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

Inhoud

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:

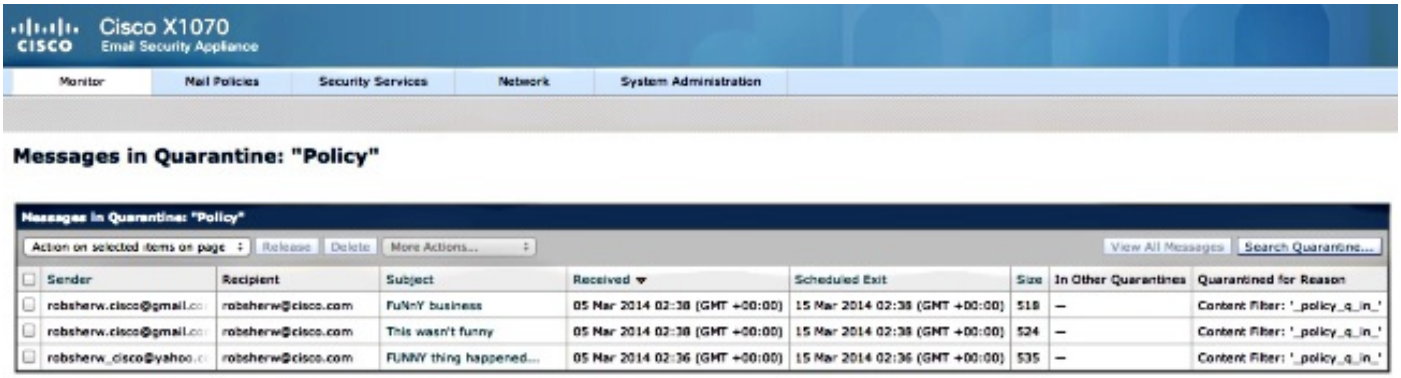
- Beheerders kunnen quarantaineberichten van meerdere e-mail security applicaties (ESA) op één locatie beheren.
- Gewoonde berichten worden achter de firewall in plaats van in de DMZ opgeslagen, wat het beveiligingsrisico vermindert.
- Van gecentraliseerde quarantaine kan een back-up worden gemaakt als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

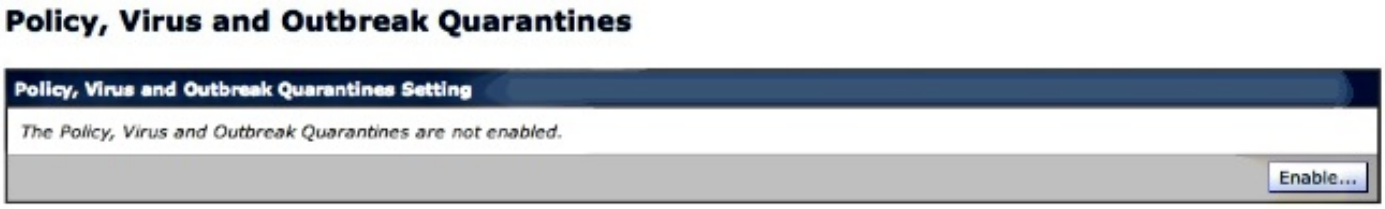
Configureren

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



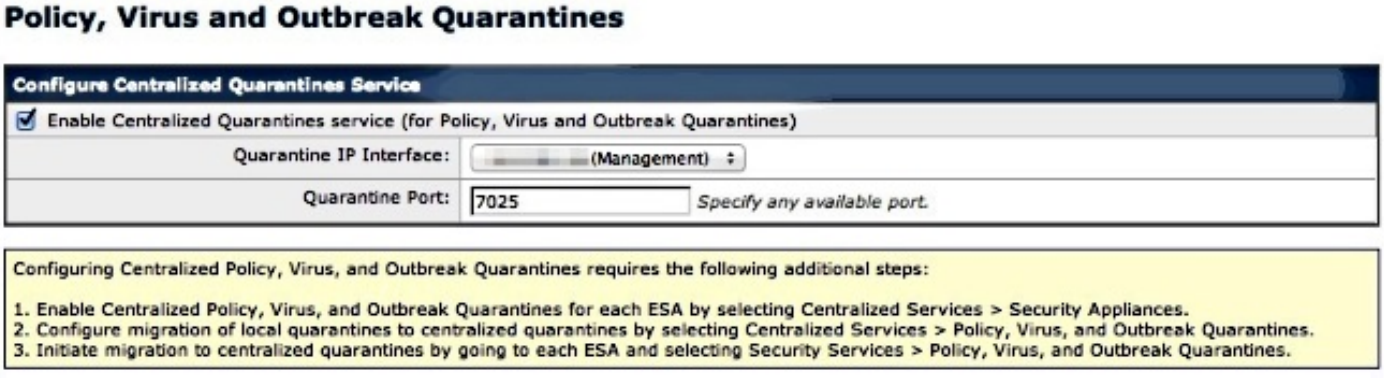
Als u deze berichten wilt verplaatsen en er vervolgens op wilt vertrouwen dat het SMA het actieve apparaat is dat eigenaar is van de Policy Quarantine, specificeert u de volgende aanwijzingen.

