

集中策略、病毒和爆發隔離區設定及從ESA遷移到SMA的最佳做法

目錄

[簡介](#)

[必要條件](#)

[設定](#)

[驗證](#)

[相關資訊](#)

簡介

以下隔離區現在可以集中到思科安全管理裝置(SMA)上：

- 防毒
- 疫情
- 策略隔離區用於以下對象捕獲的郵件：
 - 郵件過濾器
 - 內容過濾器
 - 防資料丟失策略

集中這些隔離區具有以下優點：

- 管理員可以在一個位置管理來自多個郵件安全裝置(ESA)的隔離郵件。
- 隔離的郵件儲存在防火牆後面而不是DMZ中，降低了安全風險。
- 集中式隔離區可以作為SMA標準備份功能的一部分進行備份。

必要條件

- 運行8.1的SMA(SMA使用手冊，[第8章，集中策略、病毒和爆發隔離區](#))
- 運行8.0.1的ESA(ESA使用手冊，[第27章，隔離區](#))
- 防火牆-埠7025/TCP (傳入和傳出) /主機名使用：AsyncOS IP/說明：集中此功能時，在郵件安全裝置和安全管理裝置之間傳遞策略、病毒和爆發隔離資料

設定

從ESA開始，在現有的策略隔離區中，策略隔離區中有活動郵件：

Messages in Quarantine: "Policy"

Messages in Quarantine: "Policy"								
Action on selected items on page : Release Delete More Actions...				View All Messages Search Quarantine...				
<input type="checkbox"/>	Sender	Recipient	Subject	Received	Scheduled Exit	Size	In Other Quarantines	Quarantined for Reason
<input type="checkbox"/>	robsherw.cisco@gmail.com	robsherw@cisco.com	FuN-Y business	05 Mar 2014 02:38 (GMT +00:00)	15 Mar 2014 02:38 (GMT +00:00)	518	—	Content Filter: '_policy_q_in_'
<input type="checkbox"/>	robsherw.cisco@gmail.com	robsherw@cisco.com	This wasn't funny	05 Mar 2014 02:38 (GMT +00:00)	15 Mar 2014 02:38 (GMT +00:00)	524	—	Content Filter: '_policy_q_in_'
<input type="checkbox"/>	robsherw_cisco@yahoo.com	robsherw@cisco.com	FUNNY thing happened...	05 Mar 2014 02:36 (GMT +00:00)	15 Mar 2014 02:36 (GMT +00:00)	535	—	Content Filter: '_policy_q_in_'

要遷移這些消息，然後依賴SMA作為擁有策略隔離區的活動裝置，請完成以下說明。

在SMA上，導航到管理裝置>集中服務>策略、病毒和爆發隔離區。如果尚未啟用，請點選啟用：

Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines Setting

The Policy, Virus and Outbreak Quarantines are not enabled.

[Enable...](#)

選擇用於處理從ESA到SMA的流量的介面（如果適用）。

注意：隔離埠可能已被更改，但是如果有防火牆/網路ACL，則需要打開它。

Policy, Virus and Outbreak Quarantines

Configure Centralized Quarantines Service

Enable Centralized Quarantines service (for Policy, Virus and Outbreak Quarantines)

Quarantine IP Interface:


Quarantine Port: Specify any available port.

Configuring Centralized Policy, Virus, and Outbreak Quarantines requires the following additional steps:

1. Enable Centralized Policy, Virus, and Outbreak Quarantines for each ESA by selecting Centralized Services > Security Appliances.
2. Configure migration of local quarantines to centralized quarantines by selecting Centralized Services > Policy, Virus, and Outbreak Quarantines.
3. Initiate migration to centralized quarantines by going to each ESA and selecting Security Services > Policy, Virus, and Outbreak Quarantines.

按一下Submit。螢幕將刷新以顯示「服務已啟用」消息，如下所示：

Policy, Virus and Outbreak Quarantines

Attention —  Service enabled. You may proceed with next steps to enable the functionality completely, as shown below.

