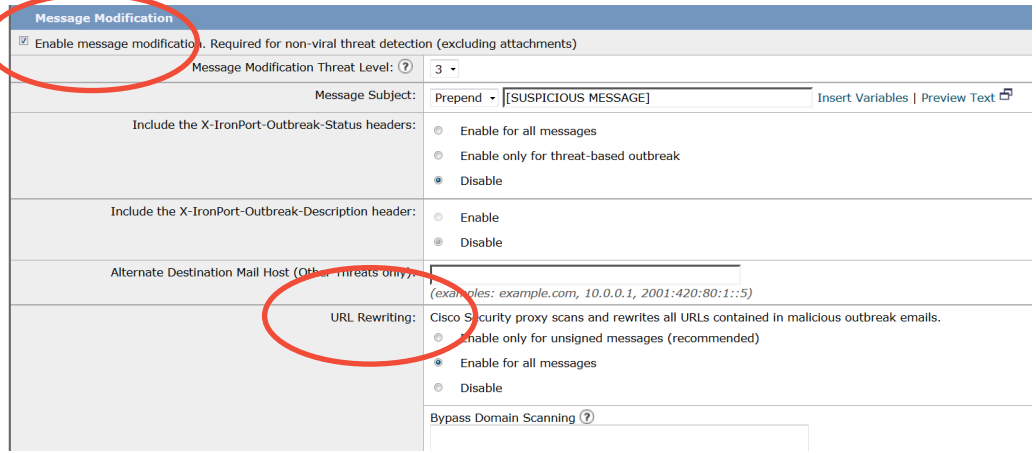
Репутация файлов, анализ, ретроспектива и реагирование для сканирования неизвестных файлов

Вручную созданные правила для задержки 0-Day malware для того, чтобы ограничить распространение

Threat Outbreak Filters

Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Quarantine MAR Action: Delete ...	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Deliver	FED_LOGHEADER	Retention Time: Virus: 1 day Other: 4 hours

- Включите Threat Outbreak Filters (не включено по умолчанию) с помощью включение Message Modification
- URL перезапись позволяет анализировать подозрительный URL облачным прокси (репутация, AV/AM, AMP



Предотвращение утечек данных

- Всегда может существовать пациент №0, и никто не сможет заблокировать все входящие попытки фишинга
- Мы можем создать правила для блокирования, каранина или шифрования данных, которые передаются из организации с помощью Content Filters или Data Loss Preventions
- Content Filters могут обнаруживать содержимое на основании регулярных выражений, словарей и объединяться с политиками доменов назначения

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	DLP	Delete
1	HR SENDERS	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	HR SSN POLICY	🗑
	Default Policy	Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver	Disabled	Disabled	Disabled	DEFAULT SSN POLICY	

Антиспуфинг

Обзор антиспуфинга

Тип	Кого подделывают	Цель спуфинга	Описание
Простой спуфинг	Внешние контрагенты	Ваши пользователи	Простой спуфинг – когда атакующий пытается изменить или манипулировать SMTP ENVELOPE FROM при SMTP обмене или изменяет поле reply-to для перенаправления писем
Похожий домен / Typo Squatting	Ваш бренд	Ваши клиенты	Атаки становятся более сложными и манипулируют написанием домена путем минимальных изменений в почтовых адресах, чтобы обмануть пользователей. Высокая вероятность успеха и сложность обнаружения в связи с большим количеством вариантов написания
Модификация отображаемого имени	Ваше руководство	Финансовые службы	Также называется Business Email Compromise (BEC). Это наиболее сложная из всех атак, она включает использование легитимных доменов (или похищенных, или созданных) и манипулирует заголовками сообщения для того, чтобы показать правильное имя отправителя и похожий домен/опечатку в адресе email, чтобы заставить пользователя отправить нужную информацию. Сейчас это одна из наиболее общих атак с очень высоким уровнем успешности

Влияние социальной инженерии

- Социальная инженерия добавила успешности спуфинг-атакам. Атакующие следят за целями месяцами, в социальных сетях, новостях и т.д.
- Создадут сообщения с «историей», чтобы добавить легитимности к запросу
- Они ищут событие – поездка за границу, большие сделки, соглашения и используют их для того, чтобы выразить срочность
- Кроме технических мер, основное средство для предотвращения атак – это *обучение пользователей*

Работа с простым спуфом

```
Mon Jun 26 16:48:31 2018 Info: New SMTP ICID 238970 interface Data 1 (216.71.129.13) address 72.142.13.157 reverse dns host
unallocated-static.rogers.com verified no
Mon Jun 26 16:48:31 2018 Info: ICID 238970 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None country Canada
Mon Jun 26 16:48:54 2018 Info: Start MID 137251 ICID 238970
Mon Jun 26 16:48:54 2018 Info: MID 137251 ICID 238970 From: <ceo@dinconsulting.com>
Mon Jun 26 16:49:09 2018 Info: MID 137251 ICID 238970 SMTP Call-Ahead bypass applied to <bob@dinconsulting.com>
Mon Jun 26 16:49:09 2018 Info: MID 137251 ICID 238970 RID 0 To: <bob@dinconsulting.com>
Mon Jun 26 16:49:40 2018 Info: MID 137251 Subject 'Re: Please pay this...'
Mon Jun 26 16:49:40 2018 Info: MID 137251 ready 202 bytes from <ceo@dinconsulting.com>
Mon Jun 26 16:49:40 2018 Info: MID 137251 matched all recipients for per-recipient policy DINCONSULTING in the inbound table
<scan results> …
```

- Обычно скомпрометированный узел на хостинг сервисе или динамическом IP
- В этом примере явная подделка внутреннего домена
- Без проверки на уровне подключения мало информации, которая поможет заблокировать это сообщение

Как это работает: SPF и DKIM

- Sender Policy Framework, описан в RFC4408
- Позволяет получателям проверять IP адреса отправителей с помощью просмотра DNS записей, в которых перечислены авторизованные шлюзы email для данного домена
- Использует DNS TXT записи
- Может проверять идентичность HELO/EHLO и MAIL FROM (FQDN)
- После оценки записей SPF, можно получить следующие результаты:

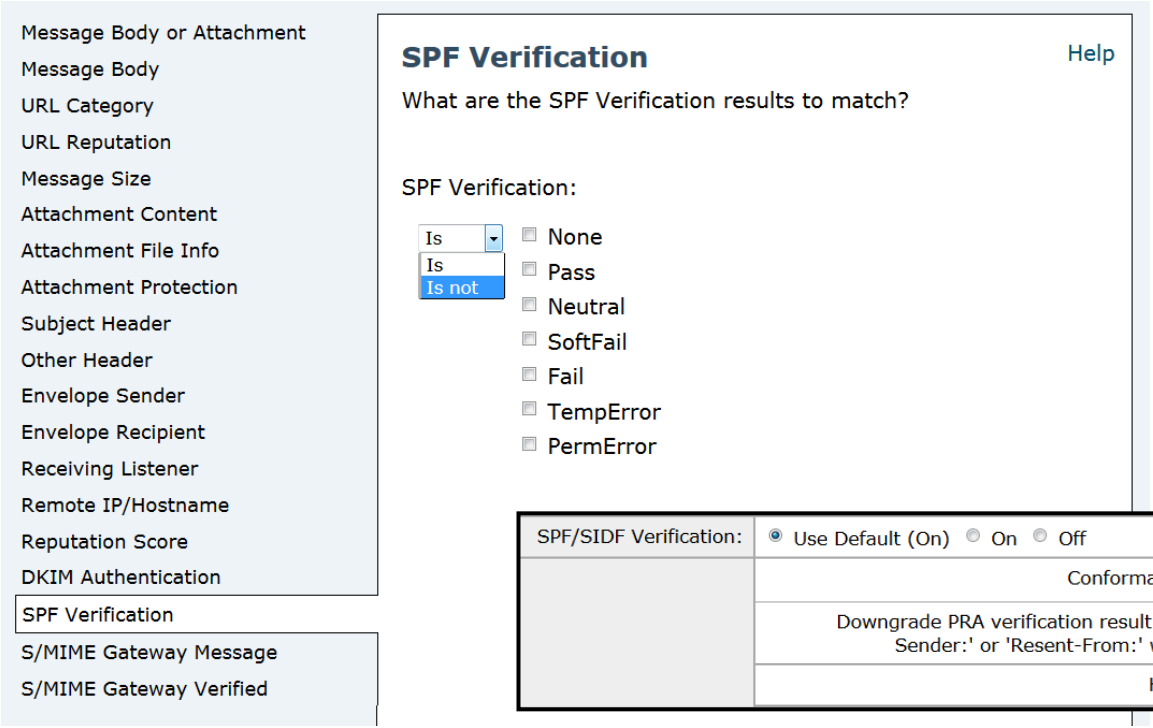
Результат	Объяснение	Рекомендуемое действие
Pass	SPF запись определяет, что узел имеет право отправлять	принять
Fail	SPF запись определяет, что хост не имеет право отправлять	отвергунть
SoftFail	SPF запрись определяет, что хост не имеет право отправлять, но пока идет переходных период	принять, но пометить
Neutral	SPF запись ничего не говорит про валидность	принять
None	У домена или нет SFP записи или запись не определена для данного узла	принять
PermError	Произошла постоянная ошибка (плохо отформатирована SPF запись)	не определено
TempError	Произошла временная ошибка (DNS Error)	принять или отвергнуть

Как это работает: SPF и DKIM

- Domain Keys Identified Mail, описан в RFC5585
- Кратко: Определяет методы криптографической подписи исходящих сообщений на шлюзе, включает проверочные данные в заголовок письма и пути, с помощью которых получатель будет **проверять целостность сообщения**
- Дополнительные RFC6376 (DKIM подписи), RFC5863 (DKIM развитие, развертывание и работа), RFC5617 (Author Domain Signing Practices (ADSP))
- Использует записи DNS TXT для публикации публичных ключей

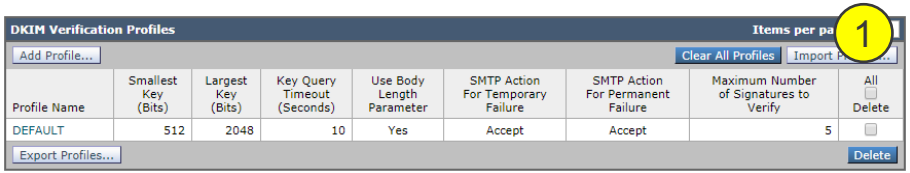
```
20120113._domainkey.gmail.com IN TXT “k=rsa\; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Kd87/UeJjenpabg
bFwh+eBCsSTrqmwIYYvywlbhbqoo2DymndFkbjOVIPIldNs/m40KF+yzMn1skyoxcTUGCQs8g3FgD2Ap3ZB5DekAo5wMmk4wimDO+U8QzI3SD
0""7y2+07wlNWwIt8svnxgdxGkVbbhzY8i+RQ9DpSVpPbF7ykQxtKXkv/ahW3KjViiAH+ghvvIhkx4xYSIc9oSwVmAl5OctMEeWUwg8Istjqz
8BZeTWbf41fbNhte7Y+YqZOwq1Sd0DbvYAD9NOZK9vlfuac0598HY+vtSBczUiKERHv1yRbcaQtZFh5wtiRrN04BLUTD21MycBX5jYchHjPY/
wIDAQAB”
```

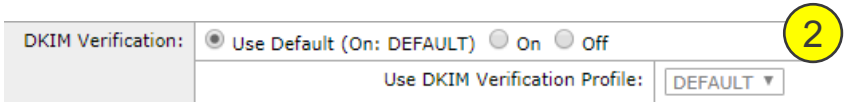
Включение проверки SPF

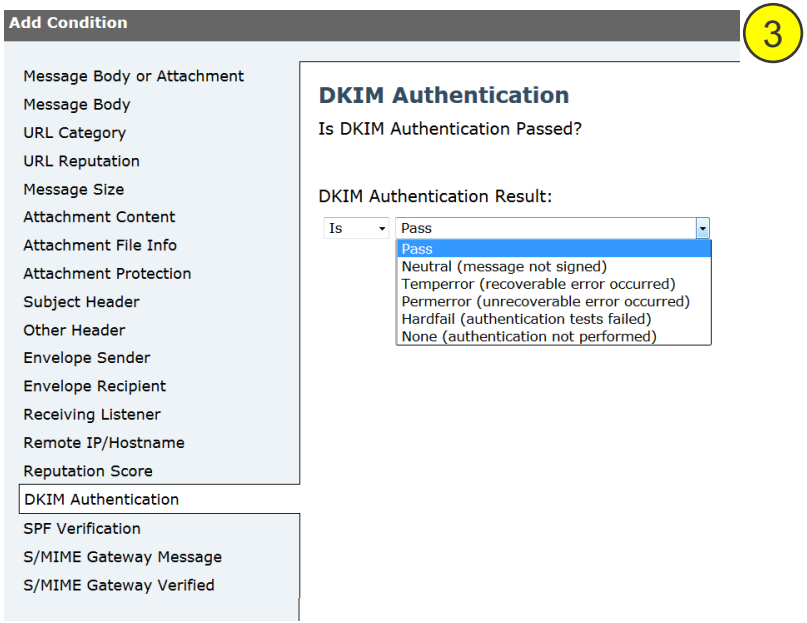


- Когда включен SPF, ESA будет «штамповать» заголовки сообщения
- Используйте результат внутри сообщения или Content Filters для определения действия
- PRA идентификаторы оцениваются только в Message Filters
- SPF vs SIDF, почитайте, это интересно: http://www.openspf.org/SPF_vs_Sender_ID

