Как заблокироваться, тип содержимого базировал наборы символов

Содержание

Введение

Этот документ описывает, как записать и настроить фильтр, чтобы обнаружить и принять меры на основанных наборах символов типа содержимого на Cisco Email Security Appliance (ESA). Следующий документ может использоваться для обнаружения основанных символов иностранного языка, замеченных в сообщениях спама.

Общие сведения

Администраторы ESA могут получить приток сообщений электронной почты, которые содержат символьно-ориентированные иностранные языки, которые не являются легитимной почтой для их компании или домена (доменов). Один способ обратиться от ESA, у нас есть две опции:

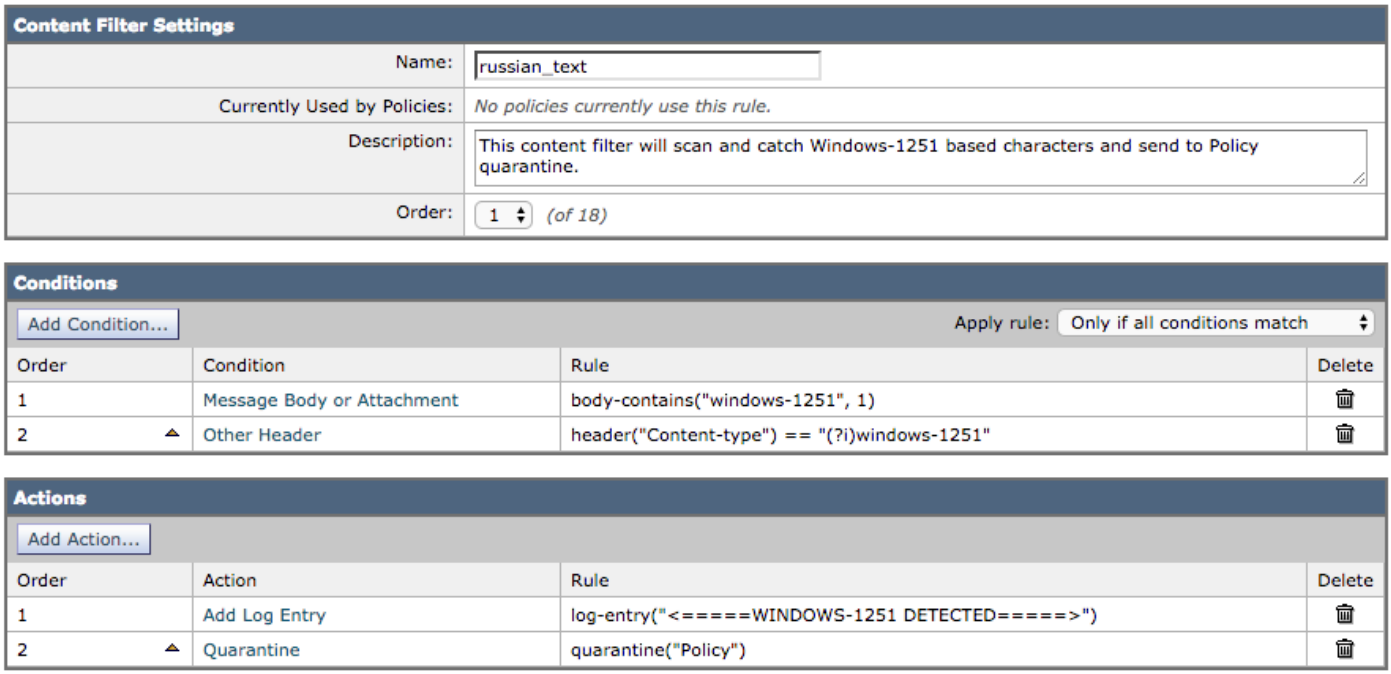
Запишите фильтр

Первый вариант для администратора, чтобы записать и настроить фильтр и привязать его к почтовой политике, по мере необходимости.

> **Примечание:** Запись и настройка этот фильтр как фильтр сообщения может быть дорогим ресурсом для сканирования тела электронных почт для наборов символов.

> **Примечание:** Настройка это как фильтр контента убедительно предполагается как фильтры контента, происходит после сканирования для защиты от спама. Однако это может быть записано и настроено как фильтр сообщения в случае необходимости.

