

根據ESA中的DKIM驗證配置傳入過濾器

簡介

本文檔介紹如何配置郵件安全裝置(ESA)，以便通過傳入內容過濾器或郵件過濾器配置對域金鑰識別郵件(DKIM)驗證採取任何操作。

必要條件

需求

思科建議您瞭解以下主題：

- ESA
- 內容過濾器配置的基本知識
- 有關郵件過濾器配置的基本知識
- 集中策略、病毒和爆發隔離區配置知識

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

步驟1.配置DKIM驗證

確保已啟用DKIM驗證。導航到**Mail Policies > Mail Flow Policies**。

在ESA上配置DKIM驗證與SPF驗證類似。在郵件流策略的**預設策略引數**中，只需將DKIM驗證設定為**開啟**。

步驟2.驗證最終動作

首先，確定根據DKIM驗證要採取的行動。例如：刪除、新增標籤或隔離。如果最終操作是隔離郵件，請檢視配置的隔離區。

- 如果您不使用集中管理：

導航至**ESA > Monitor > Policy, Virus and Outbreak Quarantines**。

- 如果已配置集中管理(SMA):

導覽至**SMA > Email > Message Quarantine > Policy, Virus and Outbreak Quarantines**，如下圖所示：

Policy, Virus and Outbreak Quarantines

Quarantines				
Add Policy Quarantine...		Search Across Quarantines		
Quarantine Name	Type	Messages	Default Action	Last
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	
Policy	Centralized Policy	0	Retain 10 days then Delete	
Unclassified	Unclassified	0	Retain 30 days then Release	
Virus	Antivirus	0	Retain 30 days then Delete	

Available space for

如果沒有針對DKIM/Domain-based Message Authentication, Reporting & Conformance(DMARC)/Sender Policy Framework(SPF)服務的特定隔離。建議建立一個。

在Policy (策略)、 Virus (病毒) 和Outbreak Quarantines (病毒和爆發隔離區) 中，選擇Add Policy Quarantine:

您可以在此處設定：

- 隔離區名稱：對於ex, **DkimQuarantine**
- 保留期：由您決定，並取決於您組織的需求和預設操作。經過保留期後，郵件將被刪除或釋放並傳送，具體取決於您的選擇，如下圖所示：

Add Quarantine

Settings	
Quarantine Name:	<input type="text"/>
Retention Period:	<input type="text" value="40"/> Hours <input type="button" value="v"/>
Default Action:	<input checked="" type="radio"/> Delete <input type="radio"/> Release <input checked="" type="checkbox"/> Free up space by applying default action on messages upon Additional options to apply on Release action (when used) <input type="checkbox"/> Modify Subject <input type="checkbox"/> Add X-Header <input type="checkbox"/> Strip Attachments
Local Users:	<i>No users defined.</i>
Externally Authenticated Users:	<i>External authentication is disabled. Go to System Administration</i>

Cancel


步驟3. ESA傳入過濾器

a.為ESA建立傳入內容過濾器：

導航到ESA > Mail Policies > Incoming Content Filters > Add Filter。

- 第一部分：您可以配置過濾器的名稱、說明和順序：

Add Incoming Content Filter

Content Filter Settings	
Name:	<input type="text"/>
Currently Used by Policies:	<i>No policies currently use this rule.</i>
Description:	<input type="text"/>
Order:	6  (of 6)

- 第二節：新增條件。您可以新增多個條件，並且可以配置多個內容過濾器，以便對DKIM驗證執行操作：

Authentication-Results expected and insights:

- 通過：消息通過了身份驗證測試。
- 中性：未執行身份驗證。
- 溫度：出現可恢復的錯誤。
- 永久錯誤：出現不可恢復的錯誤。
- Hardfail:身份驗證測試失敗。
- 無.郵件未簽名。

Add Condition

- Message Body or Attachment
- Message Body
- URL Category
- URL Reputation
- Message Size
- Message Language
- Macro Detection
- Attachment Content
- Attachment File Info
- Attachment Protection
- Subject Header
- Other Header
- Envelope Sender
- Envelope Recipient
- Receiving Listener
- Remote IP/Hostname
- Reputation Score
- DKIM Authentication**

DKIM Authentication

Is DKIM Authentication Passed?