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

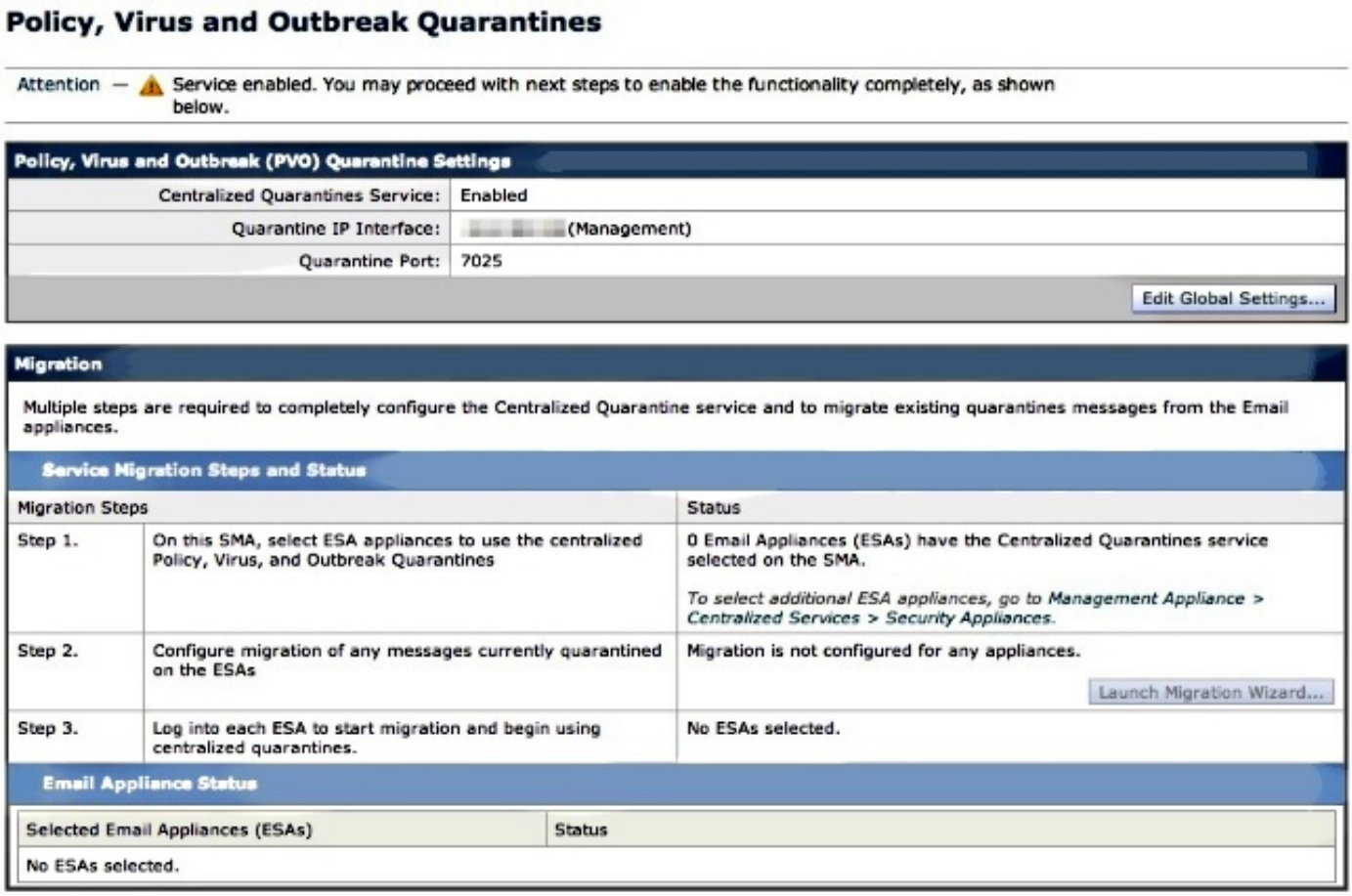


Selecteer de interface, indien van toepassing, die bedoeld is om het verkeer van de ESA naar de SMA te verwerken.