Включение проверки DKIM







1. Создайте профиль для действиях в DKIM (по умолчанию Monitor)
2. Включите проверку DKIM в Mail Flow Polices
3. Настраивайте действия в Content Filters. Используйте отправку писем в карантин для пересмотра поддельных сообщений

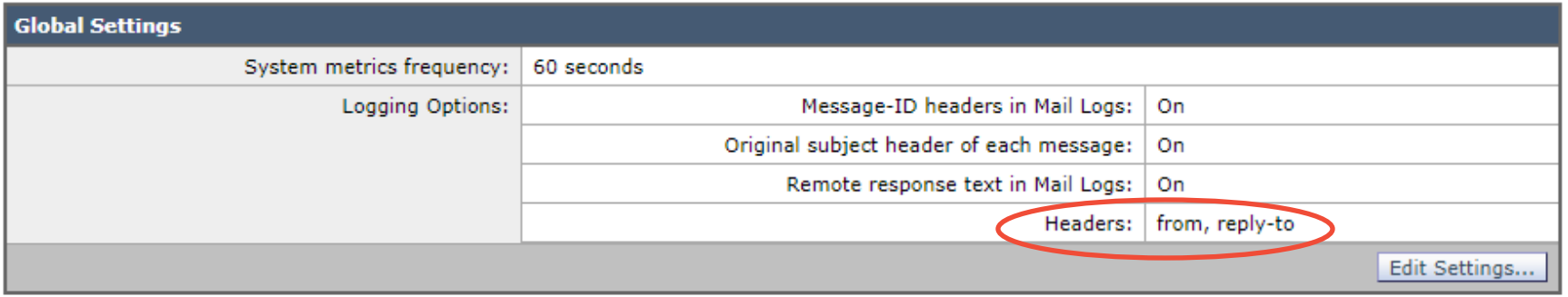
После включения SPF

```
Mon Jun 26 16:48:31 2018 Info: New SMTP ICID 238970 interface Data 1 (216.71.129.13) address 72.142.13.157 reverse dns host
unallocated-static.rogers.com verified no
Mon Jun 26 16:48:31 2018 Info: ICID 238970 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None country Canada
Mon Jun 26 16:48:54 2018 Info: Start MID 137251 ICID 238970
Mon Jun 26 16:48:54 2018 Info: MID 137251 ICID 238970 From: <ceo@dinconsulting.com>
Mon Jun 26 16:49:09 2018 Info: MID 137251 ICID 238970 SMTP Call-Ahead bypass applied to <bob@dinconsulting.com>
Mon Jun 26 16:49:09 2018 Info: MID 137251 ICID 238970 RID 0 To: <bob@dinconsulting.com>
Mon Jun 26 16:49:18 2018 Info: MID 137251 SPF: helo identity postmaster@dinconsulting.com Fail (v=spf1)
Mon Jun 26 16:49:18 2018 Info: MID 137251 SPF: mailfrom identity ceo@dinconsulting.com Fail (v=spf1)
Mon Jun 26 16:49:40 2018 Info: MID 137251 SPF: pra identity  None headers None
Mon Jun 26 16:49:40 2018 Info: MID 137251 Subject 'Re: Please pay this...'
Mon Jun 26 16:49:40 2018 Info: MID 137251 ready 202 bytes from <ceo@dinconsulting.com>
Mon Jun 26 16:49:40 2018 Info: MID 137251 matched all recipients for per-recipient policy DINCONSULTING in the inbound table
<scan results> …
```

SPF запись: TXT="v=spf1 include:spf.protection.outlook.com -all"

- Поле включения SPF вы получаете дополнительную информацию об отправителе
- Мы все еще принимаем сообщения, но мы можем позже использовать вердикт для того, чтобы принять решение об обвинении сообщения
- Эффективность ограничена участием – надо потратить время, чтобы убедиться, что SPF записи вовремя обновляются

Логирование дополнительных заголовков



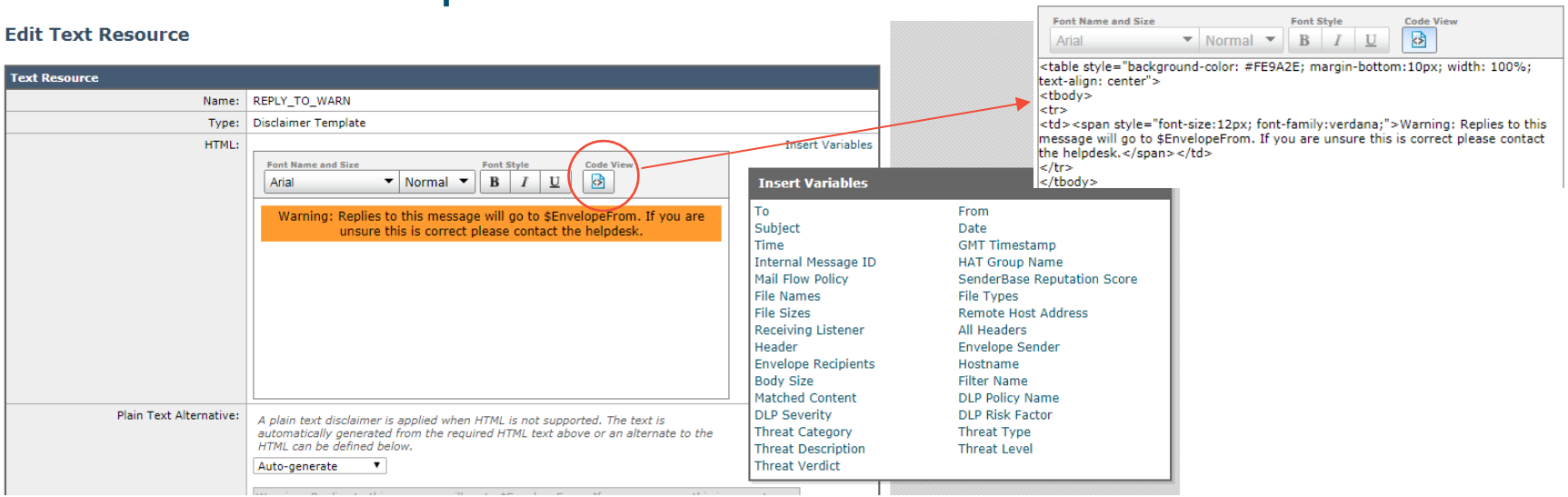
Global Settings		
System metrics frequency:	60 seconds	
Logging Options:	Message-ID headers in Mail Logs:	On
	Original subject header of each message:	On
	Remote response text in Mail Logs:	On
	Headers:	from, reply-to

Edit Settings...

```
Sat Jun 17 05:29:54 2018 Info: MID 94398 ICID 188033 From: <bob@gmail.com>
Sat Jun 17 05:29:54 2018 Info: Message done DCID 1496 MID 94399 to RID [0] [('from', 'Uncle Bob <bob@gmail.com>')]
```

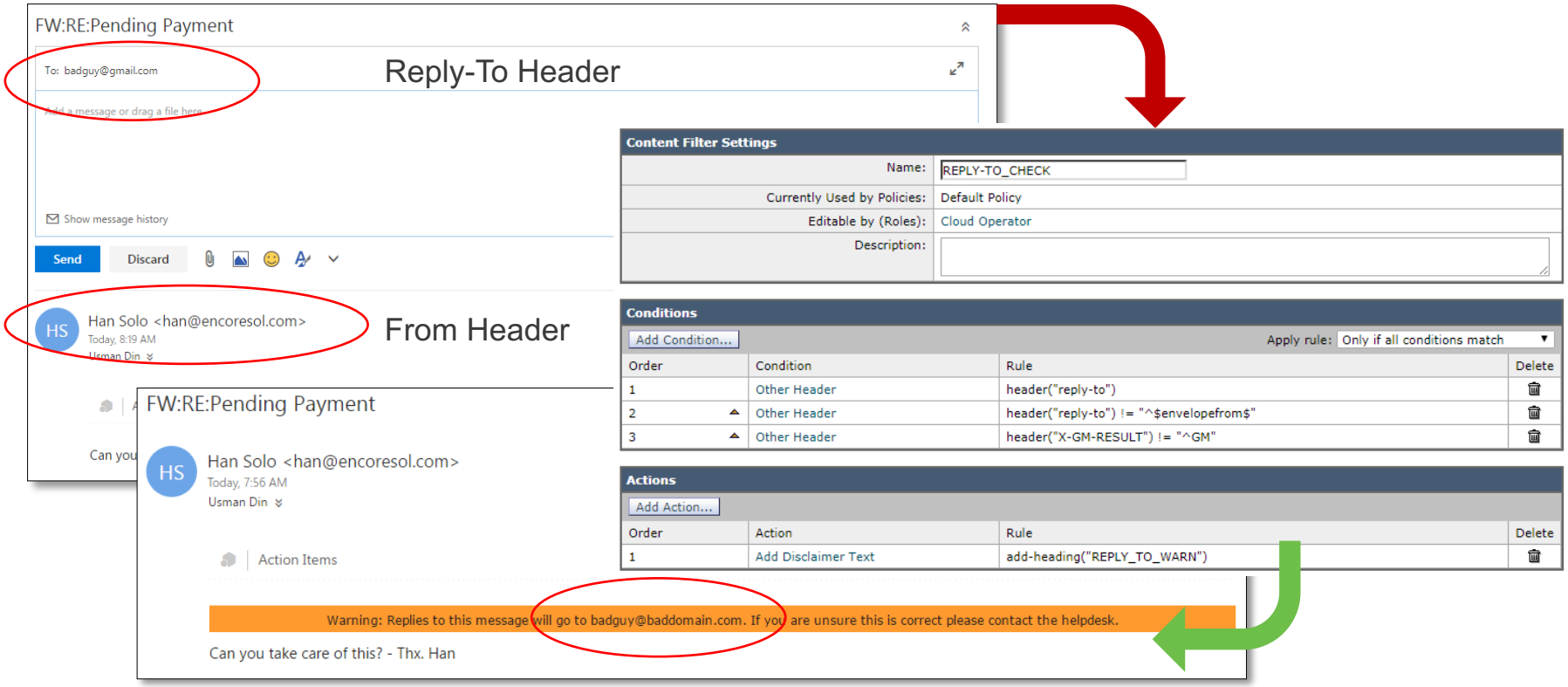
- В настройках Log Subscriptions или с помощью CLI команды logconfig, you вы можете настроить логирование дополнительных заголовков письма
- Эта информация будет показываться в mail_logs и выводе message tracking при создании DCID (Delivery Connection ID)

Disclaimers и переменные



- Вы можете создать большое количество текстовых ресурсов, которые можно использовать в фильтрах как действия для подозрительных сообщений
- Переменные могут использоваться внутри текстовых ресурсов и в content / message фильтрах

Обнаружение несоответствия Reply-To



Похожие домены и Typo-Squatting

- Обычно нацеливаются на определенный хорошо известный бренд
- Использует разные наборы техник пытаясь обмануть пользователя и заставить его поверить отправителю
- Регистрирует домен и создает записи SPF, DKIM и DMARC
- Легитимизирует хост-отправитель правильными записями DNS и rDNS.