Следующий пример примет во внимание, что сообщение электронной почты содержит русский язык основанные символы (кириллицы) через Windows 1251 базировали набор символов. Записанный как фильтр контента:



Content Filter Settings

Name:	russian_text
Currently Used by Policies:	*No policies currently use this rule.*
Description:	This content filter will scan and catch Windows-1251 based characters and send to Policy quarantine.
Order:	1 *(of 18)*

Conditions

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

Order	Condition	Rule	Delete
1	Message Body or Attachment	body-contains("windows-1251", 1)	
2	Other Header	header("Content-type") == "(?i)windows-1251"	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<=====WINDOWS-1251 DETECTED=====>")	
2	Quarantine	quarantine("Policy")	

Тестовая используемая электронная почта будет содержать придерживающееся в теле электронной почты:

```
Russian uses ?, ?, ?, ?, o, ?, ?, ?, ?, ? as vowels. You could create a message filter set to
"Matches any of the following" that test whether "Body" "contains" "?", "Body" "contains" "?"
and so forth until you covered all of the vowels. Ssince English also uses "a" , "e" , "o", and
"y" letters don't test for them. The reason for "Matches any of the following" is to logically
OR them - you want the action to take place if any of those letters are found.
```

С фильтром контента, настроенным как выше, почтовые журналы сделали бы запись подобный придерживающемуся:

```
Thu Sep 10 14:50:09 2015 Info: Start MID 164993 ICID 266729
Thu Sep 10 14:50:09 2015 Info: MID 164993 ICID 266729 From: <robsherw@cisco.com>
Thu Sep 10 14:50:09 2015 Info: MID 164993 ICID 266729 RID 0 To: <robsherw@cisco.com>
Thu Sep 10 14:50:09 2015 Info: MID 164993 using engine: SPF Verdict Cache using cached verdict
Thu Sep 10 14:50:09 2015 Info: SPF Verdict Cache cache status: hits = 1, misses = 3, expires =
0, adds = 3, seconds saved = 0.11, total seconds = 0.39
Thu Sep 10 14:50:09 2015 Info: MID 164993 SPF: helo identity postmaster@dhcp-10-150-53-
16.cisco.com None
Thu Sep 10 14:50:09 2015 Info: MID 164993 using engine: SPF Verdict Cache using cached verdict
Thu Sep 10 14:50:09 2015 Info: MID 164993 SPF: mailfrom identity robsherw@cisco.com SoftFail
(v=spf1)
Thu Sep 10 14:50:09 2015 Info: MID 164993 using engine: SPF Verdict Cache using cached verdict
Thu Sep 10 14:50:09 2015 Info: MID 164993 SPF: pra identity robsherw@cisco.com None headers from
Thu Sep 10 14:50:09 2015 Info: MID 164993 Message-ID '<7A961F85-A5F1-413F-87CB-
C31D2E5605EC@cisco.com>'
Thu Sep 10 14:50:09 2015 Info: MID 164993 Subject 'russian test'
Thu Sep 10 14:50:09 2015 Info: MID 164993 ready 2302 bytes from <robsherw@cisco.com>
Thu Sep 10 14:50:09 2015 Info: MID 164993 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Thu Sep 10 14:50:09 2015 Info: MID 164993 AMP file reputation verdict : CLEAN
Thu Sep 10 14:50:09 2015 Info: MID 164993 using engine: GRAYMAIL negative
Thu Sep 10 14:50:09 2015 Info: MID 164993 Custom Log Entry: <====== WINDOWS-1251 DETECTED
======>
Thu Sep 10 14:50:09 2015 Info: MID 164993 quarantined to "Policy" (content filter:russian_text)
```