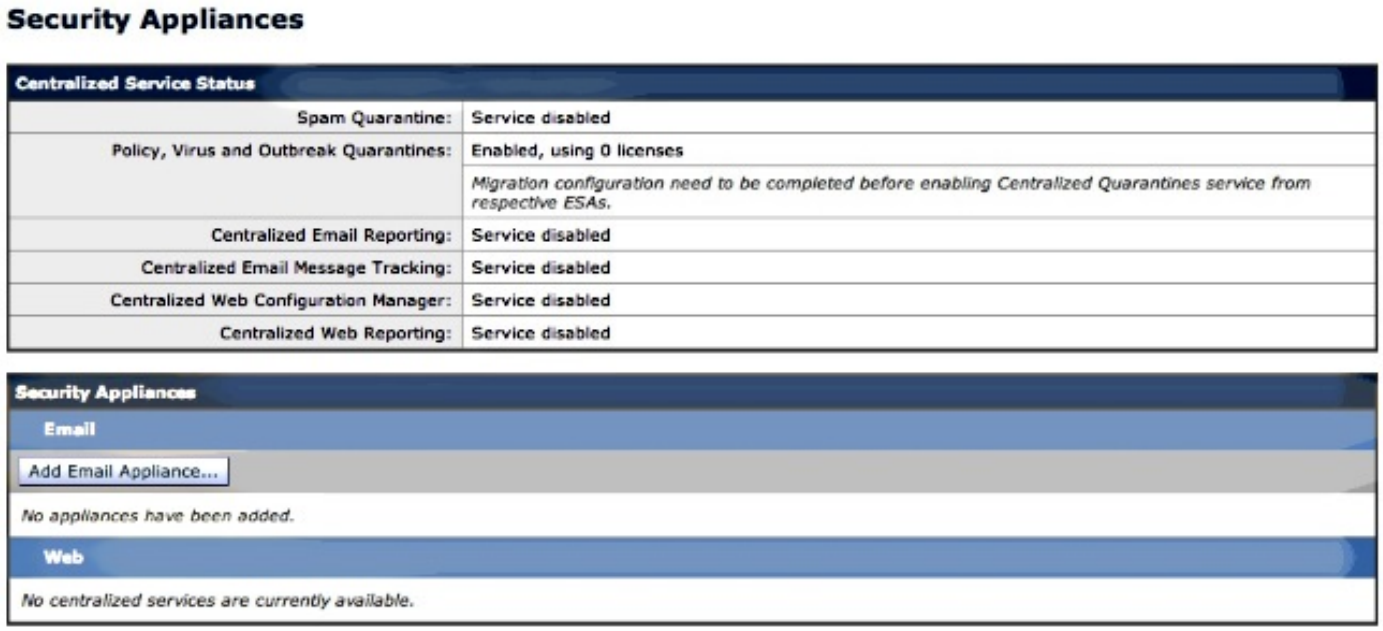
> Opmerking: De Quarantine-poort kan worden gewijzigd, maar deze moet worden geopend als er een firewall/netwerk-ACL is geïnstalleerd.