пример: cisco.com

Addition: ciscoo.com

Bitsquatting: cicco.com

Homoglyph: c1sco.com

Insertion: ciseco.com

Omission: cico.com

Repetition: cissco.com

Replacement: cizco.com

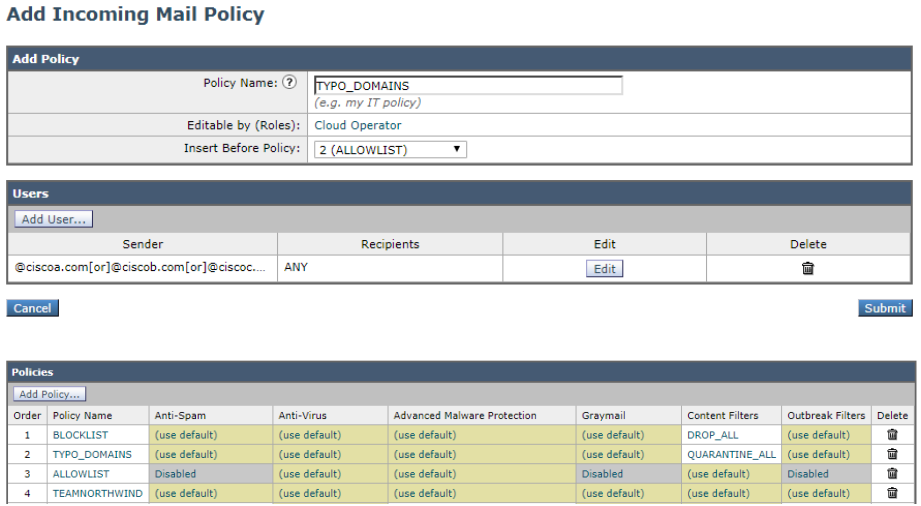
Subdomain: c.isco.com

Transposition: csico.com

Использование

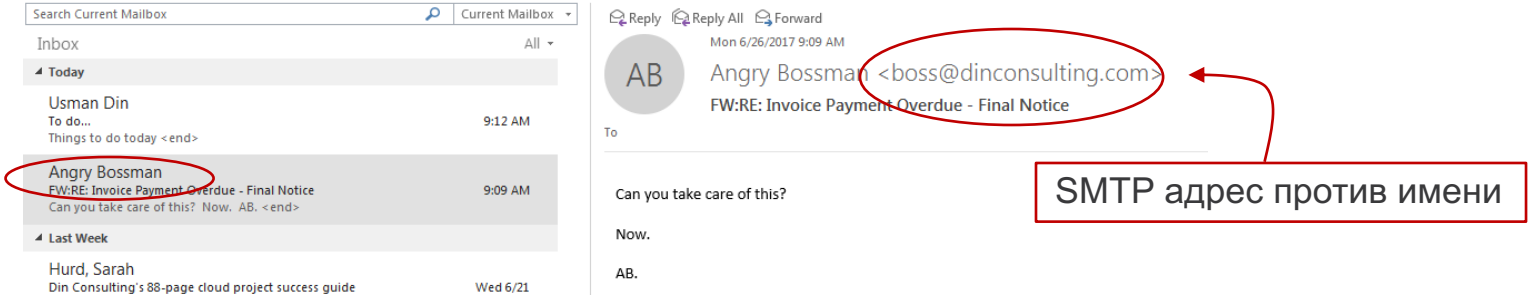
Главная страница: https://github.com/elceef/dnstwist

```
 __| |_ __  ___| |___      _(_)___| |_
 / _` | '_ \/ __| __\ \ /\ / / / __| __|
| (_| | | | \__ \ |_ \ V  V /| \__ \ |_
 \__,_|_| |_|___/\__| \_/\_/ |_|___/\__| {1.03}

Processing 140 domain variants
....................................22%.....................44%
.......65%...........85%.... 85 hits (60%)

Original*       cisco.com       72.163.4.161 2001:420:1101:1::a
Addition        ciscoa.com      52.7.234.86
Addition        ciscob.com      -
Addition        ciscoc.com      103.224.182.238
Addition        ciscod.com      184.168.221.45
Bitsquatting    cmsco.com       50.204.65.37
Bitsquatting    casco.com       208.73.210.202
Bitsquatting    cysco.com       121.254.178.253
Bitsquatting    circo.com       208.73.210.202
Bitsquatting    cicco.com       146.112.61.107
Homoglyph       cisc0.com       66.45.246.141
Homoglyph       c1sco.com       -
Homoglyph       clsco.com       64.254.28.227
Repetition      cissco.com      146.112.61.107
Replacement     cisci.com       185.65.56.178
Subdomain       cisc.o.com      -
Transposition   icsco.com       205.178.189.131
Transposition   csico.com       23.236.62.147
```



Модификация имени

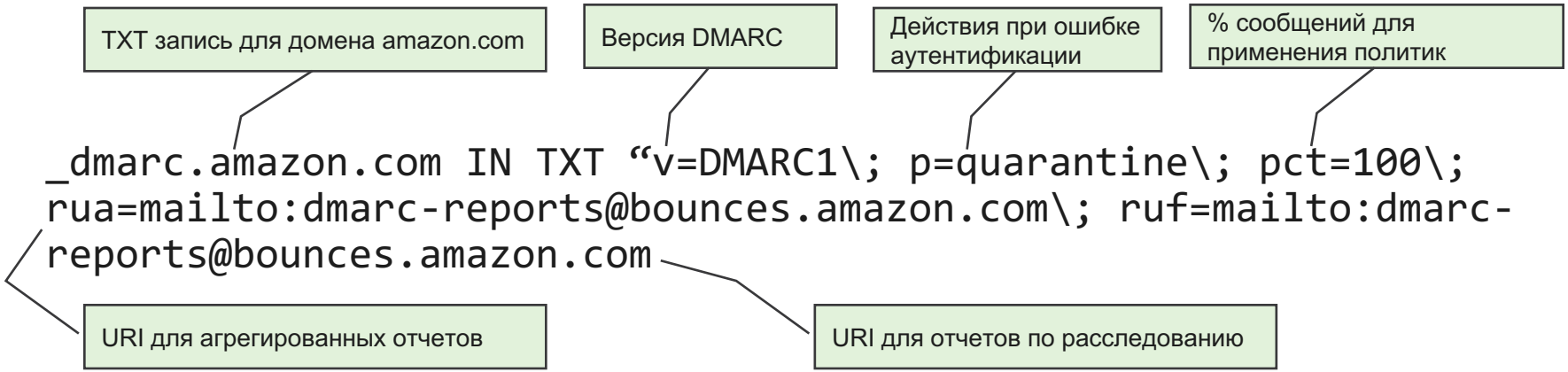
```
Mon Jun 26 18:07:54 2018 Info: MID 137261 ICID 239041 From: <reallybad@gmail.com>
Mon Jun 26 18:08:07 2018 Info: MID 137261 ICID 239041 RID 0 To: <usman@dinconsulting.com>
Mon Jun 26 18:08:10 2018 Info: MID 137261 SPF: SPF: helo identity postmaster@mail-wr0-f180.google.com None
Mon Jun 26 18:08:10 2018 Info: MID 137261 SPF: mailfrom identity reallybad@gmail.com Pass (v=spf1)
Mon Jun 26 18:09:15 2018 Info: MID 137261 SPF: pra identity boss@dinconsulting.com None headers from
Mon Jun 26 18:09:15 2018 Info: MID 137261 DKIM: pass signature verified (d=gmail.com s=20161025 i=@gmail.com)
Mon Jun 26 18:09:15 2018 Info: MID 137261 Subject 'FW:RE: Invoice Payment Overdue - Final Notice'
Mon Jun 26 18:09:15 2018 Info: MID 137261 ready 304 bytes from <reallybad@gmail.com>
Mon Jun 26 18:09:15 2018 Info: MID 137261 matched all recipients for per-recipient policy DINCONSULTING in the inbound table
…<scan engines>…
…<start delivery>…
Mon Jun 26 18:09:21 2018 Info: Message done DCID 1555 MID 137261 to RID [0] [('from', 'Angry Bossman <boss@dinconsulting.com>',
('reply-to', 'badguy@gmail.com'))]
```



Как это работает: DMARC

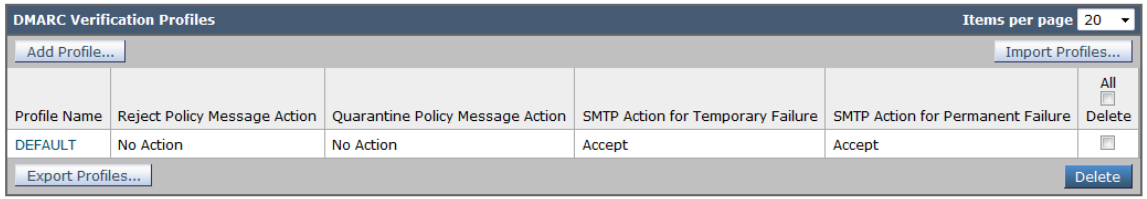
- Как DKIM, так и SPF имеют недостатки. Не из-за плохого дизайна, а из-за разной природы каждой из технологий.
- Таким образом, родился DMARC:
  - Использование существующих технологий, предоставление среды для их синхронизации и позволяет **отправителям** получить полномочия по управлению политиками блокировки и иметь видимость поддельного трафика
- Domain-based Message Authentication, Reporting And Conformance
  - Определен в RFC 7489
  - Обеспечивает:
    - DKIM проверку
    - SPF аутентификацию
    - **Синхронизацию между идентификаторами отправителя (Envelope From, Header From)**
    - Сообщает о поддельном объекте

Как это работает: структура записи DMARC

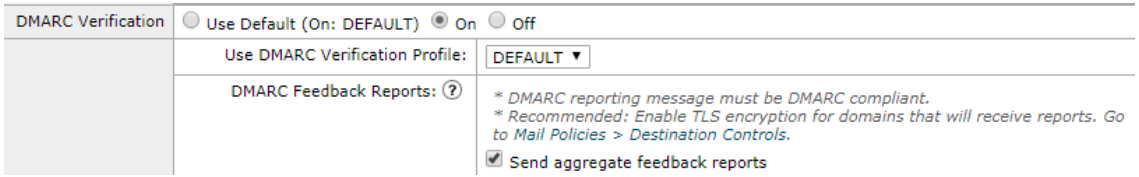


Как включить DMARC

1



2



- DMARC настраивается с помощью определения профиля и применения профиля к Mail Flow Policy
- По умолчанию профиль стоит в режиме Monitor для нарушений DMARC, но для оценки DMARC записей надо применить политику
- Выполняйте мониторинг параметров и настраивайте их, когда будете готовы, переходите в режим блокировки

Как работает DMARC

DMARC Verification Profiles — Items per page: 20

Add Profile... | Import Profiles...

Profile Name	Reject Policy Message Action	Quarantine Policy Message Action	SMTP Action for Temporary Failure	SMTP Action for Permanent Failure	All Delete
BLOCKING	Reject	Quarantine	Accept	Accept	
DEFAULT	No Action	No Action	Accept	Accept	

Export Profiles... | Delete

v=DMARC1; p=reject; pct=100; rua=mailto:dmarc_y_rua@yahoo.com

```
Tue Jun 27 00:09:24 2018 Info: MID 140370 ICID 242100 From: root@cannon.teamnorthwind.com
Tue Jun 27 00:09:24 2018 Info: MID 140370 ICID 242100 RID 0 To: usman@dinconsulting.com
Tue Jun 27 00:09:24 2018 Info: MID 140370 SPF: helo identity postmaster@cannon-master None
Tue Jun 27 00:09:24 2018 Info: MID 140370 SPF: mailfrom identity root@cannon.teamnorthwind.com None
Tue Jun 27 00:09:25 2018 Info: MID 140370 SPF: pra identity gguy@yahoo.com None headers from
Tue Jun 27 00:09:25 2018 Info: MID 140370 DMARC: Message from domain yahoo.com, DMARC fail, (SPF
aligned False, DKIM aligned False) DMARC policy is reject, applied policy is reject
Tue Jun 27 00:09:25 2018 Info: MID 140370 DMARC: Verification failed.
Tue Jun 27 00:09:25 2018 Info: MID 140370 DMARC: Message rejected by DMARC policy.
Tue Jun 27 00:09:25 2018 Info: MID 140370 rejected by DMARC policy
Tue Jun 27 00:09:25 2018 Info: Message aborted MID 140370 Receiving aborted
```

Инструменты, которые помогут запустить DMARC

DMARC Lookup Tools:

https://www.agari.com/project/dmarc/, https://www.valimail.com/dmarc/domain-checker#/

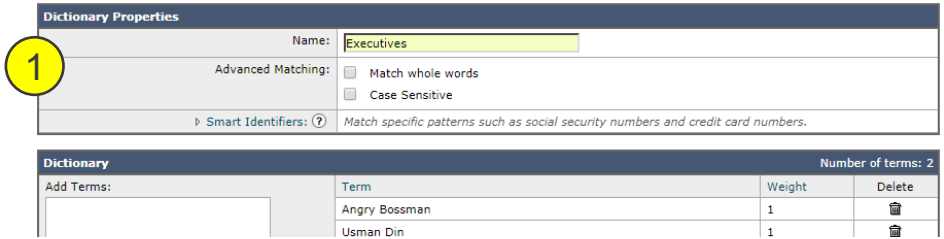
DMARC Wizard:

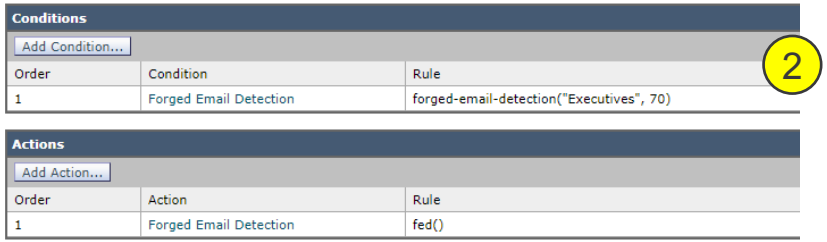
https://dmarc.globalcyberalliance.org/

DMARC Aggregation Reporting Tool (БЕСПЛАТНО!)

http://dmarc.postmarkapp.com/

Forged Email Detection – Нечеткое соответствие заголовков






```
MID 143464 Forged Email Detection on the From: header with score of 100
Info: Message done DCID 1570 MID 143464 to RID [0] [('From', 'Angry Bossman <angryboss@gmail.com>']
```

- Идея, которая лежит за технологией Forged Email Detection -- это предоставить метод поиска соответствия имени, которое отображается в почтовом клиенте (Display Name) именам руководящего персонала
- Эта функция может помочь сузить целевой спуфинг, использовать любое действия в content / message фильтрах, также вы можете убрать заголовок From для того, чтобы показать реальный Envelope From
- **Использование его приводит к ложным срабатываниям**! Используйте его вместе с другими правилами

Что мы ищем?