Policy, Virus and Outbreak (PVO) Quarantine Settings	
Centralized Quarantines Service:	Enabled
Quarantine IP Interface:	(Management)
Quarantine Port:	7025

[Edit Global Settings...](#)

Migration

Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.

Service Migration Steps and Status

Migration Steps	Status
Step 1. On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	0 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. <i>To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.</i>
Step 2. Configure migration of any messages currently quarantined on the ESAs	Migration is not configured for any appliances. Launch Migration Wizard...
Step 3. Log into each ESA to start migration and begin using centralized quarantines.	No ESAs selected.

Email Appliance Status

Selected Email Appliances (ESAs)	Status
No ESAs selected.	

導航到管理裝置>集中服務>安全裝置，並將ESA通訊增加到SMA：

Security Appliances

Centralized Service Status	
Spam Quarantine:	Service disabled
Policy, Virus and Outbreak Quarantines:	Enabled, using 0 licenses <i>Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.</i>
Centralized Email Reporting:	Service disabled
Centralized Email Message Tracking:	Service disabled
Centralized Web Configuration Manager:	Service disabled
Centralized Web Reporting:	Service disabled

Security Appliances

Email

[Add Email Appliance...](#)

No appliances have been added.

Web

No centralized services are currently available.

按一下Add Email Appliance。

註：您只需增加SMA與ESA通訊時使用的IP地址。裝置名稱僅用作管理參考。

Add Email Security Appliance

Email Security Appliance Settings	
Appliance Name:	ESA
IP Address: ?	192.168.1.100
ESA Centralized Services:	<input type="checkbox"/> Spam Quarantine: service disabled <input checked="" type="checkbox"/> Policy, Virus and Outbreak Quarantines <input type="checkbox"/> Centralized Reporting: service disabled <input type="checkbox"/> Centralized Message Tracking: service disabled
Connection Status:	Not established. Establish an SSH connection for synchronization of the Spam Quarantine's Safelist/Blocklist, Policy, Virus and Outbreak Quarantines, Centralized Reporting, and Message Tracking. <input type="button" value="Establish Connection..."/> <input type="button" value="Test Connection"/>

請確保建立連線和測試連線。建立從SMA到ESA的連線時，將請求管理員使用者名稱和密碼。這是正在增加的ESA的管理使用者和密碼。根據已啟用的內容與正在增加的內容，測試結果可能會有所不同，但應類似於：

Add Email Security Appliance

Warning — Not all services are correctly configured on the remote appliance:

- Policy, Virus and Outbreak Quarantines capability check: OK
- Policy, Virus and Outbreak Quarantines service check: Warning: Go to *Centralized Services > Policy, Virus and Outbreak Quarantine* to configure migration once you submit/commit the changes.

確保此時在SMA上進行提交和提交更改。

此時，如果您重新訪問ESA並嘗試配置策略隔離的Centralized Services部分，則類似於以下內容：



Monitor

Mail Policies

Security Services

Network

IP Interfaces

Network Interfaces and IP Addresses

Add IP Interface...

Name

Management

Anti-Spam

IronPort Anti-Spam

Anti-Virus

Sophos

McAfee

Data Loss Prevention

RSA Email DLP

Cisco IronPort Email Encryption

IronPort Image Analysis

Outbreak Filters

SenderBase

Centralized Services

Reporting

Message Tracking

Policy, Virus and Outbreak Quarantines

Spam Quarantine

Service Updates

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved.

Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines Setting

The Policy, Virus and Outbreak (PVO) Quarantines service is not enabled.

There are multiple steps to centralizing Policy, Virus and Outbreak (PVO) Quarantines, before you can enable service on this ESA...

- To configure migration of PVO Quarantines, go to SMA > Management Appliance > Centralized Services > Policy, Virus and Outbreak Quarantines).
- After you enable service and configure migration on the SMA, return here to enable Centralized Policy, Virus and Outbreak (PVO) Quarantines for this ESA.