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

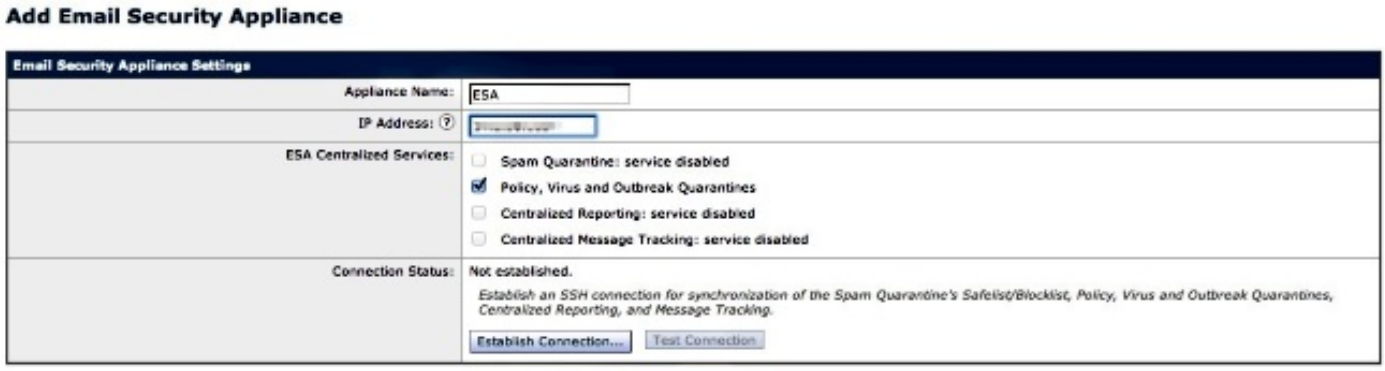


Navigatie in naar **Management-applicatie > Gecentraliseerde services > security applicaties** en voeg de ESA-communicatie toe aan SMA:

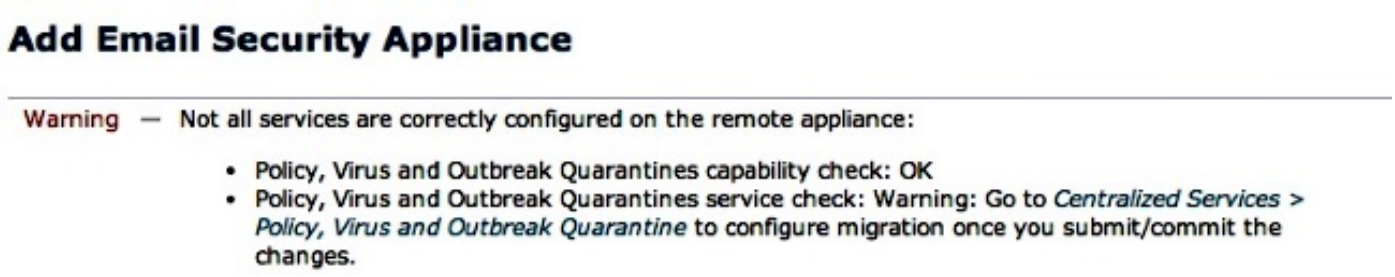


Klik op **E-mail toevoegen**.

> 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.