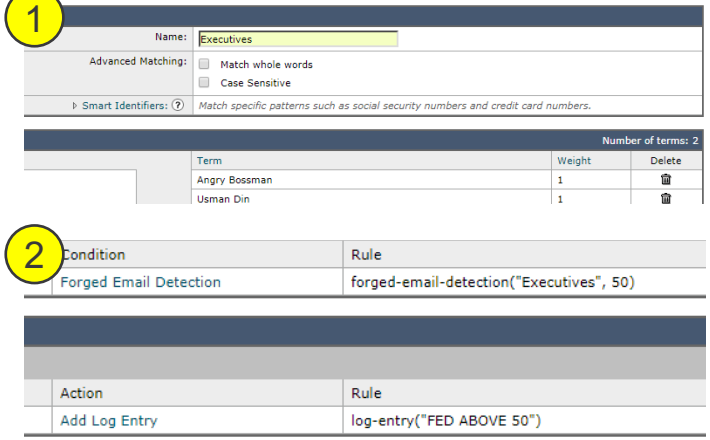
- Forged Email Detection ищет соответсвия Header From (RFC5322) а именно Display Name (т.е. First Last <user@domain.com>)
- В ранних релизах были проблемы с эффективностью, которые были исправлены в **v10.0.3+ и v11.0.1+**
- Примеры соответствий:

```
Amgry Bossman -> Forged Email Detection on the From: header with score of 93
Angerry Bossman -> Forged Email Detection on the From: header with score of 92
Angry Bosman -> Forged Email Detection on the From: header with score of 96
Angry B0ssman -> Forged Email Detection on the From: header with score of 93
Angry Bossm4n -> Forged Email Detection on the From: header with score of 92
Andry Bossman  -> Forged Email Detection on the From: header with score of 92
```

Начало работы с FED

- FED только создает запись в логе, если граничное значение выше или равно тому, которое настроено
- Начните с создания фильтра с низким граничным значением и сохраняйте результаты для каждого значения выше границы
- Включите логирование заголовков From и Reply-To

1



2

Condition	Rule
Forged Email Detection	forged-email-detection("Executives", 50)

Action	Rule
Add Log Entry	log-entry("FED ABOVE 50")

3

```
New SMTP ICID 452471 interface Data 1 (216.71.132.15) address 45.55.251.155 reverse dns host unknown verified no
ICID 452471 ACCEPT SG BYPASSLIST match 45.55.251.155 SBRS None country United States
Start MID 126811 ICID 452471
MID 126811 ICID 452471 From: <root@cannon.teamnorthwind.com>
MID 126811 ICID 452471 SMTP Call-Ahead bypass applied to <usman@encoresol.net>
MID 126811 ICID 452471 RID 0 To: <usman@encoresol.net>
MID 126811 Message-ID '<20171220212032.GA13397@cannon.teamnorthwind.com>'
MID 126811 Subject 'hello'
MID 126811 ready 569 bytes from <root@cannon.teamnorthwind.com>
MID 126811 matched all recipients for per-recipient policy ENCORESOL_NET in the inbound table
ICID 452471 close
MID 126811 interim verdict using engine: CASE spam negative
MID 126811 using engine: CASE spam negative
MID 126811 interim AV verdict using Sophos CLEAN
MID 126811 antivirus negative
MID 126811 AMP file reputation verdict : CLEAN
MID 126811 using engine: GRAYMAIL negative
MID 126811 Forged Email Detection on the From: header with score of 92, against the dictionary entry Angry Bossman
MID 126811 Custom Log Entry: FED ABOVE 50
MID 126811 Outbreak Filters: verdict negative
MID 126811 queued for delivery
Delivery start DCID 0 MID 126811 to RID [0]
Message done DCID 0 MID 126811 to RID [0] [('from', 'Andry Bossman <angry@encoresol.com>')]
MID 126811 RID [0] Response '/dev/null'
Message finished MID 126811 done
```

Примеры фильтра Forged Email Detection

Перед FED()

FW:RE: Invoice Payment Overdue - Final Notice

AB Angry Bossman <boss@dinconsulting.com>

Can you take care of this?

Now.

После FED()

FW:RE: Invoice Payment Overdue - Final Notice

R root@cannon.teamnorthwind.com

Strip From header

Insert Disclaimer

Warning: The email has been flagged as a potential spoof. If you are unsure of the sender do not reply or open links and contact the helpdesk.

Conditions

Add Condition... Apply rule: Only if all conditions match

Order	Condition	Rule	Delete
1	Reputation Score	reputation <= -1.0	
2	Forged Email Detection	forged-email-detection("Executives", 70)	

Actions

Add Action...

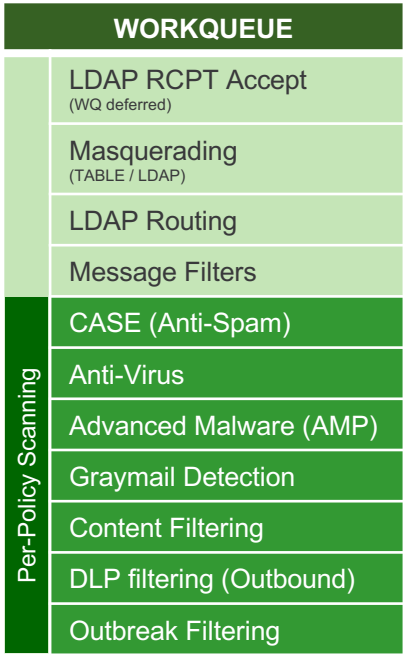
Order	Action	Rule	Delete
1	Forged Email Detection	fed()	
2	Add Disclaimer Text	add-heading("FED_WARN")	

- В этом примере мы добавили значение репутации отправителя для того, чтобы сфокусироваться на соответствии недоверенным отправителям
- Используя Forged Email Detection мы можем предпринять дополнительные требуемые действия
- Используйте вместе с программой обучения пользователей

Добавление информационных x-headers

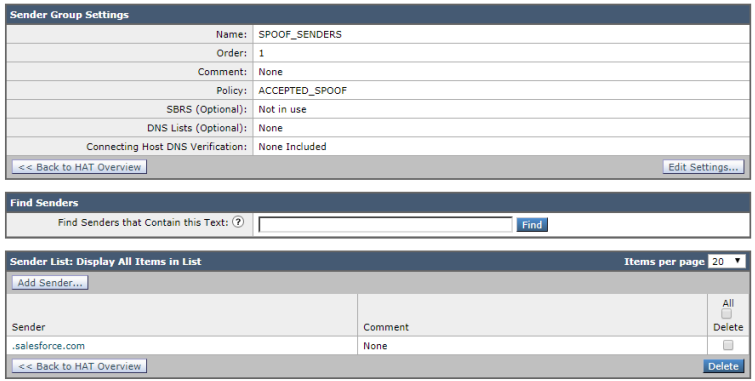
- Используйте Message Filters для того, чтобы проштамповать x-headers, которые используют переменные
- Может использоваться для решения проблем с сообщениями в почтовом ящике пользователя
- Также можно использовать для запуска Content Filters позже в процессе обработки

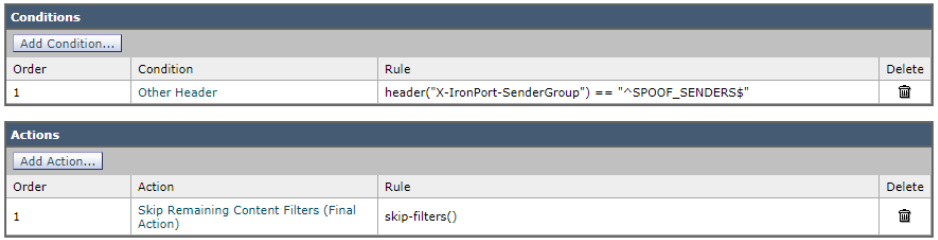
```
addHeaders:  if (sendergroup != "RELAYLIST")
{
     insert-header("X-IronPort-RemoteIP", "$RemoteIP");
     insert-header("X-IronPort-MID", "$MID");
     insert-header("X-IronPort-Reputation", "$Reputation");
     insert-header("X-IronPort-Listener", "$RecvListener");
     insert-header("X-IronPort-SenderGroup", "$Group");
     insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```



Разрешенные поддельные источники

- Существуют варианты, когда внешние организации отправляют почту вашим пользователям от имени вашей организации
- Разрешение подобный действий надо создать правила для того, чтобы выключить проверку соединений и любые проверки заголовков
- Создайте Mail Flow Policy для обходаSBRS, DMARC, SPF, and DKIM
- Вы можете дополнительно использовать x-headers для того, чтобы принять решение об обработке письма на основании соответствия SenderGroups





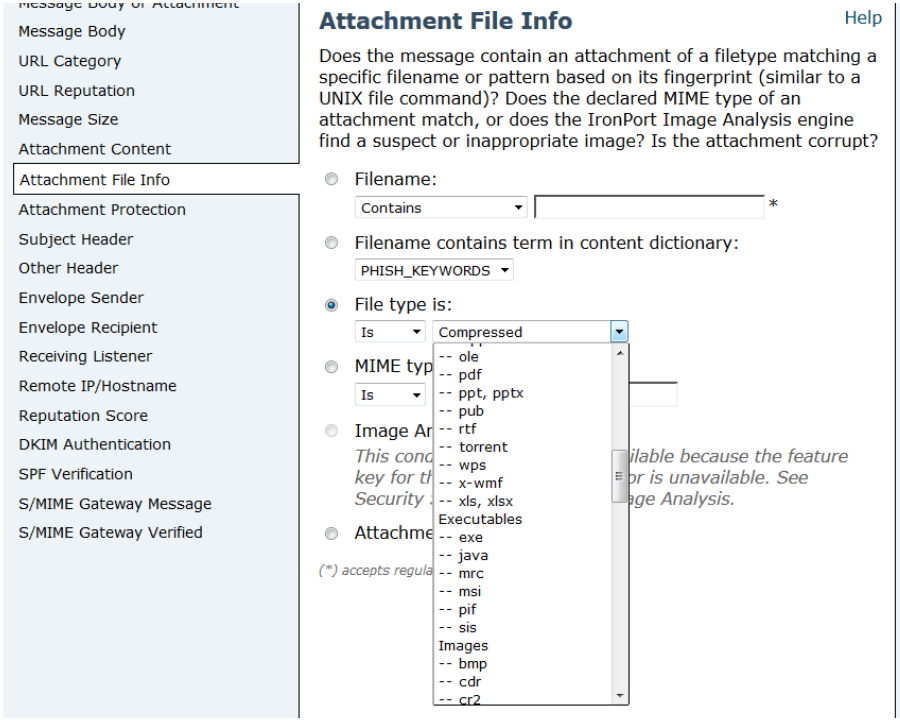
Проверочная таблица антифишинга/антиспуфинга

- Включите URL фильтрацию на ESA
- Включите Web Interaction Tracking (если разрешено политикой)
- Включите для администрарово видимость URL в Message Tracking(если разрешено политикой)
- Включите Threat Outbreak Filtering и модификацию сообщений – предупредите ваших пользователей!
- Партнерские URL поместите в белый список, используйте значения репутации для остальных
- Объединяйте репутационные правила и используйте детектор языков как часть логики.
- Используйте политики для определенияуровня блокировки в наборах правил.
- Создайте план для внедрения SPF, DKIM и DMARC
- Знайте, кому разрешено отправлять почту от вашего имени и отслеживайте их фильтрами и политиками.
- Постройте список исключений, ловите всех остальных
- Начиная с версии 10.0 используйте функцию Forged Email Detection для того, чтобы искать соответствия Display Name, если есть близкое совпадение, удаляйте заголовок From
- Отправляйте копию подозрительных спуф-писем в карантин для анализа и затем настраивайте политики чтобы начать блокировать сообщения.

Управление присоединенными файлами и защита от них

Блокирование нежелательных типов файлов

- С помощью Content/Message фильтров вы можете определить как обрабатывать файлы на основании политик.
- В общем случае клиенты создают фильтры для блокирования нежелательных типов файлов
- Использование предопределенных библиотек упрощает процесс
- Система обнаруживает измененные расширения или попытки скрыть файлы в множественных архивах для того, чтобы избежать блокировки.



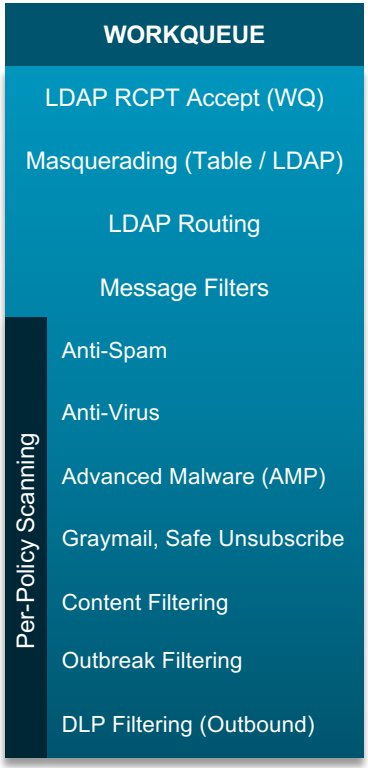
Блокирование на ранних этапах обработки

- Если файлы должны быть сброшены (исполняемые файлы), то желательно это сделать как можно раньше, для сохранения ресурсов системы