Enable...

SMA上的遷移步驟仍然必須完成。返回SMA並繼續下一節。




Policy, Virus and Outbreak Quarantines

Warning — Appliance ESA has been added. Not all services are correctly configured on the remote appliance:

- Policy, Virus and Outbreak Quarantines capability check: OK
- Policy, Virus and Outbreak Quarantines service check: Warning: Go to *Centralized Services > Policy, Virus and Outbreak Quarantine* to configure migration once you submit/commit the changes.

Policy, Virus and Outbreak (PVO) Quarantine Settings	
Centralized Quarantines Service:	Enabled
Quarantine IP Interface:	1 (Management)
Quarantine Port:	7025

[Edit Global Settings...](#)

Migration		
Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.		
Service Migration Steps and Status		
Migration Steps		Status
Step 1.	On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. <i>To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.</i>
Step 2.	Configure migration of any messages currently quarantined on the ESAs	 Migration is not configured for 1 out of 1 selected ESAs. <i>Click on the Commit Changes to proceed with 'Launch Migration Wizard' for recently added appliances.</i> Launch Migration Wizard...
Step 3.	Log into each ESA to start migration and begin using centralized quarantines.	 Service is not active on 1 out of 1 selected ESAs. <i>Log into each ESA as required to enable the service (see status below).</i>
Email Appliance Status		
Selected Email Appliances (ESAs)		Status
ESA		 Action Required: Use Migration Wizard to define migration mapping.

完成提交更改後，第2步中的啟動遷移嚮導？將變為活動狀態：

 Migration is not configured for 1 out of 1 selected ESAs.

Use the Migration Wizard to configure how quarantined messages will be migrated.

[Launch Migration Wizard...](#)

選擇Launch Migration Wizard並繼續以下操作：

Configure Migration

Configure migration of ESA Policy Quarantines to Centralized Policy Quarantines

Please Note:
Migration of messages will start **when you will enable centralization** of Policy Quarantines from respective ESAs. At the same time, following things will happen:

- "Virus" and "Outbreak" Quarantines from selected ESAs, will be automatically migrated to respective Centralized Quarantines
- After completion of migration, all the local Policy Quarantines from ESA's (along with "Virus" and "Outbreak") will be deleted
- New messages will begin using new destination Centralized Quarantine on SMA

Configure migration of Policy Quarantines from ESAs associated with this SMA.

Automatic

- All (1) local Policy Quarantines and their messages will be migrated from all (1) ESAs.
- Centralized Policy Quarantine names will be created from existing local Policy Quarantine names.

Custom

- You can select local Policy Quarantines from individual ESAs to migrate.
- You can specify a Centralized Policy Quarantine name for each local ESA Policy Quarantines to migrate.

[Cancel](#) [Next >](#)

如果僅遷移特定隔離區，請選擇Custom。在本示例中，我們將繼續執行自動，此操作會將任何/所有策略隔離區從ESA遷移到SMA。請注意，您將會看到在前面提到的ESA增加期間選擇的指定名稱，後面是通訊中使用的IP地址：

Configure Migration

Configure migration of ESA Policy Quarantines to Centralized Policy Quarantines

Centralized Quarantines

Quarantine names will be automatically created on the SMA by replicating local Policy Quarantine names from ESAs.
If the same Policy Quarantine name exists on multiple ESAs, a single Centralized Policy Quarantine with that name will be created on the SMA.

