

# Best Practices for Centralised Policy, Virus en Outbreak Quarantines Setup en Migratie van ESA naar SMA

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Configureren](#)

[Verificatie](#)

[Gerelateerde informatie](#)

## Inleiding

De volgende quarantaine kan nu collectief worden gecentraliseerd op een Cisco Security Management-applicatie (SMA):

- tegen het virus
- uitbarsting
- Beleidsquarantines die worden gebruikt voor berichten die worden ingesloten door:  
BerichtfiltersContent FiltersBeleid ter voorkoming van gegevensverliezen

Het centraliseren van deze quarantaine biedt de volgende voordelen:

- Beheerders kunnen quarantaineberichten van meerdere e-mail security applicaties (ESA) op één locatie beheren.
- Gewoone berichten worden achter de firewall in plaats van in de DMZ opgeslagen, wat het beveiligingsrisico vermindert.
- Van gecentraliseerde quarantaine kan een back-up worden gemaakt als onderdeel van de standaardback-upfunctie op de SMA.

## Voorwaarden

- SMA met 8.1 (SMA-gebruikersgids, [hoofdstuk 8, Gecentraliseerd beleid, virus en Outbreak-wachtrijen](#))
- ESR van 8.0.1 (ESR-gebruikersgids, [hoofdstuk 27, Garantines](#))
- Firewall - poort 7025 / TCP (in en uit) / Hostname: AsyncOS IPs / Description: Doorgeven van beleid, virus en quarantainegegevens tussen e-mail security applicaties en het Security Management-apparaat wanneer deze optie gecentraliseerd is

## Configureren

Om te beginnen met de ESA, zijn er in een bestaande Policy Quarantine actieve berichten in de Policy Quarantine:

The screenshot shows the Cisco X1070 Email Security Appliance interface. At the top, there are navigation tabs: Monitor, Mail Policies, Security Services, Network, and System Administration. Below this, the page is titled "Messages in Quarantine: 'Policy'". A table lists three quarantined messages:

Sender	Recipient	Subject	Received	Scheduled Exit	Size	In Other Quarantines	Quarantined for Reason
robsherw.cisco@gmail.com	robsherw@cisco.com	FuNnY business	05 Mar 2014 02:38 (GMT +00:00)	15 Mar 2014 02:38 (GMT +00:00)	518	—	Content Filter: '_policy_q_in.'
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.'
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.'

Als u deze berichten wilt verplaatsen en er vervolgens op wilt vertrouwen dat het SMA het actieve apparaat is dat eigenaar is van de Policy Quarantine, specificeert u de volgende aanwijzingen.

Ga in het SMA naar **Management-applicatie > Gecentraliseerde services > Policy, Virus en Outbreak Quarantines**. Als deze nog niet is ingeschakeld, klik op **Enable**:

### Policy, Virus and Outbreak Quarantines

The screenshot shows the "Policy, Virus and Outbreak Quarantines Setting" page. A message states: "The Policy, Virus and Outbreak Quarantines are not enabled." There is an "Enable..." button in the bottom right corner.

Selecteer de interface, indien van toepassing, die bedoeld is om het verkeer van de ESA naar de SMA te verwerken.

Opmerking: De Quarantine-poort kan worden gewijzigd, maar deze moet worden geopend als er een firewall/netwerk-ACL is geïnstalleerd.

### Policy, Virus and Outbreak Quarantines


The screenshot shows the "Configure Centralized Quarantines Service" page. The "Enable Centralized Quarantines service (for Policy, Virus and Outbreak Quarantines)" checkbox is checked. The "Quarantine IP Interface" is set to "(Management)" and the "Quarantine Port" is set to "7025".

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.

Klik op **Inzenden**. Het scherm zal verfrissen om de "service ingeschakeld" te tonen? bericht , zie hieronder :

## 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 &gt; Centralized Services &gt; Security Appliances.</i>
Step 2.	Configure migration of any messages currently quarantined on the ESAs	Migration is not configured for any appliances. <a href="#">Launch Migration Wizard...</a>
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.		

Navigatie in naar **Management-applicatie > Gecentraliseerde services > security applicaties** en voeg de ESA-communicatie toe aan 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	
<a href="#">Add Email Appliance...</a>	
No appliances have been added.	
Web	
No centralized services are currently available.	

Klik op **E-mail toevoegen**.

Opmerking: U hoeft alleen het IP-adres toe te voegen dat de SMA gebruikt om met de ESA te communiceren. De naam van het apparaat wordt alleen gebruikt als administratieve referentie.

## 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"/>

Zorg ervoor dat u **een verbinding** en **testverbinding** instelt. Na de aansluiting van de SMA op de ESA, zal de naam en het wachtwoord van de beheerder worden gevraagd. Dit is de administratieve gebruiker en het wachtwoord van de ESA dat wordt toegevoegd. Op basis van wat al actief is vs. wat wordt toegevoegd, kunnen de resultaten van de test verschillen, maar moeten vergelijkbaar zijn met:

## 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.

Zorg ervoor dat u op dit moment **wijzigingen** op de SMA kunt **indienen** en **doorgeven**.

Als u nu het ESA opnieuw zou bekijken en zou proberen om het Sectie Gecentraliseerde Services van de Beleidsquarantaine te configureren zou deze vergelijkbaar zijn met het volgende:



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...

De migratiestappen moeten nog op de SMA worden uitgevoerd. Ga terug naar de SMA en ga verder met het volgende gedeelte.




## 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 &gt; Centralized Services &gt; 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>  <a href="#">Launch Migration Wizard...</a>
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.