```
strip_all_exes: if (true) {
drop-attachments-by-filetype ('Executable', "Removed attachment:
$dropped_filename");}
```

- Все неокончательные действия, такие как карантин продолжают обрабатывать письмо с файлов и к нему могут применяться другие вердикты

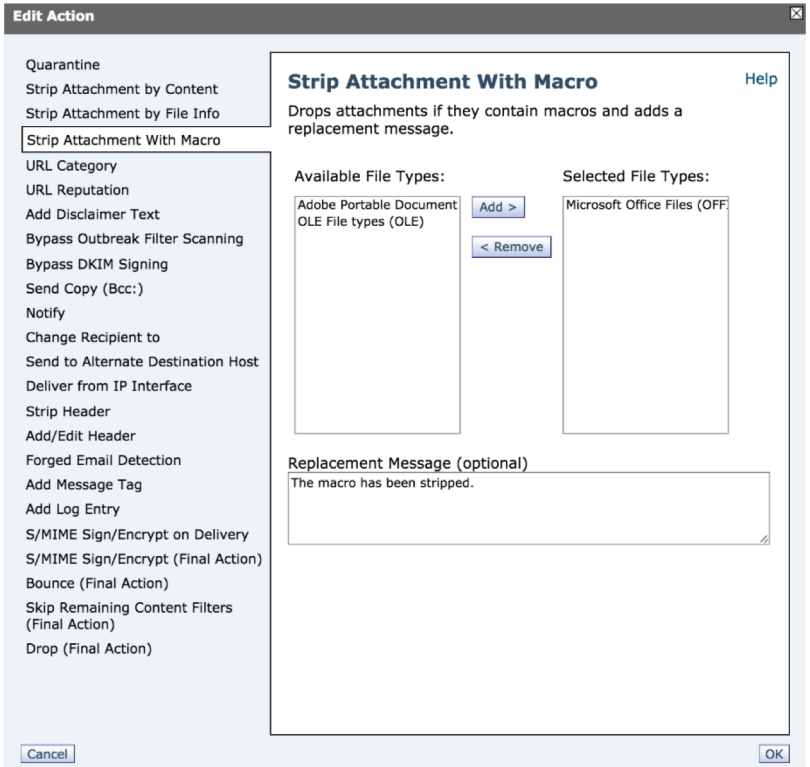
Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters
(use default)	Disabled	(use default)	(use default)	(use default)	(use default)
(use default)	Disabled	(use default)	(use default)	(use default)	(use default)
IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Quarantine MAR Action: Delete ...	Graymail Detection Unsubscribe: Enabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	FED_LOGHEADER FED_STRIPHEADER LOG_URL BLOCK_URLS BLOCK_FILETYPES ...	Retention Time: Virus: 1 day Other: 4 hours



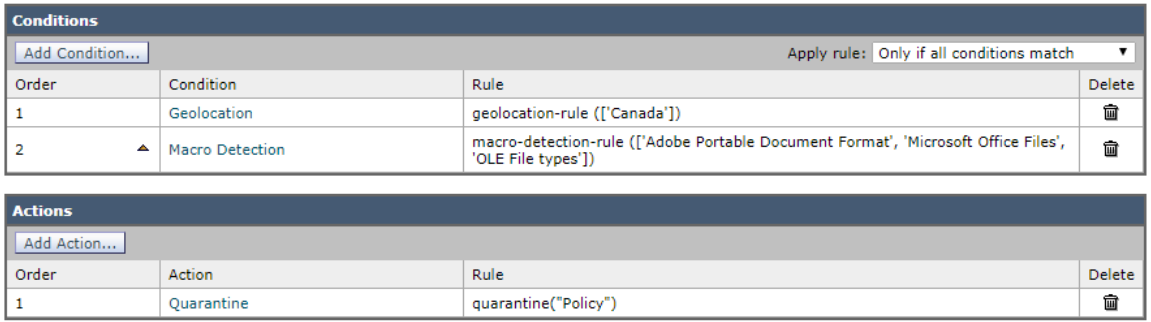
Детектор макросов (Версия 10.0.2+)

Детектирование документов с макросами позволяет администраторам настроить Message/Content фильтры для файлов, которые содержат макросы или скрипты и применить действия:

- Отправить сообщение в каранит
- Удалить присоединенный файл
- Удалить присоединенный файл и добавить текст в тело сообщения
- Модифицировать тему
- Добавить заголовок
- Перенаправить на другой адрес



Объединяйте факторы для эффективного блокирования



Conditions

Add Condition... | Apply rule: Only if all conditions match

Order	Condition	Rule	Delete
1	Geolocation	geolocation-rule (['Canada'])	
2	Macro Detection	macro-detection-rule (['Adobe Portable Document Format', 'Microsoft Office Files', 'OLE File types'])	

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	quarantine("Policy")	

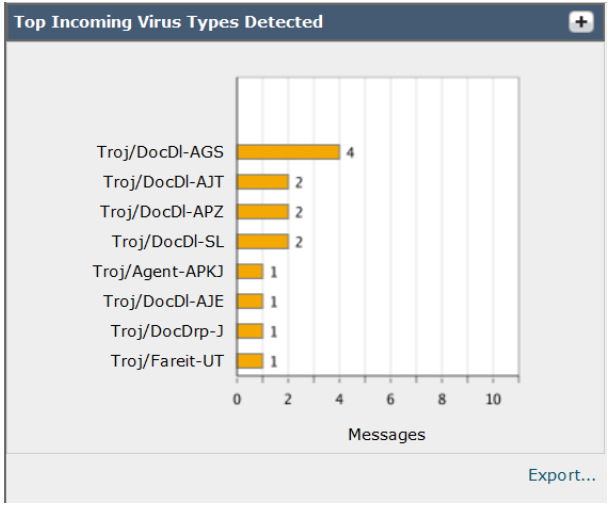
- Штампование X-headers
- Вердикты от других движков
- Репутация отправителя
- Репутация URL
- Геолокация
- И т.д...

- Используйте комбинацию источника и содержимого для создания правил безопасности, которые позволят реализовать политики безопасности для вашей организации
- Можно сделать как с помощью Message, так и Content Filters
- Объединяйте действия карантина и нотификации или отправляйте сообщение без присоединенного файла пользователю.

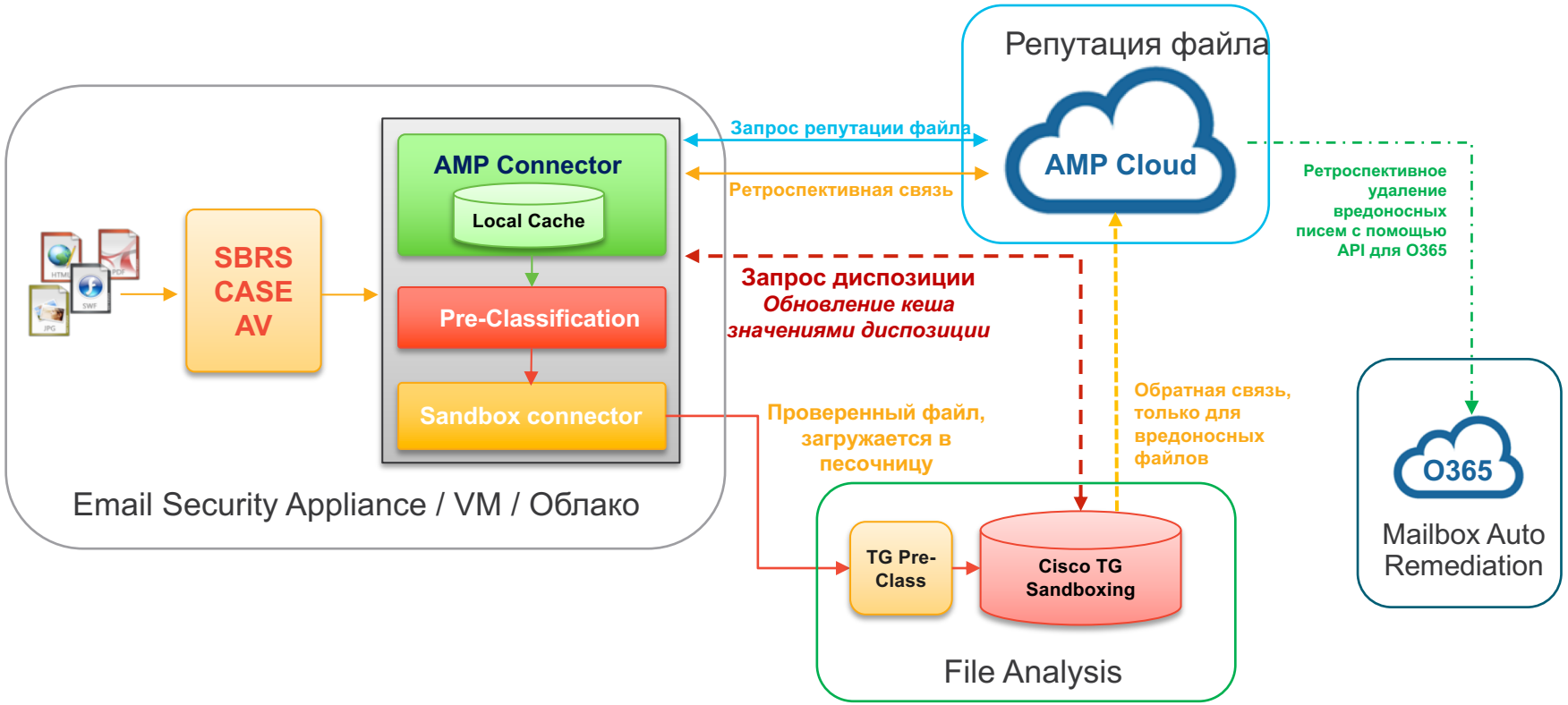
Блокирование известных вирусов

Default Policy	IronPort Anti-Spam	Sophos	File Reputation	Graymail Detection	FED_LOGHEADER	Retention Time:
	Positive: Quarantine Suspected: Quarantine	Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Unscannable: Deliver Malware File: Drop Pending Analysis: Quarantine MAR Action: Delete ...	Marketing: Deliver Social: Deliver Bulk: Deliver		Virus: 1 day Other: 4 hours

- Sophos входит в лицензию, блокирование известных вирусов
- Encrypted => Password Protected, Signed
- Unscannable => слишком большой, невозможно прочитать
- Вы все еще пытаетесь лечить? Большинство пользователей сейчас даже не включают опцию лечения для зараженных сообщений
- В версии 10.0.1 появился новый движок Sophos CxMail



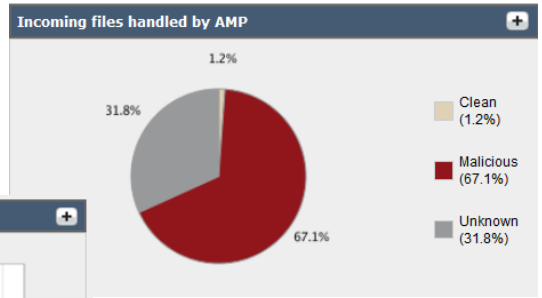
Как работает AMP

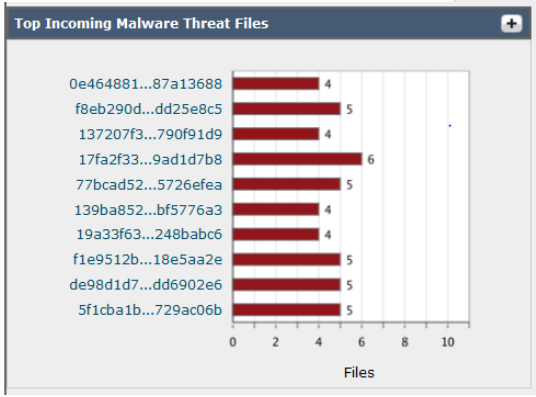


Включение AMP

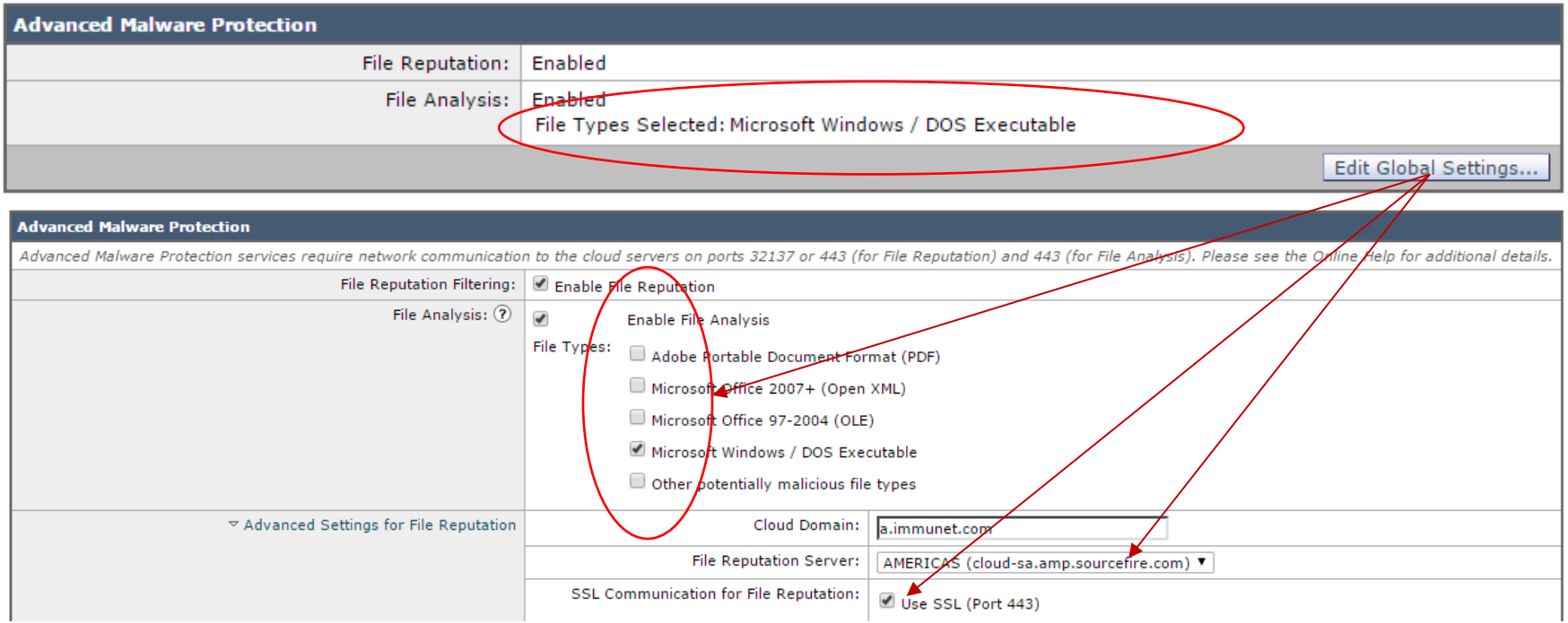
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Deliver	LOG_FED_SCORE REPLY-TO_CHECK FED_WARN BAD_URL_IN_DOC SPF_CHECK ...	Retention Time: Virus: 1 day Other: 4 hours	

- AMP – это дополнительная лицензия на ESA и CES
- Включается для входящей и исходящей почты
- 4 компонента AMP:
  - File Reputation
  - File Analysis
  - File Retrospection
  - Mailbox Auto Remediation (v10+)



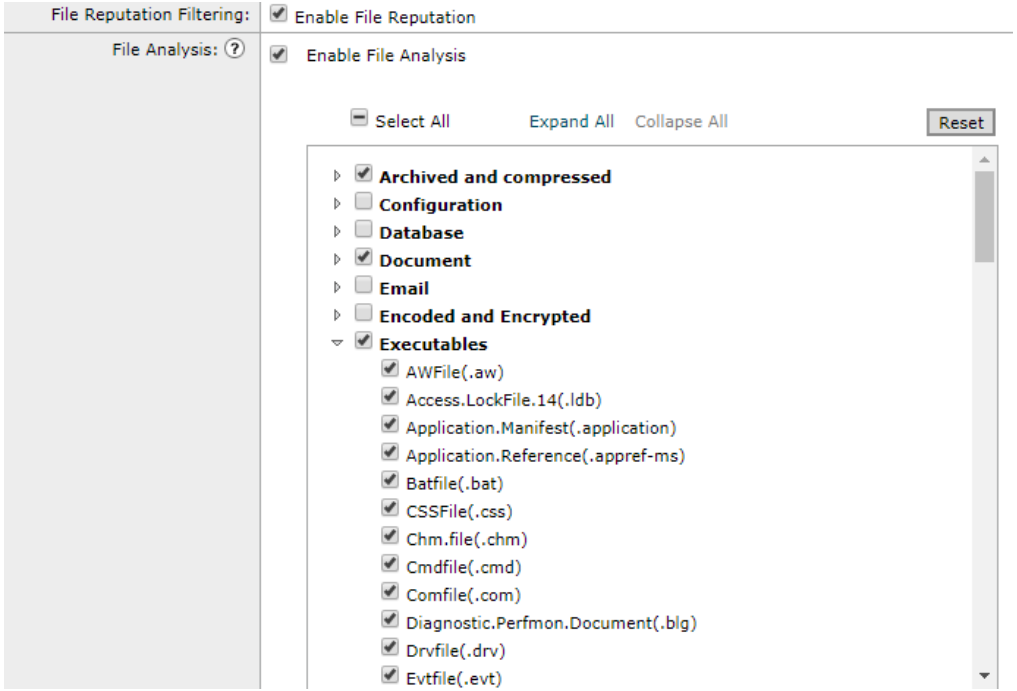


Анализ файлов AMP File Analysis – Проверьте тип и настройки

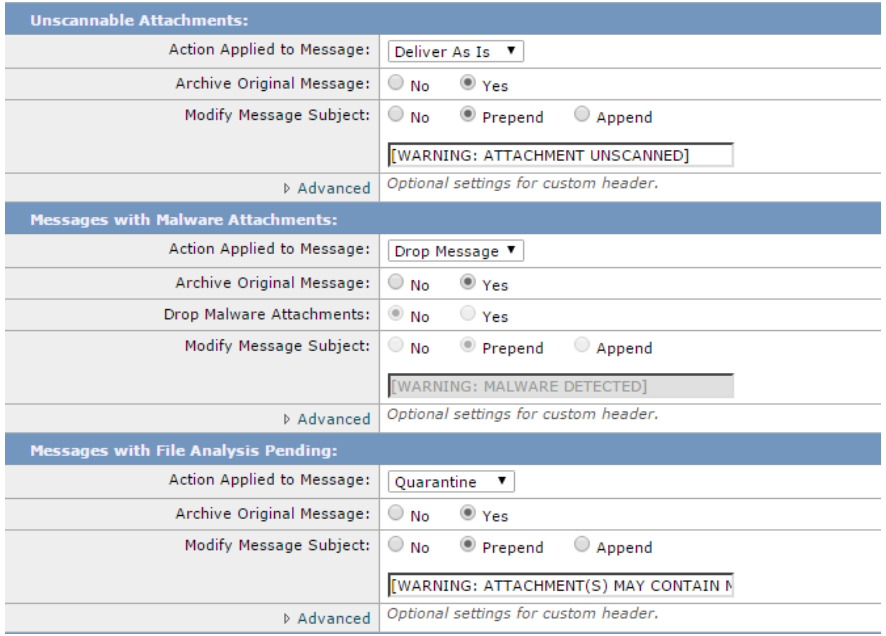


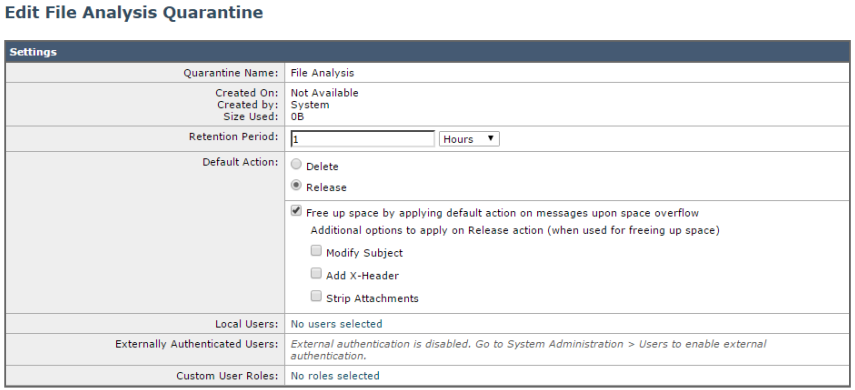
В версии 11.1 увеличилось количество файлов.

- 11.1 обеспечивает паритет с файлами, которые поддерживает ThreatGrid
- Новый механизм преклассификации позволяет загружать дополнительные типы файлов
- Преклассификация в облаке увеличивает количество информации для анализа