Centralized Policy Quarantine Name	Migrating from ESA	Size
Policy	ESA (*****)	1.54K

(01) Local Virus Quarantines (from selected 1 ESAs) will be automatically migrated to Centralized "Virus" Quarantine
(01) Local Outbreak Quarantines (from selected 1 ESAs) will be automatically migrated to Centralized "Outbreak" Quarantine

All (1) local Policy Quarantines and their messages will be migrated from all selected (1) ESAs (total 0G)
Available free space at Centralized Policy Quarantines is 36G

[< Back](#) [Next >](#)

按一下Next，然後繼續：

Configure Migration

Configure migration of ESA Policy Quarantines to Centralized Policy Quarantines

Migration is configured

Please Note:
Migration of messages will start **when you will enable centralization** of Policy Quarantines from respective ESAs. At the same time, following things will happen:

- "Virus" and "Outbreak" Quarantines from selected ESAs, will be automatically migrated to respective Centralized Quarantines
- After completion of migration, all the local Policy Quarantines from ESA's (along with "Virus" and "Outbreak") will be deleted
- New messages will begin using new destination Centralized Quarantine on SMA

最後，按一下Submit，此時將顯示「Success」通知：

Policy, Virus and Outbreak Quarantines

Success — Settings have been saved.

Policy, Virus and Outbreak (PVO) Quarantine Settings

Centralized Quarantines Service:	Enabled
Quarantine IP Interface:	Management (Management)
Quarantine Port:	7025

[Edit Global Settings...](#)

Migration

Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.

Service Migration Steps and Status

Migration Steps	Status
Step 1. On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. <i>To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.</i>
Step 2. Configure migration of any messages currently quarantined on the ESAs	Migration is configured for all appliances. <i>Use the Migration Wizard to configure how quarantined messages will be migrated.</i>
Step 3. Log into each ESA to start migration and begin using centralized quarantines.	⚠ Service is not active on 1 out of 1 selected ESAs. <i>Log into each ESA as required to enable the service (see status below).</i>

[Launch Migration Wizard...](#)

Email Appliance Status

Selected Email Appliances (ESAs)	Status
ESA	⚠ Action Required: Log into ESA to enable Centralized Quarantine.

在SMA上提交更改。

返回ESA，導航到安全服務>策略、病毒和爆發隔離區。SMA的先決條件步驟現已得到確認：

Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines Setting

✓ The prerequisite for enabling Centralized Policy, Virus, and Outbreak Quarantines service and configuring migration on the SMA are complete.

You can enable this ESA to use Centralized PVO Quarantines. This will begin migration of messages and quarantines to the Centralized Policy, Virus, and Outbreak Quarantines on the SMA. All messages and quarantines will be deleted from this ESA.

[Enable...](#)

按一下Enable？，然後繼續：

Policy, Virus and Outbreak Quarantines

Configure Centralized Quarantines Service	
<input checked="" type="checkbox"/> Enable Centralized Quarantines (for Policy, Virus and Outbreak Quarantines)	
SMA in use:	:7025
IP interface to accept messages released from SMA:	Management <small>Note: Please make sure selected interface is reachable from SMA 14.2.30.116. Use ping from the SMA to check for a working connection.</small>
Port:	7025 <small>You may use any available free port.</small>
Send Notification When Migration is Complete (Optional)	<input type="text"/> <small>Separate multiple email addresses with commas.</small>

Quarantines Migration			
<ul style="list-style-type: none">Migration to centralized quarantines will start as soon as you submit and commit this page.Please confirm that the migration configuration shown below is correct. Make any changes needed on the SMA before proceeding.Any Policy Quarantines not selected for migration will not be migrated and will be deleted from the ESA.			
Migration Configuration for Policy Quarantines (as Saved at :): ?			
Local (ESA) Quarantine	Target Centralized Quarantine at SMA		
Policy	Policy (Default Policy Quarantine)		
Filters and Actions to be Updated: ?			
Filters and Actions Requiring Updates	Type	Original Policy Quarantine (ESA)	New Centralized Policy Quarantine
No updates are required.			