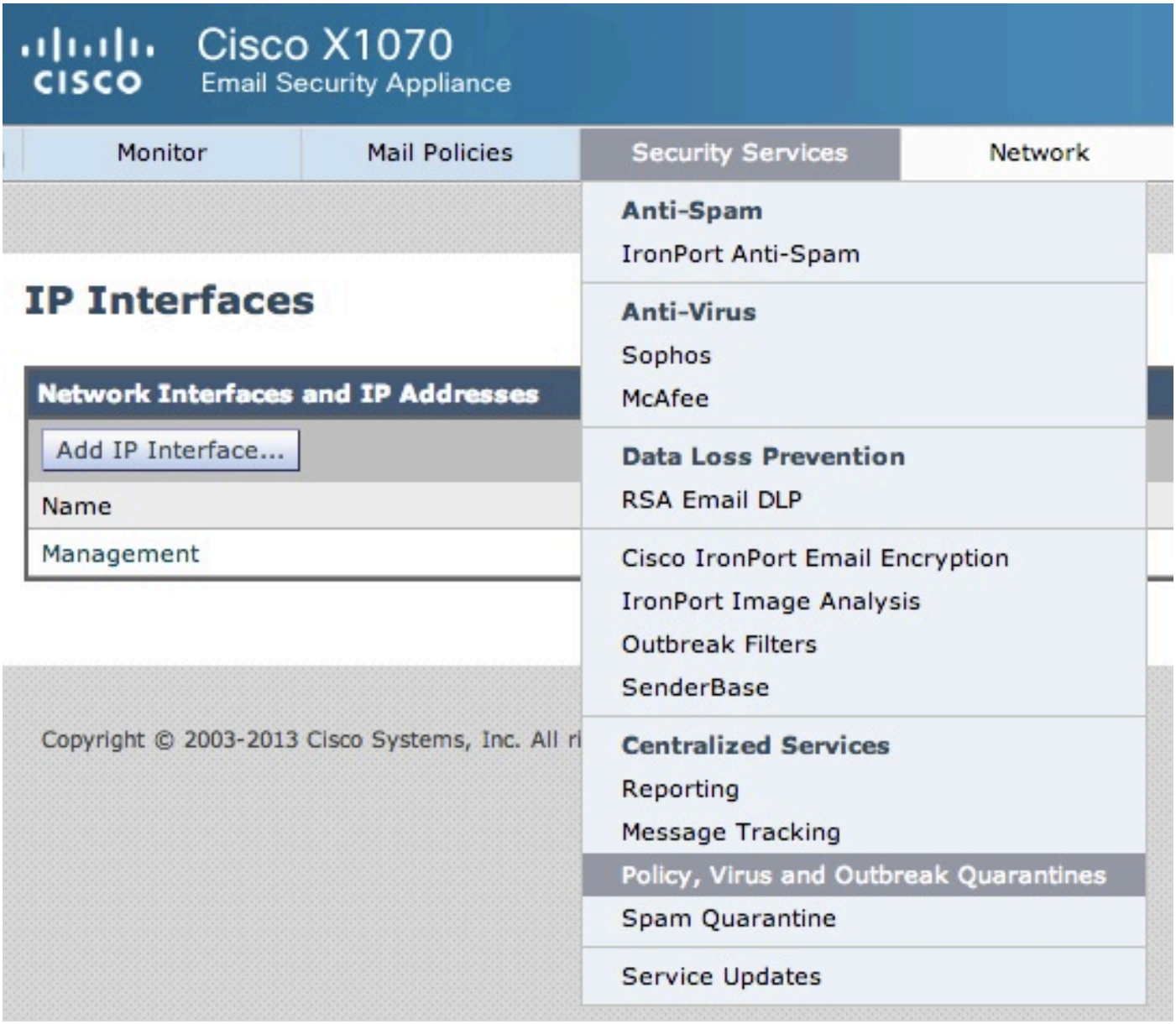


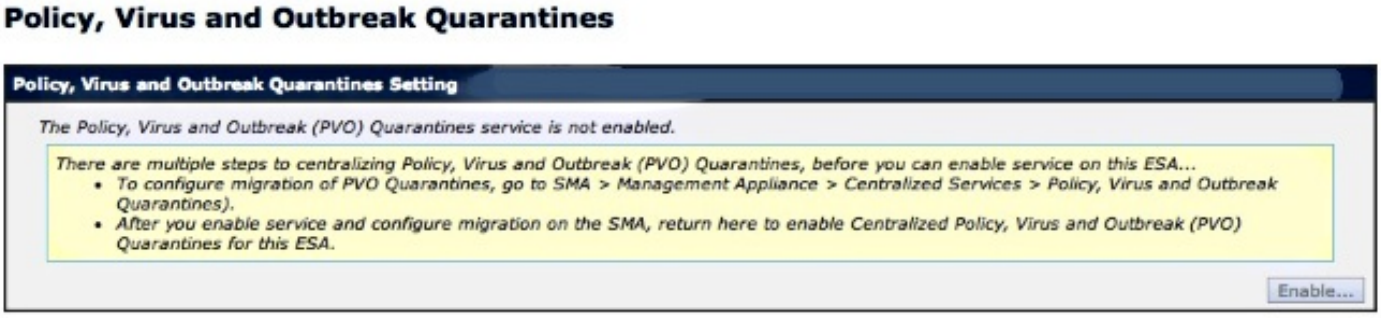
Zorg ervoor dat u **een verbinding** en **testverbinding** instelt. Na de aansluiting van de SMA op de ESA, zal de naam en het wachtwoord van de beheerder worden gevraagd. Dit is de administratieve gebruiker en het wachtwoord van de ESA dat wordt toegevoegd. Op basis van wat al actief is vs. wat wordt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