- Надо включить после апгрейда



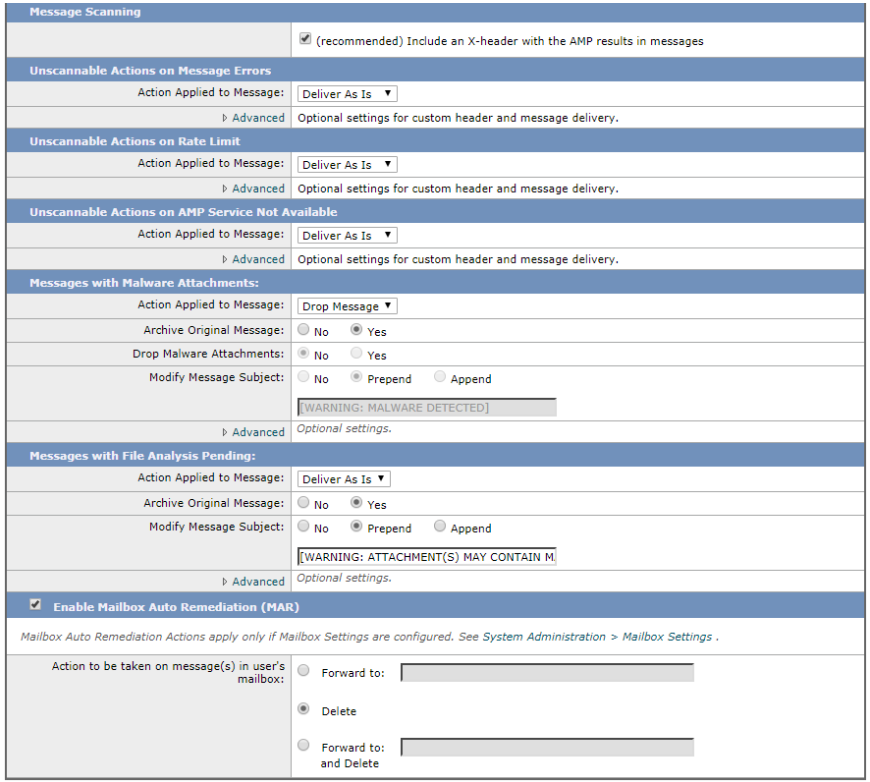
Динамический карантин AMP





- Используйте карантин для задержки файлов и ожидания результатов анализа
- Обычно результаты возвращаются в течение 10 минут, настройки по умолчанию – ждать 1 час перед освобождением из карантина

Настройки политик AMP(11.1)



- Все действия включают возможность отправить файл в каранин без помощи Content Filter
- В версии 11.1 доступна опция Unscannable
- Доступны дополнительные ограничения
- Если AMP недоступен, вы можете выбрать опцию Fail или Close

Ретроспективные предупреждения AMP

AMP генерирует два вида ретроспективных событий:

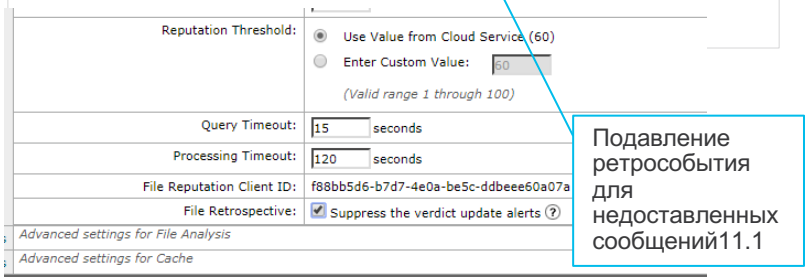
Изменение диспозиции, **сообщение не доставлено**.

The Info message is:

Retrospective verdict received.

SHA256: 7c48eb3b1fea5705fc70539f2a0539a3be794d6b70408a31c9ea461855657cd0
Timestamp: 2016-09-19T19:39:13Z
Verdict: MALICIOUS
Reputation Score: 0
Spyname: W32.Auto:7c48eb3b1f.in05.Talos

Version: 10.0.0-124
Serial Number: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Timestamp: 19 Sep 2016 14:39:13 -0500



Подавление ретрособытия для недоставленных сообщений11.1

Изменение диспозиции, **сообщение доставлено**.

The Info message is:

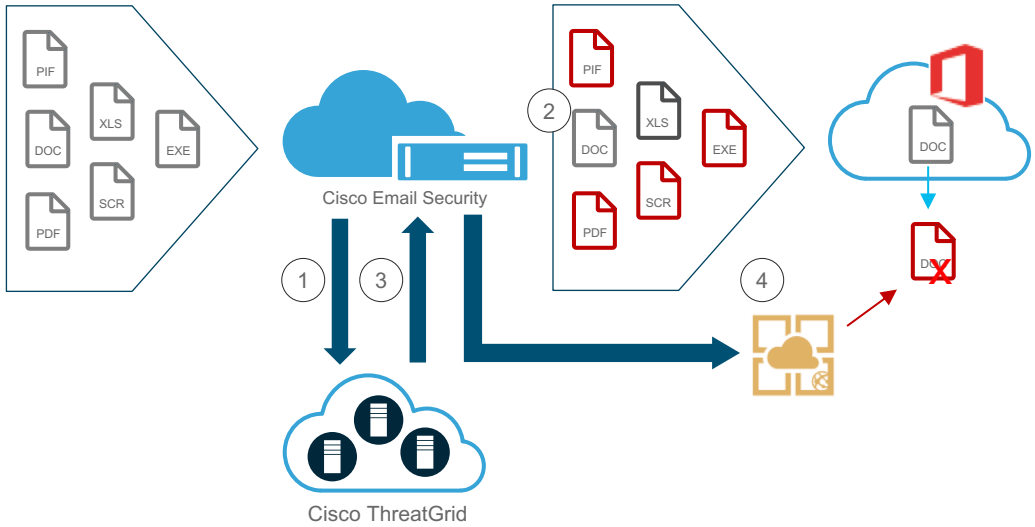
Retrospective verdict received for NEW SAMPLE ORDER 1.doc.

SHA256: ce49d65659304dcb7ae63182e17aa4b6f09740caaf77f1565a682bd2bb4e2bf4
Timestamp: 2016-09-19T19:39:12Z
Verdict: MALICIOUS
Reputation Score: 0
Spyname: RTF.CE49D65659.agent.tht.Talos

Total users affected: 1
---------- Affected Messages ----------

Message 1
MID : 20045
Subject : Sample Pictures and Letter of Intent as shown on attached files (3)
From : alfredo@comerquim.com.ec
Bcc : LAURA.LEWIS@somecustomername.com
File name : NEW SAMPLE ORDER 1.doc
Parent SHA256 : ,
Parent File name : ,
Date : 2016-09-19T05:35:48Z

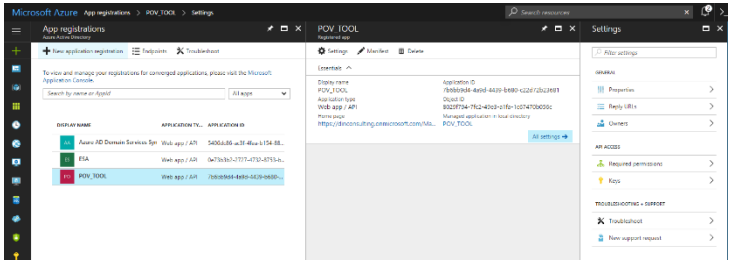
Mailbox Auto Remediation

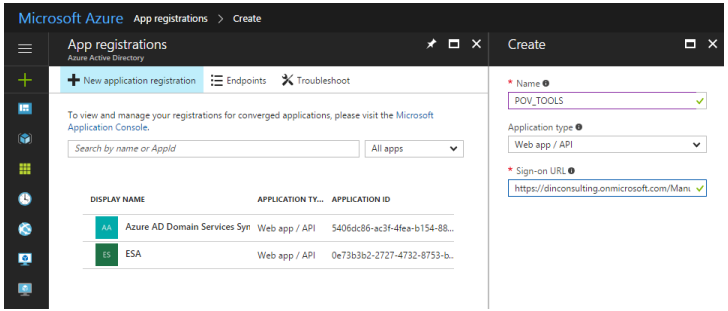


1. Аттачи анализируются
2. Диспозиция аттача неизвестная и доставляется пользователю
3. Происходит ретроспективное событие и файл теперь помечен как вредоносный
4. Делается автоматизированный вызов APIи сообщение может быть перенаправлено или удалено из почтового ящика пользователя

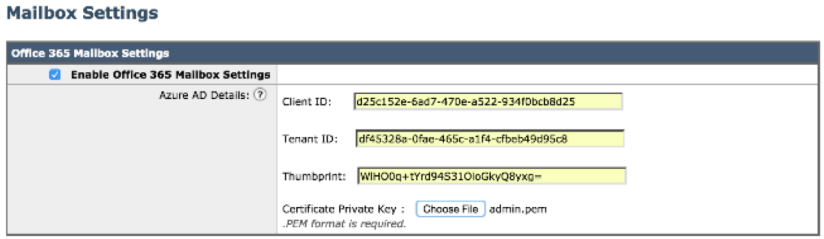
Настройка Mailbox Remediation

Шаг 1: Создайте Azure Web Application в вашем tenant

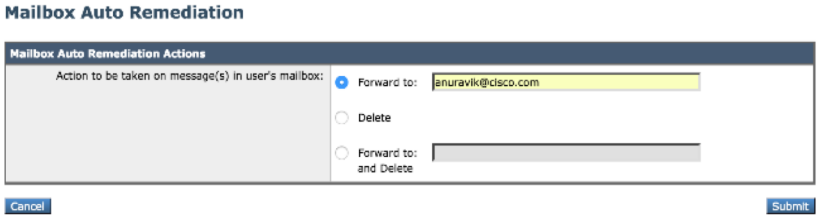




Шаг 2: Подключите его к ESAs / CES



Шаг 3: Настройте политику для Remediation

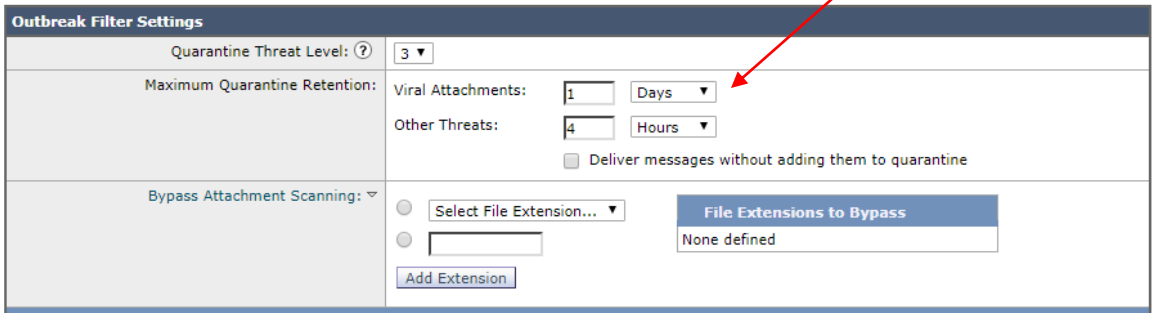


https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/guide-c07-738370.pdf

Включение Virus Outbreak Filters

Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Quarantine MAR Action: Delete ...	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Deliver	FED_LOGHEADER	Retention Time: Virus: 1 day Other: 4 hours

- VOF включен по умолчанию и обеспечивает динамический каранин (также называемый каранин задержки) и основывается на правилах, согласно которым может продолжать удерживать сообщение или освободить его для анализа AMP или AV



http://www.senderbase.org/static/malware/#tab=0

Выгоды от использования Virus Outbreak Filters

- Обеспечивает высокий уровень обнаружения при вспышках атак по сравнению с традиционными движками, так как добавляется «человеческий» элемент к правилам, кроме сигнатур, эвристики и хеш-сканирования
- Во время вспышек атак 0-day обеспечивается 9-часовое опережение по сравнению с антивирусоами

20 MOST RECENT VIRUS OUTBREAKS FROM EMAIL

MALWARE NAME	CISCO	SOPHOS	MCAFEE	TREND MICRO	SYMANTEC
Troj/AutoIt-CDQ	+0d 16h 45m	+1d 10h 50m	1st Sun, 17 Dec 2017 14:30:00 GMT	Not Published	Not Published
Mal/Generic-S	+0d 16h 0m	+0d 12h 55m	1st Sun, 17 Dec 2017 14:30:00 GMT	Not Published	Not Published
Mal/Generic-S	1st Fri, 15 Dec 2017 14:41:00 GMT	+1d 9h 14m	Not Published	Not Published	Not Published