請注意，此處再次註明了用於通訊的正確埠。這些必須匹配，並且，如果使用了防火牆/網路ACL，則必須打開才能在ESA和SMA之間正確遷移。

注意：如果您在ESA上配置了策略、病毒和爆發隔離區，則一旦您提交此更改，隔離區及其所有郵件都將立即開始遷移。

注意：任何時候只能有一個移轉程式正在進行中。在之前的遷移完成之前，請勿在其他郵件安全裝置上啟用集中策略、病毒和爆發隔離區。

按一下Submit，最後按一下Commit。資訊通知應該類似。如果本地隔離區中已有大量郵件，則從ESA到SMA處理這些郵件可能需要一些時間：

Policy, Virus and Outbreak Quarantines

Info — Migration of Policy, Virus and Outbreak Quarantines finished

Migration of Policy, Virus and Outbreak Quarantines is in progress: **100 %** Complete

Policy, Virus and Outbreak Quarantines Setting

Status:	Enabled
SMA in use:	 :7025
IP interface to accept messages released from SMA:	Management
Port:	7025

[Edit Settings](#)


Centralized Policy Quarantines being used by this ESA (as configured at SMA " ")

Centralized Quarantines
Policy

重新訪問SMA，然後導航到管理裝置>集中服務>策略、病毒和爆發隔離區。現在將完成遷移步驟：

Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak (PVO) Quarantine Settings

Centralized Quarantines Service:	Enabled
Quarantine IP Interface:	 (Management)
Quarantine Port:	7025

[Edit Global Settings...](#)

Migration

Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.

Service Migration Steps and Status

Migration Steps	Status
Step 1. On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. <i>To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.</i>
Step 2. Configure migration of any messages currently quarantined on the ESAs	Migration is configured for all appliances. <i>Use the Migration Wizard to configure how quarantined messages will be migrated.</i>
Step 3. Log into each ESA to start migration and begin using centralized quarantines.	Service is active on all selected ESAs.

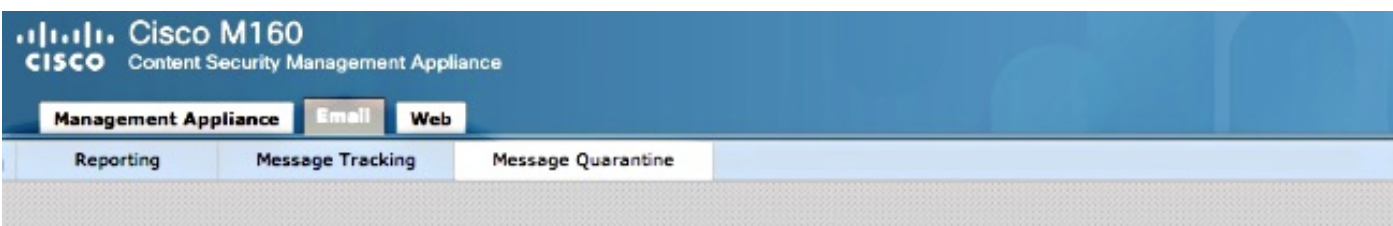
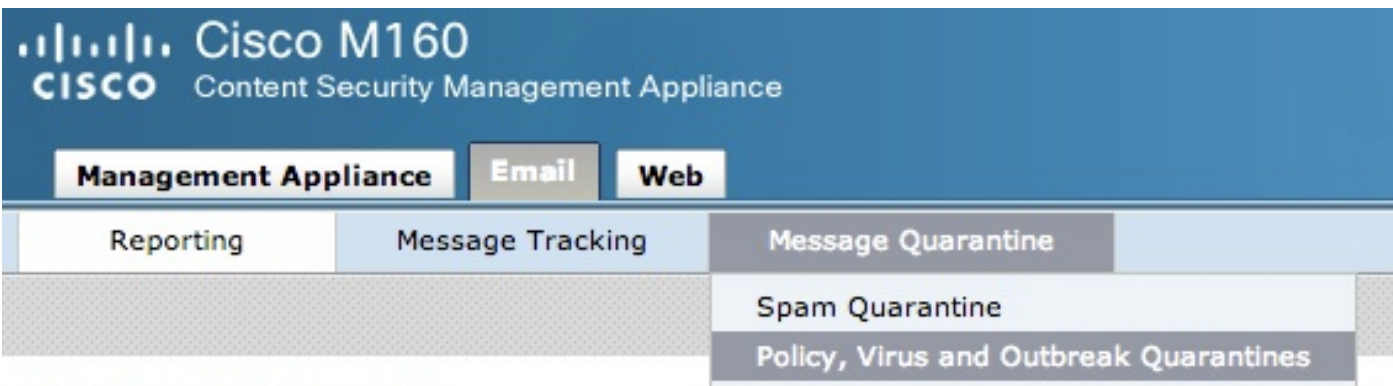
[Launch Migration Wizard...](#)