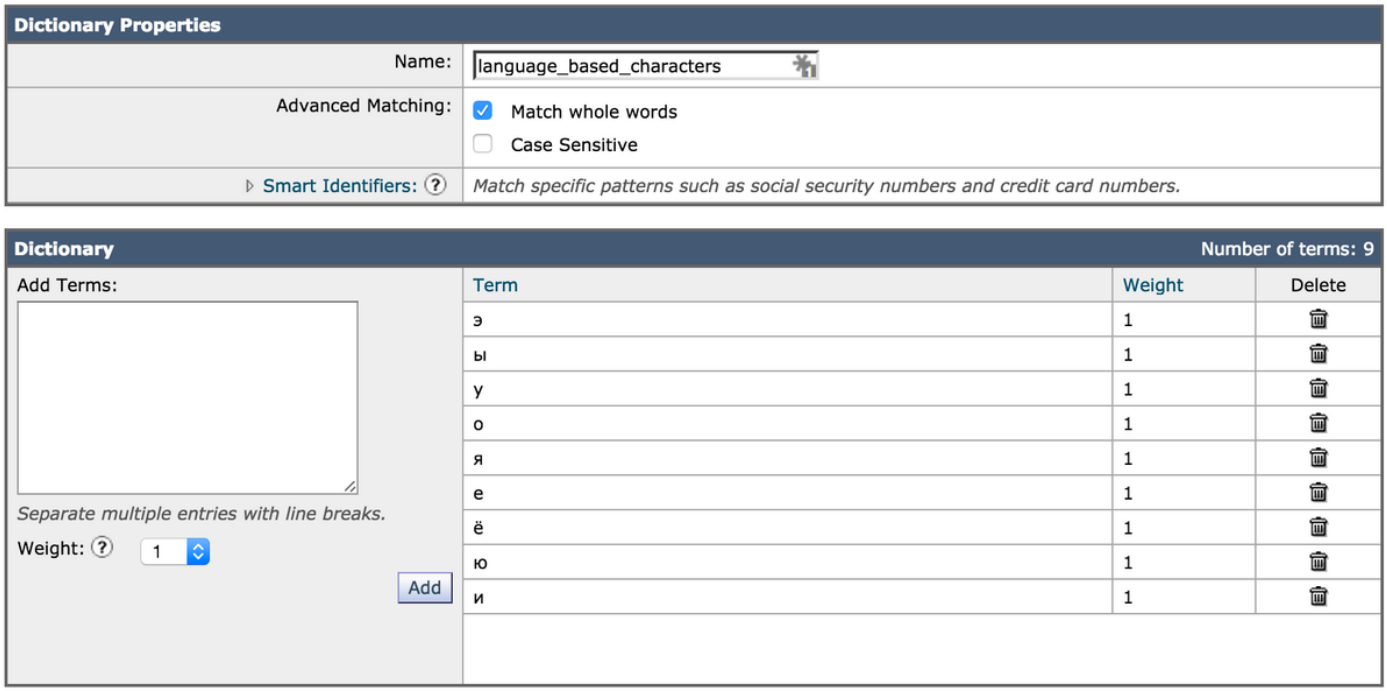
```
Thu Sep 10 14:50:09 2015 Info: Message finished MID 164993 done
```

Другие языки и наборы символов могут использоваться. Посмотрите Ссылочный раздел для дополнительных сведений.

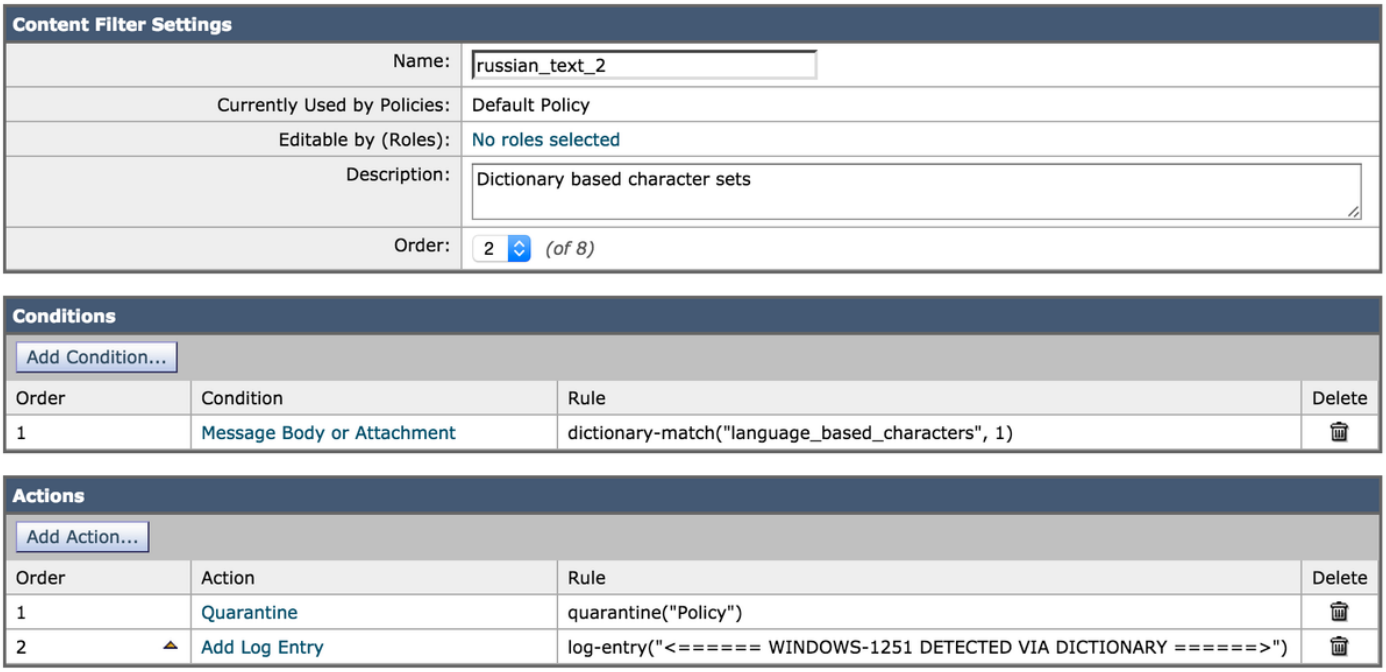
Сошлитесь на символьно-ориентированный словарь

Вторая опция должна добавить список наборов символов к текстовому файлу словаря и обратиться к этому в фильтре.