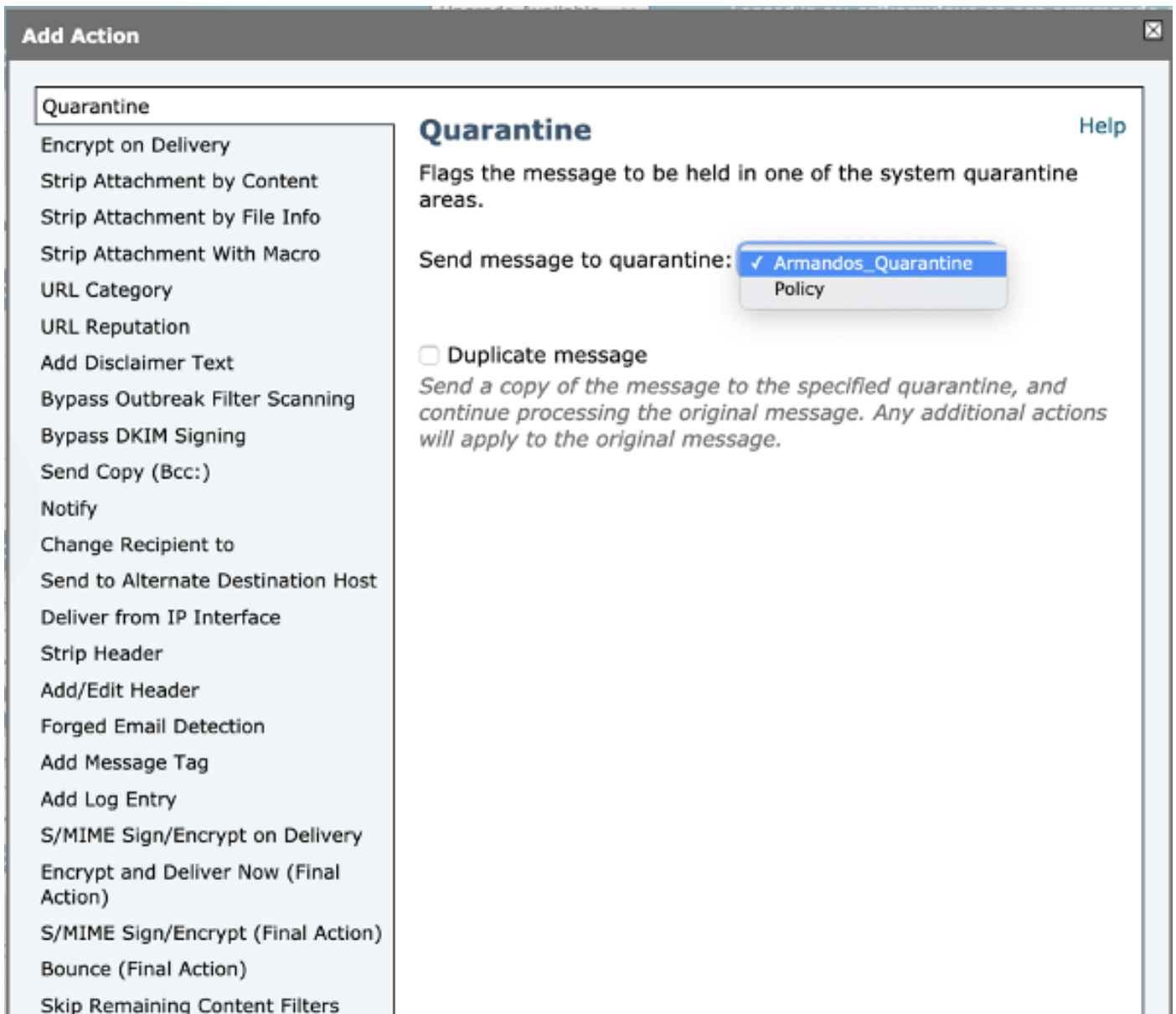
DKIM Authentication Result:

Is **Pass**

- Neutral (message not signed)
- Temperror (recoverable error occurred)
- Permerror (unrecoverable error occurred)
- Hardfail (authentication tests failed)
- None (authentication not performed)