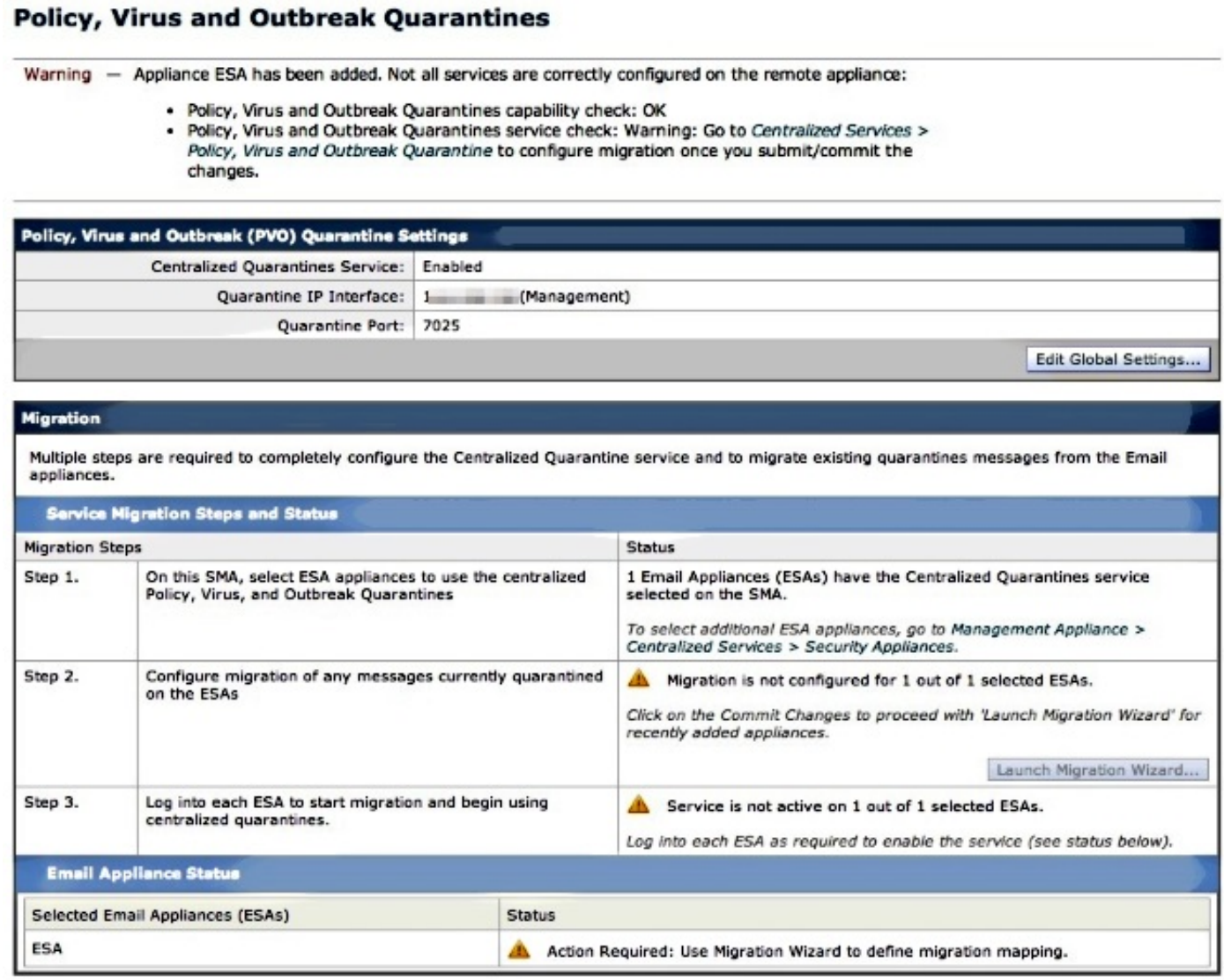
Zorg ervoor dat u op dit moment **wijzigingen** op de SMA kunt **indienen** en **doorgeven**.