Mal/Generic-S	+0d 21h 27m	+0d 20h 25m	1st Thu, 14 Dec 2017 17:10:00 GMT	Not Published	Not Published
Mal/Generic-L	+0d 21h 6m	+1d 4h 45m	1st Thu, 14 Dec 2017 17:10:00 GMT	Not Published	Not Published
Java/Adwind-CMH	1st Thu, 14 Dec 2017 12:15:00 GMT	+1d 14h 5m	Not Published	Not Published	Not Published
Mal/Generic-S	+0d 3h 20m	1st Thu, 14 Dec 2017 08:40:00 GMT	+0d 11h 25m	Not Published	Not Published
Java/Adwind-CMG	1st Thu, 14 Dec 2017 10:30:00 GMT	+1d 11h 25m	Not Published	Not Published	Not Published
Java/Adwind-CMF	1st Thu, 14 Dec 2017 09:35:00 GMT	+1d 12h 20m	Not Published	Not Published	Not Published
Troj/Chisbur-TW	+0d 8h 20m	+1d 4h 0m	1st Wed, 13 Dec 2017 23:55:00 GMT	Not Published	Not Published
Troj/DocDl-LWP	1st Thu, 14 Dec 2017 07:40:00 GMT	+0d 20h 15m	Not Published	Not Published	Not Published
Java/Adwind-CLW	1st Wed, 13 Dec 2017 12:01:00 GMT	+1d 15h 54m	Not Published	Not Published	Not Published
Troj/DocDl-LVX	1st Wed, 13 Dec 2017 10:47:00 GMT	+0d 8h 8m	Not Published	Not Published	Not Published
Java/Adwind-CLY	1st Wed, 13 Dec 2017 10:41:00 GMT	+1d 17h 14m	Not Published	Not Published	Not Published
Mal/Generic-S	1st Wed, 13 Dec 2017 07:54:00 GMT	+1d 10h 11m	Not Published	Not Published	Not Published
Troj/DocDl-LVX	1st Wed, 13 Dec 2017 07:12:00 GMT	+0d 11h 43m	+1d 12h 53m	Not Published	Not Published
Java/Adwind-CJZ	1st Tue, 12 Dec 2017 14:10:00 GMT	+1d 4h 45m	Not Published	Not Published	Not Published
Troj/DocDl-LVT	1st Tue, 12 Dec 2017 11:40:00 GMT	+1d 12h 15m	+1d 13h 25m	Not Published	Not Published
Mal/Generic-L	1st Tue, 12 Dec 2017 10:20:00 GMT	+3d 3h 15m	+2d 9h 45m	Not Published	Not Published
Java/Adwind-CLZ	1st Tue, 12 Dec 2017 10:20:00 GMT	+4d 3h 35m	Not Published	Not Published	Not Published

https://www.talosintelligence.com/reputation_center/malware_rep#mal-outbreaks

Проверочная таблица для обработки файлов

- Создайте фильтр для блокирования, карантина или вырезания файлов, которые определены рискованными для организации
- Используйте AV для блокирования известных вирусов. Рекомендуется выключить очистку или лечение, а удалять письма с зараженными файлами.
- Проверьте, что Virus Outbreak включен для всех ваших политик, он может обеспечить примерно 10 часовое опережение для атак 0-day
- Обновитель до 10.0.1+ и используйте фильтр макросов для обнаружения и реагирования на нежелательные файлы с макросами.
- Оцение AMP если его у вас еще нет
- AMP проверяет все файлы и определяет файловую репутацию
- Установите действие File Analysis Pending в Quarantine для задержки сообщения, пока не будет известен вердикт
- File Analysis в AMP проверяет и макросы в том числе
- Для Office 365 с Azure API доступна опция реагирования.

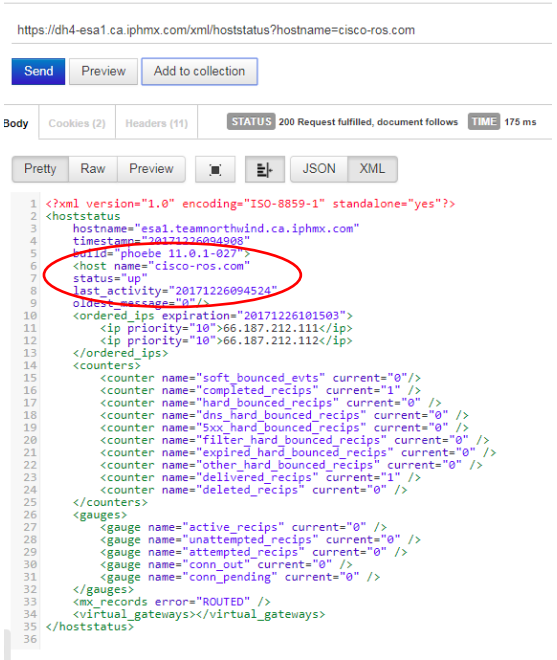
Мониторинг и инструменты

Использование XML страниц

- Переход на https://hostname/xml/status will предоставляет текущую информацию о параметрах и здоровье системы
- Дополнительные страницы для:
  - Host Status: https://hostname/xml/hoststatus?hostname= host
  - DNS Status: https://hostname/xml/dnsstatus
  - Top Incoming Domains: https://hostname/xml/topin
  - Top Outgoing Domains: https://hostname/xml/tophosts

Out of Band (OOB) Monitoring c XML

- Популярный продукт для мониторинга SolarWinds предлагает шаблоны для использования XML статуса для мониторинга OOB: https://thwack.solarwinds.com/docs/DOC-174863
- Используйте Host Status: http://hostname/xml/hoststatus?hostname=mydomain.com для того, чтобы проверять возможные проблемы с доставкой писем
- Для получения быстрых метрик можно использовать скрипты с cURL через HTTPS
- XML статус не требует дополнительных настроек или открытия портов
- Статус только для индивидуального сервера (не для кластера или пула серверов)



Reporting API

- Анонсирован в версии 9.0
- Полный REST API для данных отчетности
- Результаты возвращаются в формате JSON
- Запросы через HTTP/S, через определенный порт
- Ответы для индивидуального сервера