附註：DKIM驗證要求：發件人必須在郵件上簽名才能對其進行驗證。傳送域必須具有在DNS中可用的公鑰以進行驗證。

- **第三節：**選擇操作。您可以新增多個操作，如新增日誌條目、傳送到隔離區、刪除電子郵件、通知等。在這種情況下，選擇先前配置的隔離區，如下圖所示：



向郵件流策略新增新篩選器：

建立過濾器後。在ESA中，對要通過最終操作驗證DKIM的每個郵件流策略新增過濾器。導覽至 **ESA>郵件策略>傳入郵件策略**，如下圖所示：

Incoming Mail Policies

Find Policies

Email Address: Recipient Sender [Find Policies](#)

Policies

[Add Policy...](#)

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	Allow_only_user	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	
2	Tizoncito	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Quarantine Virus Positive: Quarantine	Disabled	Not Available	File_Test	Retention Time: Virus: 1 day Other: 4 hours	

按一下**Content filters**列和**Mail flow policy**行。

附註：（使用預設值）操作並不意味著將其配置為預設策略設定。使用所需的過濾器配置每個郵件流策略。

b. 為ESA建立郵件過濾器：

從ESA CLI配置所有消息過濾器。輸入命令**Filters**並按照說明操作：

```
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW
Enter filter script. Enter '.' on its own line to end.
DKIM_Filter:
If (dkim-authentication == "hardfail" )
{
quarantine("DkimQuarantine");
}
.
1 filters added.
```

建立過濾器後，檢視圖例：**新增了1個篩選條件。**

要配置的條件和操作與傳入內容過濾器使用的條件和操作相同。

驗證

使用本節內容，確認您的組態是否正常運作。

傳入內容過濾器：

- 從ESA Web使用者介面(WebUI)

a. 檢查過濾器是否已設定：

導航到**ESA > Mail Policies > Incoming Content Filters**。必須根據之前在顯示的清單中選定的順序配置過濾器。

b. 檢查過濾器是否已應用：

導航到**ESA > Mail Policies > Incoming mail policies**。

必須在「內容過濾器」列和「郵件流」策略行中顯示過濾器的名稱。如果清單很寬並且看不到名稱，請按一下過濾器清單以標識應用於策略的過濾器。

郵件過濾器：

```
From ESA CLI:
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
```

```
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[ ]> list
```

Num Active Valid Name

```
1 Y Y DKIM_Filter
```

該清單顯示過濾器是否已配置且處於活動狀態。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

驗證設定：

您必須確保：

- 郵件流策略為dkim:驗證
- 在內容篩選器或郵件篩選器中配置了操作
- 如果是內容過濾器，請驗證該過濾器是否與郵件流關聯

驗證郵件跟蹤：

郵件跟蹤允許我們觀察：

- DKIM驗證的結果，例如：permfail
- 配置的日誌條目（如果已配置）
- 應用的篩選器（名稱和執行的操作）

從ESA跟蹤：

```
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 From: <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 RID 0 To: <userb@domainb.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 Message-ID '<3903af$2r@mgt.esa.domain.com>' Fri Apr 26
11:33:44 2019 Info: MID 86 DKIM: permfail body hash did not verify [final]
Fri Apr 26 11:33:44 2019 Info: MID 86 Subject "Let's go to camp!"
Fri Apr 26 11:33:44 2019 Info: MID 86 ready 491 bytes from <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 matched all recipients for per-recipient policy
Allow_only_user in the inbound table
Fri Apr 26 11:33:46 2019 Info: MID 86 interim verdict using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 interim AV verdict using Sophos CLEAN
Fri Apr 26 11:33:46 2019 Info: MID 86 antivirus negative
Fri Apr 26 11:33:46 2019 Info: MID 86 AMP file reputation verdict : UNSCANNABLE
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: GRAYMAIL negative
Fri Apr 26 11:33:46 2019 Info: MID 86 Custom Log Entry: The content that was found was:
DkimFilter
Fri Apr 26 11:33:46 2019 Info: MID 86 Outbreak Filters: verdict negative
Fri Apr 26 11:33:46 2019 Info: MID 86 quarantined to "DkimQuarantine" by add-footer filter
'DkimFilter '
Fri Apr 26 11:33:46 2019 Info: Message finished MID 86 done
```

相關資訊

- [最佳實踐ESA-SPF-DKIM-DMARC](#)
- [郵件安全裝置最終使用手冊](#)
- [DKIM RFC4871](#)
- [DKIM RFC8301](#)
- [DKIM RFC8463](#)
- [技術支援與文件 - Cisco Systems](#)