Пример добавления символов к словарю:



Символы теперь назначены на словарь, и на сам словарь ссылаются в элементах условия для фильтра:



Использование того же теста посылает по электронной почте как выше, это содержит

придерживающееся в теле электронной почты:

```
Russian uses ?, ?, ?, ?, o, ?, ?, ?, ?, ? as vowels. You could create a message filter set to
"Matches any of the following" that test whether "Body" "contains" "?", "Body" "contains" "?"
and so forth until you covered all of the vowels. Ssince English also uses "a" , "e" , "o", and
"y" letters don't test for them. The reason for "Matches any of the following" is to logically
OR them - you want the action to take place if any of those letters are found.
```

С фильтром контента, настроенным как выше использования условия соответствия словаря, почтовые журналы сделали бы запись подобный придерживающемуся:

```
Thu Sep 10 15:26:08 2015 Info: New SMTP ICID 266737 interface Management (172.18.249.222)
address 10.150.53.16 reverse dns host dhcp-10-150-53-16.cisco.com verified yes
Thu Sep 10 15:26:08 2015 Info: ICID 266737 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
Thu Sep 10 15:26:08 2015 Info: Start MID 164995 ICID 266737
Thu Sep 10 15:26:08 2015 Info: MID 164995 ICID 266737 From: <robsherw@cisco.com>
Thu Sep 10 15:26:08 2015 Info: MID 164995 ICID 266737 RID 0 To: <robsherw@cisco.com>
Thu Sep 10 15:26:08 2015 Info: MID 164995 using engine: SPF Verdict Cache using cached verdict
Thu Sep 10 15:26:08 2015 Info: SPF Verdict Cache cache status: hits = 6, misses = 4, expires =
1, adds = 4, seconds saved = 0.50, total seconds = 0.85
Thu Sep 10 15:26:08 2015 Info: MID 164995 SPF: helo identity postmaster@dhcp-10-150-53-
16.cisco.com None
Thu Sep 10 15:26:08 2015 Info: MID 164995 using engine: SPF Verdict Cache using cached verdict
Thu Sep 10 15:26:08 2015 Info: MID 164995 SPF: mailfrom identity robsherw@cisco.com SoftFail
(v=spf1)
Thu Sep 10 15:26:08 2015 Info: MID 164995 using engine: SPF Verdict Cache using cached verdict
Thu Sep 10 15:26:08 2015 Info: MID 164995 SPF: pra identity robsherw@cisco.com None headers from
Thu Sep 10 15:26:08 2015 Info: MID 164995 Message-ID '<BCC88307-EB91-476E-8732-
334E9EE84EC8@cisco.com>'
Thu Sep 10 15:26:08 2015 Info: MID 164995 Subject 'russian test 3'
Thu Sep 10 15:26:08 2015 Info: MID 164995 ready 2316 bytes from <robsherw@cisco.com>
Thu Sep 10 15:26:08 2015 Info: MID 164995 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Thu Sep 10 15:26:08 2015 Info: MID 164995 AMP file reputation verdict : CLEAN
Thu Sep 10 15:26:08 2015 Info: MID 164995 using engine: GRAYMAIL negative
Thu Sep 10 15:26:08 2015 Info: MID 164995 Custom Log Entry: <====== WINDOWS-1251 DETECTED VIA
DICTIONARY ======>
Thu Sep 10 15:26:08 2015 Info: MID 164995 quarantined to "Policy" (content
filter:russian_text_2)
Thu Sep 10 15:26:08 2015 Info: Message finished MID 164995 done
```

Ссылки

- Microsoft предоставляет названия набора символов (*название.NET*) в их Идентификаторах кодовых страниц , на которые можно сослаться при записи и настройке фильтров.

  Примечание: Страницы кода ANSI могут быть другими на других компьютерах или могут быть изменены для одиночного компьютера, приведя к нарушению целостности данных. Для самых последовательных результатов приложения должны использовать Юникод, такой как UTF 8 или UTF 16, вместо определенной кодовой страницы.

- Mozillazine предоставляет всестороннюю подробную информацию для Типа содержимого: заголовок, внешние буквы, внешние слова, и больше, в их статье для спама Иностранного языка

Дополнительные сведения

- Homoglyph усовершенствованные фишинговые атаки
- Руководства конечного пользователя устройства безопасности электронной почты Cisco
- Cisco Systems – техническая поддержка и документация