Nadat de **Commit Verandering** is voltooid, de **Wizard Start Migratie?** van stap 2 wordt actief :

 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...](#)

Selecteer de **wizard Migratie starten** en ga als volgt verder:

## 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 >](#)

Als u slechts een bepaalde quarantaine wilt migreren, kiest u **Aangepast**. In dit voorbeeld gaan we verder met **Automatic**, waardoor **ELKE/ALLE** beleidslijnen van het ESA naar SMA zullen worden gemigreerd. Let op dat de gespecificeerde naam die tijdens het ESA werd gekozen, eerder vermeld wordt, gevolgd door het IP-adres dat in de communicatie wordt gebruikt:

## 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 (10.10.10.10)	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 >](#)

Klik op **Volgende** en ga verder:

## 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

Klik tot slot op **Inzenden** en het bericht "Succes" wordt weergegeven:

## 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 &gt; Centralized Services &gt; 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>

**Email Appliance Status**

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


[Launch Migration Wizard...](#)

Doe je wijzigingen in de VS.

Terugkeren naar de ESA, navigeer naar **Security Services > Policy, Virus en Outbreak Quarantines**. De noodzakelijke stappen op de SMA worden nu erkend:

## 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...](#)

Klik op **Inschakelen?** en ga verder:



## 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"><li>Migration to centralized quarantines will start as soon as you submit and commit this page.</li><li>Please confirm that the migration configuration shown below is correct. Make any changes needed on the SMA before proceeding.</li><li>Any Policy Quarantines <b>not selected</b> for migration will <b>not be migrated</b> and will be <b>deleted</b> from the ESA.</li></ul>			
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.			

Merk op dat hier opnieuw de juiste poort wordt gebruikt voor communicatie. Deze moeten overeenkomen en indien ACL-firewall/netwerk in gebruik is, moeten deze worden geopend om een goede migratie tussen ESA en SMA mogelijk te maken.

**Opmerking:** Als je beleid, virus en quarantaine-uitbraken hebt ingesteld op een ESA, begint de migratie van quarantaine en al hun berichten zodra je deze verandering geëngageerd hebt.

**Opmerking:** Op ieder moment kan slechts één migratieproces worden doorlopen. Laat geen gecentraliseerde beleids-, virus- en uitbraakquarantaine op een ander e-mailsecurity apparaat inschakelen totdat de vorige migratie is voltooid.


Klik op **Inzenden** en klik vervolgens op **Commit**. De informatie moet gelijkaardig zijn. Als er al een groot aantal berichten in de plaatselijke quarantaine zijn, kan het tijd duren om deze te verwerken van ESA tot SMA:

## 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

Controleer de **startvertraging** en navigeer naar **applicatie > Gecentraliseerde services > Wachtwoord voor beleid, virus en uiteinde**. De migratiestappen worden nu uitgevoerd:

## 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
<p>Step 1. On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines</p>	<p>1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA.</p> <p><i>To select additional ESA appliances, go to Management Appliance &gt; Centralized Services &gt; Security Appliances.</i></p>
<p>Step 2. Configure migration of any messages currently quarantined on the ESAs</p>	<p>Migration is configured for all appliances.</p> <p><i>Use the Migration Wizard to configure how quarantined messages will be migrated.</i></p> <p style="text-align: right;"><a href="#">Launch Migration Wizard...</a></p>
<p>Step 3. Log into each ESA to start migration and begin using centralized quarantines.</p>	<p>Service is active on all selected ESAs.</p>

#### Email Appliance Status

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

## Verificatie

Op dat moment is de migratie van de Beleidsquarantaine van de ESA naar de SMA voltooid. Controleer voor eindcontrole de Policy Quarantine op de SMA:

Management Appliance

Email

Web

Reporting

Message Tracking

Message Quarantine

Spam Quarantine

Policy, Virus and Outbreak Quarantines

Management Appliance

Email

Web

Reporting

Message Tracking

Message Quarantine

## 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.

U dient dezelfde berichten te zien als die welke oorspronkelijk in de ESA stonden. Selecteer de # hyperlink in de berichtenkolom en controleer:

### 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"/>	robshew.cisco@gmail.com	robshew@cisco.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"/>	robshew.cisco@gmail.com	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.com	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_'

Als je kijkt naar de mail\_logs van de ESA, zal de migratie van de eigenlijke berichten worden gepresenteerd:

**Opmerking:** Let op het gebruik van communicatie tussen de ESA (XX.X.XX.XXX) en SMA (YY.Y.YY.YYY) via poort 7025.

```
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

```

Revisit the ESA, en het volgende wordt nu getoond wanneer je het Policy, Virus, Outbreak Quarantines bekijkt:

The screenshot shows the Cisco X1070 Email Security Appliance interface. The top navigation bar includes 'Monitor', 'Mail Policies', 'Security Services', 'Network', and 'System Administration'. The main heading is 'Policy, Virus and Outbreak Quarantines'. Below this, a message box contains the following text:

**Policy, Virus and Outbreak Quarantines**

Policy, Virus and Outbreak Quarantines are not visible as Centralized Quarantine service (for Policy, Virus and Outbreak Quarantines) is enabled. Please see details at Security Services > Centralized Services > Policy, Virus and Outbreak Quarantines.

De volgende stap van controle is het sturen van een nieuw testbericht door de ESA dat zal worden gevangen voor beleidsmatige quarantaine. Als je kijkt naar mail\_logs op het ESA, merk dan de gemarkeerde lijn op die aangeeft dat ESA via 7025 overhevelt naar SMA, met vermelding van de Beleidsquarantaine:

```

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

Herzie de eerder genoemde Policy Quarantine op de SMA en het nieuwe testbericht is nu ook in quarantaine geplaatst:

#### 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.co	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_'	

## Gerelateerde informatie

- [ESA Centralizing Policy, Virus en Outbreak Quarantine \(PVO\) kunnen niet worden ingeschakeld](#)
- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)