Email Appliance Status

Selected Email Appliances (ESAs)	Status
ESA	Centralized quarantines are active.

驗證

此時，策略隔離從ESA遷移到SMA的工作已完成。要進行最終驗證，請檢查SMA上的策略隔離：



Policy, Virus and Outbreak Quarantines

Quarantines						
Add Policy Quarantine...		Search Across Quarantines				
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	3	Retain 10 days then Delete	--	1.54K	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 36G.

您應該會看到最初在ESA上列出的相同消息。選取「訊息」欄位中的#超連結，然後確認：

Messages in Quarantine: "Policy"

Messages in Quarantine: "Policy"									
Action on selected items on page: <input type="checkbox"/> Release <input type="checkbox"/> Delete <input type="checkbox"/> More Actions...			View All Messages Search Quarantine...						
<input type="checkbox"/>	Sender	Recipient	Subject	Received	Scheduled Exit	Size	In Other Quarantines	Originating ESA	Quarantined for Reason
<input type="checkbox"/>	robshew_cisco@gmail.co	robshew@cisco.com	Fu/nY business	05 Mar 2014 02:38 (GMT)	15 Mar 2014 02:38 (GMT)	518	--	ESA [14.2.30.113]	Content Filter: '_policy_q_in_'
<input type="checkbox"/>	robshew_cisco@gmail.co	robshew@cisco.com	This wasn't funny	05 Mar 2014 02:38 (GMT)	15 Mar 2014 02:38 (GMT)	524	--	ESA [14.2.30.113]	Content Filter: '_policy_q_in_'
<input type="checkbox"/>	robshew_cisco@yahoo.co	robshew@cisco.com	FUNNY thing happened...	05 Mar 2014 02:36 (GMT)	15 Mar 2014 02:36 (GMT)	535	--	ESA [14.2.30.113]	Content Filter: '_policy_q_in_'

如果您檢視ESA上的mail_logs，將會顯示實際郵件的遷移：

注意：注意ESA (XX.X.XX.XXX)和SMA (YY.Y.YY.YYY)之間透過埠7025進行的通訊。

```

Wed Mar  5 02:48:40 2014 Info: New SMTP DCID 2 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:48:40 2014 Info: DCID 2 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:49:52 2014 Info: New SMTP DCID 3 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:49:52 2014 Info: DCID 3 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:22 2014 Info: New SMTP DCID 4 interface XX.X.XX.XXX address
  
