

Comment bloquer le type satisfait a basé des jeux de caractères

Contenu

[Introduction](#)

[Informations générales](#)

[Écrivez un filtre](#)

[Mettez en référence un dictionnaire basé par caractère](#)

[Références](#)

[Informations connexes](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit comment écrire et configurer un filtre afin de détecter et agir sur les jeux de caractères basés de type satisfait sur l'appliance de sécurité du courrier électronique de Cisco (ESA). Le document suivant peut être utilisé pour détecter les caractères basés sur un langage étrangers vus dans les messages spam.

[Informations générales](#)

Les administrateurs ESA peuvent recevoir un afflux des messages qui contiennent les langues étrangères basées par caractère qui ne sont pas messagerie légitime pour leur société ou domaines. Une manière d'adresser de l'ESA, nous avons deux options :

Écrivez un filtre

Le premier choix est pour que l'administrateur écrive et pour configure un filtre, et l'associe à une stratégie de messagerie, comme nécessaire.

Remarque: L'inscription et configurer de ce filtre comme filtre de message peuvent être ressource-chères afin de balayer le corps des emails pour les jeux de caractères.

Remarque: Configurer ceci comme un filtre satisfait est fortement suggéré, comme les filtres satisfaits se produisent après la lecture d'anti-Spam. Cependant, ceci peut être écrit et configuré comme filtre de message, si nécessaire.

L'exemple suivant prendra en considération un message contiennent les caractères basés (cyrilliques) russes par l'intermédiaire du jeu de caractères basé par Windows-1251. Écrit comme

filtre satisfait :

Content Filter Settings	
Name:	<input type="text" value="russian_text"/>
Currently Used by Policies:	No policies currently use this rule.
Description:	<input type="text" value="This content filter will scan and catch Windows-1251 based characters and send to Policy quarantine."/>
Order:	<input type="text" value="1"/> (of 18)

Conditions			
<input type="button" value="Add Condition..."/>		Apply rule:	<input type="text" value="Only if all conditions match"/>
Order	Condition	Rule	Delete
1	Message Body or Attachment	body-contains("windows-1251", 1)	<input type="button" value="Delete"/>
2	Other Header	header("Content-type") == "(?)windows-1251"	<input type="button" value="Delete"/>

Actions			
<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<====WINDOWS-1251 DETECTED====>")	<input type="button" value="Delete"/>
2	Quarantine	quarantine("Policy")	<input type="button" value="Delete"/>

L'email de test utilisé contiendra le suivant dans le corps de l'email :

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.

Le filtre de contenu étant configuré comme ci-dessus, les logs de messagerie enregistreraient semblable à ce qui suit :

```
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
```

D'autres langages et jeux de caractères peuvent être utilisés. Veuillez voir la section de références pour information les informations complémentaires.

Mettez en référence un dictionnaire basé par caractère

La deuxième option est d'ajouter la liste de jeux de caractères à un fichier texte de dictionnaire et de se reporter à cela dans le filtre.

Exemple d'ajouter les caractères au dictionnaire :

Dictionary Properties	
Name:	language_based_characters
Advanced Matching:	<input checked="" type="checkbox"/> Match whole words <input type="checkbox"/> Case Sensitive
Smart Identifiers:	Match specific patterns such as social security numbers and credit card numbers.

Dictionary		Number of terms: 9																														
Add Terms: <div style="border: 1px solid gray; height: 80px; width: 100%;"></div> Separate multiple entries with line breaks. Weight: <input type="text" value="1"/> <input type="button" value="Add"/>	<table border="1"> <thead> <tr> <th>Term</th> <th>Weight</th> <th>Delete</th> </tr> </thead> <tbody> <tr><td>э</td><td>1</td><td></td></tr> <tr><td>ы</td><td>1</td><td></td></tr> <tr><td>у</td><td>1</td><td></td></tr> <tr><td>о</td><td>1</td><td></td></tr> <tr><td>я</td><td>1</td><td></td></tr> <tr><td>е</td><td>1</td><td></td></tr> <tr><td>ё</td><td>1</td><td></td></tr> <tr><td>ю</td><td>1</td><td></td></tr> <tr><td>и</td><td>1</td><td></td></tr> </tbody> </table>	Term	Weight	Delete	э	1		ы	1		у	1		о	1		я	1		е	1		ё	1		ю	1		и	1		
Term	Weight	Delete																														
э	1																															
ы	1																															
у	1																															
о	1																															
я	1																															
е	1																															
ё	1																															
ю	1																															
и	1																															

Les caractères sont maintenant assignés au dictionnaire et le dictionnaire lui-même est mis en référence dans les éléments de condition pour le filtre :

Content Filter Settings	
Name:	russian_text_2
Currently Used by Policies:	Default Policy
Editable by (Roles):	No roles selected
Description:	Dictionary based character sets
Order:	2 (of 8)

Conditions			
<input type="button" value="Add Condition..."/>			
Order	Condition	Rule	Delete
1	Message Body or Attachment	dictionary-match("language_based_characters", 1)	

Actions			
<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Quarantine	quarantine("Policy")	
2	Add Log Entry	log-entry("<===== WINDOWS-1251 DETECTED VIA DICTIONARY =====>")	

Utilisant le même email de test comme ci-dessus, il contient le suivant dans le corps de l'email :

Russian uses э, ы, у, о, я, е, ё, ю, и as vowels. You could create a message filter set to "Matches any of the following" that test whether "Body" "contains" "э", "Body" "contains" "ы" 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.

Le filtre de contenu étant configuré comme ci-dessus utilisant l'état de correspondance de dictionnaire, les logs de messagerie enregistreraient semblable à ce qui suit :

```
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
```

Références

- Microsoft fournit des noms de jeu de caractères (*nom de .NET*) dans leurs [identifiants de page de code](#) qui peuvent être mis en référence en écrivant et en configurant des filtres.

Remarque: Les pages de code d'ANSI peuvent être différentes sur différents ordinateurs, ou peuvent être changées pour un ordinateur unique, menant à la corruption des données. Pour les résultats les plus cohérents, les applications devraient utiliser Unicode, tel qu'UTF-8 ou UTF-16, au lieu d'une page de code spécifique.

- Mozillazine fournit les détails en profondeur pour le type de contenu : en-tête, lettres étrangères, mots étrangers, et plus, en leur article pour le [Spam de langue étrangère](#)

[Informations connexes](#)

- [Homoglyph a avancé des attaques par phishing](#)
- [Guides d'utilisateur final d'appareils de sécurité du courrier électronique de Cisco](#)
- [Support et documentation techniques - Cisco Systems](#)