```
GET /api/v1.0/health HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json

HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Wed, 02 Jul 2014 05:07:50 GMT
Content-type: application/json
Content-Length: 246
Connection: close

{
    "data":{
        "percentage_ram_utilization":10,
        "percentage_diskio":20,
        "resource_conservation":3,
        "messages_in_workqueue":189,
        "messages_in_pvo_quarantines":12,
        "percentage_swap_utilization":2.0,
        "percentage_queue_utilization":5.0,
        "percentage_cpu_load":12
    },
    "uri":"/api/v1.0/health/"
}
```

Resource request (Health Status)

Agent

Auth Type

Data returned in JSON

Пакетные команды в CLI

- CLI поддерживает те же команды, что и GUI, и даже немногоо больше
- Некоторые команды могут использовать аргумены, введите **help <command>**, чтобы увидеть все опции
- Описание команд в CLI reference guide: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/cli_reference_guide/b_CLI_Reference_Guide.html

Примеры:

- Добавьте объект в SMTP Route

```
> smtproutes new mynewdomain.com 215.55.66.77, 215.55.66.88
```

- Добавьте объект в HAT Table

```
> listenerconfig edit IncomingMail hostaccess new sendergroup REDLIST possible_spammer.com Policy: "THROTTLED"
```

Использование Expect для автоматизации

- Expect – это стандартный инструмент для отправки и получения команд
- Для того, чтобы заставить скрипт работать, надо знать предыдущий вывод
- Может использоваться для автоматизации команд – некоторые клиенты строят целые процессы вокруг expect скриптов
- Используйте вместе с пакетными командами для того, чтобы достичь быстрого, автоматизированного выполнения задач

https://www.nist.gov/services-resources/software/expect

```
#!/usr/bin/expect -f

set domain [lindex $argv 0]

spawn ssh admin@192.168.1.110

expect "> "
send "destconfig\n"
expect "[]> "
send "new\n"
expect "[]> "
send "$domain\n"
expect "]> "
send "N\n"
expect "]> "
send "N\n"
expect "]> "
send "N\n"
expect "]> "
send "Y\n"
expect "]> "
send "3\n"
expect "]> "
send "N\n"
expect "]> "
send "N\n"
expect "]> "
send "\n"
expect "> "
send "commit\n"
expect "[]> "

send "added $domain to destconfig for TLS required\n"
expect "> "
send "exit\n"
```

Краткое резюме

- Дни «установил и забыл» давно проши – сейчас для защиты необходим постоянный мониторинг и настройка
- Понимайте, какое состояние безопасности вашей организации и настраивайте ваши устройства
- Обновляйте ваши устройства, мы постоянно анонсируем новые возможности, которые требуют обновлений
- Проверяйте наши Chalktalks на Youtube и руководства на Cisco.com для помощи с настройкой и развертванием новых возможностей Cisco Email Security

Резюме рекомендаций

Security Services

- IronPort Anti-Spam
  - Always scan 1MB and Never scan 2MB
- URL Filtering
  - Enable URL Categorization and Reputation
  - Enable Web Interaction Tracking
- Graymail Detection
  - Enable and Maximum Messages size 1 MB
- Outbreak Filters
  - Enable Adaptive Rules, Max Scan size1 MB
  - Enable Web Interaction Tracking
- Advanced Malware Protection
  - Enable additional file types after enabling feature
- Message Tracking
  - Enable Rejected Connection Logging (if required)

System Administration

- Users
  - Set password policies
  - If possible leverage LDAP for authentication
- Log Subscriptions
  - Enable Configuration History Logs
  - Enable URL Filtering Logs
  - Log Additional Header ‘From’

CLI Level Changes

- Web Security SDS URL Filtering
  - websecurityadvancedconfig >
    - disable_dns=1 , max_urls_to_scan=20 , num_handles=5 , default_ttl=600
    - Do you want to enable URL filtering for shortened URLs? [Y]> Y
- URL Logging
  - outbreakconfig> Do you wish to enable logging of URL's? [N]> y
  - http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html
- Clean URL Rewrites
  - websecurityadvancedconfig > Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
- Anti-Spoof Filter
  - https://supportforums.cisco.com/sites/default/files/attachments/discussion/forged_email_detection_with_cisco_email_security.pdf
- Header Stamping Filter

```
addHeaders:  if (sendergroup != "RELAYLIST")
{
     insert-header("X-IronPort-RemoteIP", "$RemoteIP");
     insert-header("X-IronPort-MID", "$MID");
     insert-header("X-IronPort-Reputation", "$Reputation");
     insert-header("X-IronPort-Listener", "$RecvListener");
     insert-header("X-IronPort-SenderGroup", "$Group");
     insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Резюме рекомендаций

Host Access Table

- Additional SenderGroups
  - SKIP_SBRS – Place higher for sources that skip reputation
  - SPOOF_ALLOW – Part of Spoofing Filter
  - PARTNER – For TLS Forced connections
- In SUSPECTLIST
  - Include SBRS Scores on None
  - Optionally, include failed PTR checks
- Aggressive HAT Sample
  - BLACKLIST [-10 to -2] POLICY: BLOCKED
  - SUSPECTLIST [-2 to -1] POLICY: HEAVYTHROTTLE
  - GRAYLIST[-1 to 2 and NONE] POLICY: LIGHTTHROTTLE
  - ACCEPTLIST [2 to 10] POLICY: ACCEPTED

Mail Flow Policy (default)

- Security Settings
  - Set TLS to preferred
  - Enable SPF
  - Enable DKIM
  - Enable DMARC and Send Aggregate Feedback Reports

Incoming Mail Policies

- Anti-Spam thresholds
  - Positive = 90, Suspect = 39
- Anti-Virus
  - Don't repair, Disable Archive Message
- AMP
  - Add "AMP" to Subject Prepend for Unscannable, Disable Archive Message
- Graymail
  - Scanning enabled for each Verdict, Prepend Subject and Deliver
  - Add x-header for Bulk email header = X-BulkMail, value = True
- Outbreak Filters
  - Enable message modification. Rewrite URL for unsigned message.
  - Change Subject prepend to: [Possible $threat_category Fraud]

Outgoing Mail Policies

- Anti-Virus
  - Anti-Virus Virus Infected: Prepend Subject: Outbound Malware Detected: $Subject.
  - Other Notification to Others: Order form admin contact
  - Anti-virus Unscannable don't Prepend the Subject
  - Uncheck Include an X-header with the AV scanning results in Message

Резюме рекомендаций

Policy Quarantines

- Pre-Create the following Quarantines
  - Inappropriate Inbound
  - Inappropriate Outbound
  - URL Malicious Inbound
  - URL Malicious Outbound
  - Suspect Spoof
  - Malware

Other Settings

- Dictionaries
  - Enable / Review Profanity and Sexual Terms Dictionary
  - Create Forged Email Dictionary with Executive Names
  - Create Dictionary for restricted or other keywords
- Destination Controls
  - Enable TLS for default destination
  - Set lower thresholds for webmail domains
  - http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118573-technote-esa-00.html

Content Filters

- Inappropriate language Content Filter
  - Conditions Profanity OR Sexual dictionary match, send a copy to the Inappropriate quarantine.
- URL Malicious Reputation Content Filter
  - Send a copy to the URL Malicious (-10 to -6) to quarantine.
- URL Category Content Filter with these selected
  - Adult, Pornography, Child Abuse, Gambling.
  - Send a copy to the Inappropriate quarantine.
- Forged Email Detection
  - Dictionary named "Executives_FED"
  - FED() threshold 90 Quarantine a copy.
- Macro Enabled Documents content filter
  - if one or more attachments contain a Macro
  - Optional condition -> From Untrusted SBRS range
  - Send a copy to quarantine
- Attachment Protection
  - if one or more attachments are protected
  - Optional condition -> From Untrusted SBRS range
  - Send a copy to quarantine

Ресурсы

- ESA ChalkTalks: https://www.youtube.com/playlist?list=PLFT-9JpKjRTANXKBmLbQ611TPYLXbUL_0
- URL Best Practices: http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html?referring_site=RE&pos=2&page=http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/white_paper_c11-684611.html
- Anti-Spam Tuning Guide: http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/white-paper-c11-732910.html
- Other Guides: http://www.cisco.com/c/en/us/products/security/email-security-appliance/white-paper-listing.html
- Knowledge base: http://www.cisco.com/c/en/us/products/security/email-security-appliance/q-and-a-listing.html
- Cisco Email Security Best Practices https://www.cisco.com/c/m/en_us/products/security/esa-best-practices.html
- Configuration Best Practices for CES ESA https://www.cisco.com/c/en/us/support/docs/security/cloud-email-security/210890-Configuration-Best-Practices-for-CES-ESA.html


CISCO