```

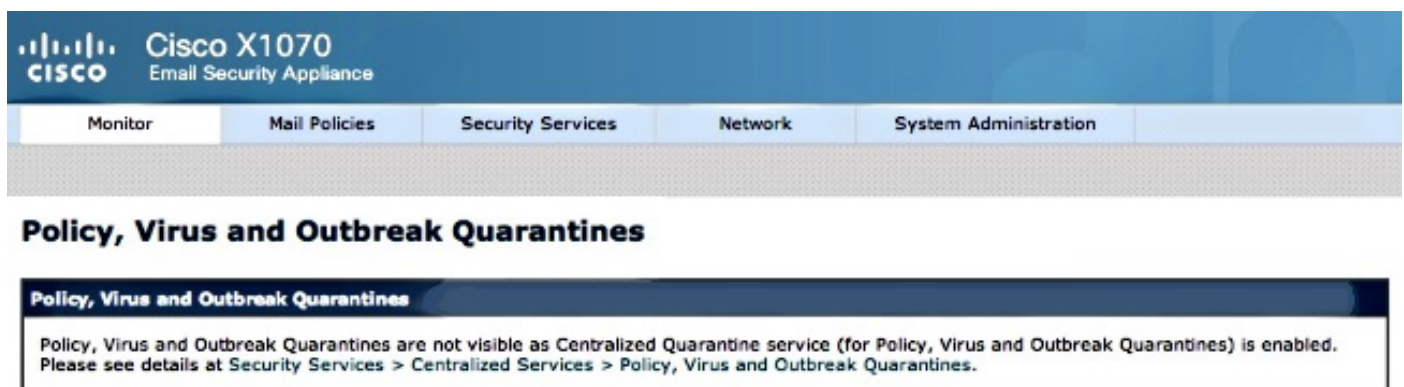
YY.Y.YY.YYY port 7025
Wed Mar 5 02:50:22 2014 Info: DCID 4 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:50:23 2014 Info: New SMTP DCID 5 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:50:23 2014 Info: DCID 5 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:50:40 2014 Info: New SMTP DCID 6 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:50:40 2014 Info: DCID 6 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:50:41 2014 Info: New SMTP DCID 7 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:50:41 2014 Info: DCID 7 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:50:42 2014 Info: New SMTP DCID 8 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:50:42 2014 Info: DCID 8 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:51:01 2014 Info: New SMTP DCID 9 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:51:01 2014 Info: DCID 9 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:51:01 2014 Info: CPQ listener cpq_listener starting
Wed Mar 5 02:51:01 2014 Info: New SMTP DCID 10 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:51:01 2014 Info: DCID 10 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:51:02 2014 Info: New SMTP DCID 11 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:51:02 2014 Info: DCID 11 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:51:02 2014 Info: MID 1 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar 5 02:51:02 2014 Info: MID 1 queued for delivery
Wed Mar 5 02:51:02 2014 Info: New SMTP DCID 12 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:51:02 2014 Info: DCID 12 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:51:02 2014 Info: Delivery start DCID 12 MID 1 to RID [0] to Centralized
Policy Quarantine
Wed Mar 5 02:51:02 2014 Info: MID 2 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar 5 02:51:02 2014 Info: MID 2 queued for delivery
Wed Mar 5 02:51:02 2014 Info: MID 3 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar 5 02:51:02 2014 Info: MID 3 queued for delivery
Wed Mar 5 02:51:02 2014 Info: Message done DCID 12 MID 1 to RID [0] (centralized
policy quarantine)
Wed Mar 5 02:51:02 2014 Info: MID 1 RID [0] Response 'ok: Message 1 accepted'
Wed Mar 5 02:51:02 2014 Info: Message finished MID 1 done
Wed Mar 5 02:51:02 2014 Info: MID 1 migrated from all quarantines
Wed Mar 5 02:51:02 2014 Info: Delivery start DCID 12 MID 2 to RID [0] to Centralized
Policy Quarantine
Wed Mar 5 02:51:02 2014 Info: New SMTP DCID 13 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:51:02 2014 Info: DCID 13 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:51:02 2014 Info: New SMTP DCID 14 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:51:02 2014 Info: DCID 14 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host

```

Wed Mar 5 02:51:02 2014 Info: Message done DCID 12 MID 2 to RID [0] (centralized
policy quarantine)
Wed Mar 5 02:51:02 2014 Info: MID 2 RID [0] Response 'ok: Message 2 accepted'
Wed Mar 5 02:51:02 2014 Info: Message finished MID 2 done
Wed Mar 5 02:51:02 2014 Info: MID 2 migrated from all quarantines
Wed Mar 5 02:51:02 2014 Info: Delivery start DCID 12 MID 3 to RID [0] to Centralized
Policy Quarantine
Wed Mar 5 02:51:02 2014 Info: Message done DCID 12 MID 3 to RID [0] (centralized
policy quarantine)
Wed Mar 5 02:51:02 2014 Info: MID 3 RID [0] Response 'ok: Message 3 accepted'
Wed Mar 5 02:51:02 2014 Info: Message finished MID 3 done
Wed Mar 5 02:51:02 2014 Info: MID 3 migrated from all quarantines
Wed Mar 5 02:51:02 2014 Info: New SMTP DCID 15 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:51:02 2014 Info: DCID 15 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:51:07 2014 Info: DCID 12 close

```

重新訪問ESA，檢視策略、病毒、爆發隔離區時將顯示以下內容：



驗證的下一步是透過ESA傳送新的測試消息，該消息將被捕獲以進行策略隔離。在ESA上檢視 mail_logs，注意突出顯示的一行，指示透過7025從ESA傳輸到SMA，指示策略隔離：

```

Wed Mar 5 02:57:47 2014 Info: Start MID 4 ICID 6
Wed Mar 5 02:57:47 2014 Info: MID 4 ICID 6 From: <robsherw.cisco@gmail.com>
Wed Mar 5 02:57:47 2014 Info: MID 4 ICID 6 RID 0 To: <robsherw@cisco.com>
Wed Mar 5 02:57:47 2014 Info: MID 4 Message-ID
'<7642E61C-4BA2-432E-A524-E163EA0B9753@gmail.com>'
Wed Mar 5 02:57:47 2014 Info: MID 4 Subject 'NEW FUNNY'
Wed Mar 5 02:57:47 2014 Info: MID 4 ready 525 bytes from
<robsherw.cisco@gmail.com>
Wed Mar 5 02:57:47 2014 Info: MID 4 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Mar 5 02:57:47 2014 Info: MID 4 enqueued for transfer to centralized
quarantine "Policy" (content filter _policy_q_in_)
Wed Mar 5 02:57:47 2014 Info: MID 4 queued for delivery
Wed Mar 5 02:57:47 2014 Info: New SMTP DCID 16 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar 5 02:57:47 2014 Info: DCID 16 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar 5 02:57:47 2014 Info: Delivery start DCID 16 MID 4 to RID [0] to Centralized
Policy Quarantine
Wed Mar 5 02:57:47 2014 Info: Message done DCID 16 MID 4 to RID [0] (centralized

```

policy quarantine)

Wed Mar 5 02:57:47 2014 Info: MID 4 RID [0] Response 'ok: Message 4 accepted'

Wed Mar 5 02:57:47 2014 Info: Message finished MID 4 done

Wed Mar 5 02:57:52 2014 Info: DCID 16 close

再次訪問SMA上前面提到的策略隔離，新的測試消息現在也處於隔離狀態：

Messages in Quarantine: "Policy"

Messages in Quarantine: "Policy"									
Action on selected items on page		Release	Delete	More Actions...		View All Messages Search Quarantine...			
<input type="checkbox"/>	Sender	Recipient	Subject	Received	Scheduled Exp	Size	In Other Quarantines	Originating ESA	Quarantined for Reason
<input type="checkbox"/>	robsherw@disco@gmail.co	robsherw@disco.com	NEW FUNNY	05 Mar 2014 02:57 (GMT)	15 Mar 2014 02:57 (GMT)	525	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'
<input type="checkbox"/>	robsherw@disco@gmail.co	robsherw@disco.com	FuNny business	05 Mar 2014 02:38 (GMT)	15 Mar 2014 02:38 (GMT)	518	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'
<input type="checkbox"/>	robsherw@disco@gmail.co	robsherw@disco.com	This wasn't funny	05 Mar 2014 02:38 (GMT)	15 Mar 2014 02:38 (GMT)	524	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'
<input type="checkbox"/>	robsherw_cisco@yahoo.c	robsherw@disco.com	FUNNY thing happened...	05 Mar 2014 02:36 (GMT)	15 Mar 2014 02:36 (GMT)	535	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'

相關資訊

- [無法啟用ESA集中策略、病毒和爆發隔離\(PVO\)](#)
- [Cisco郵件安全裝置-最終使用手冊](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。