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:

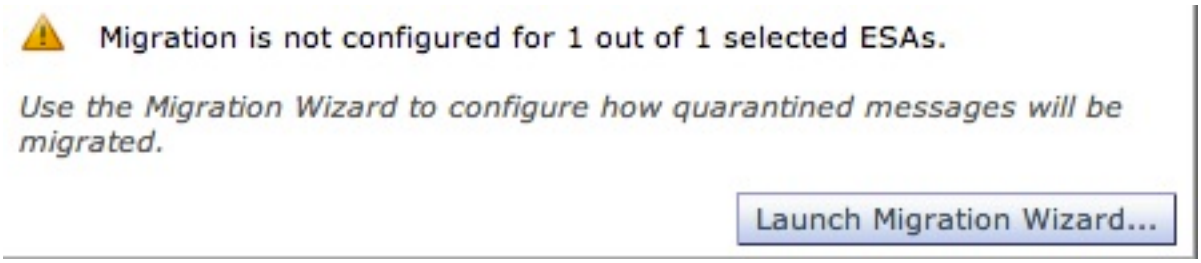




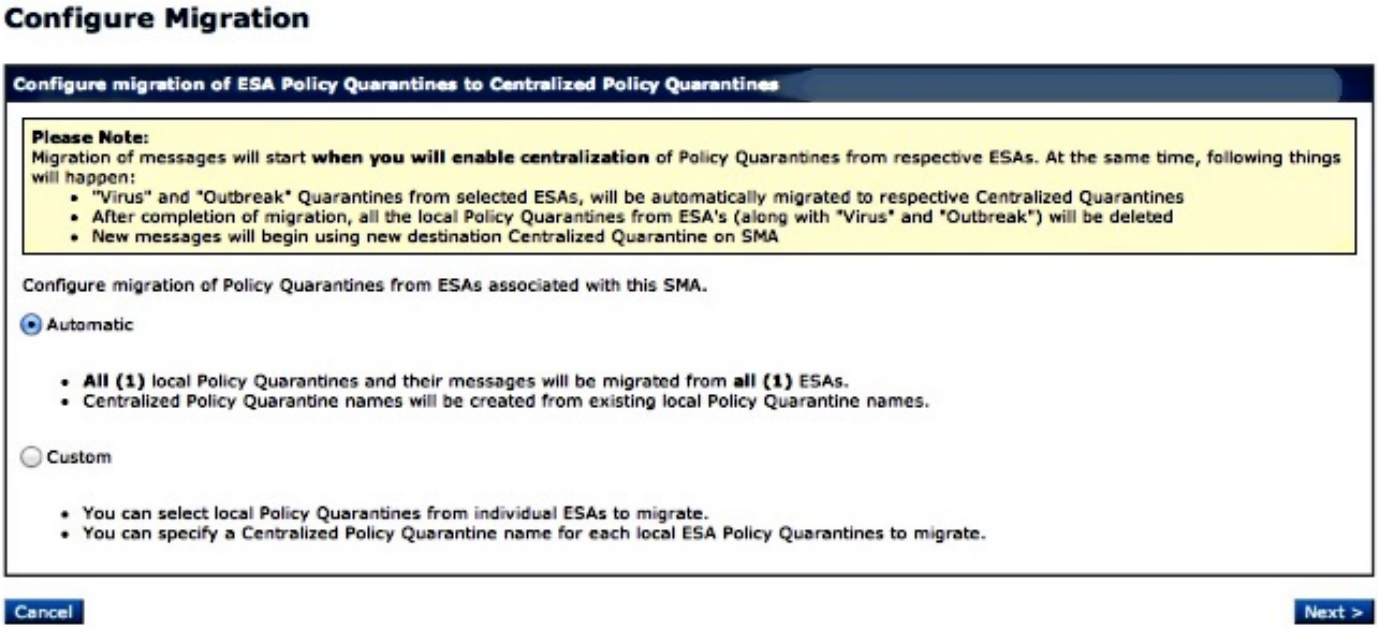
De migratiestappen moeten nog op de SMA worden uitgevoerd. Ga terug naar de SMA en ga verder met het volgende gedeelte.



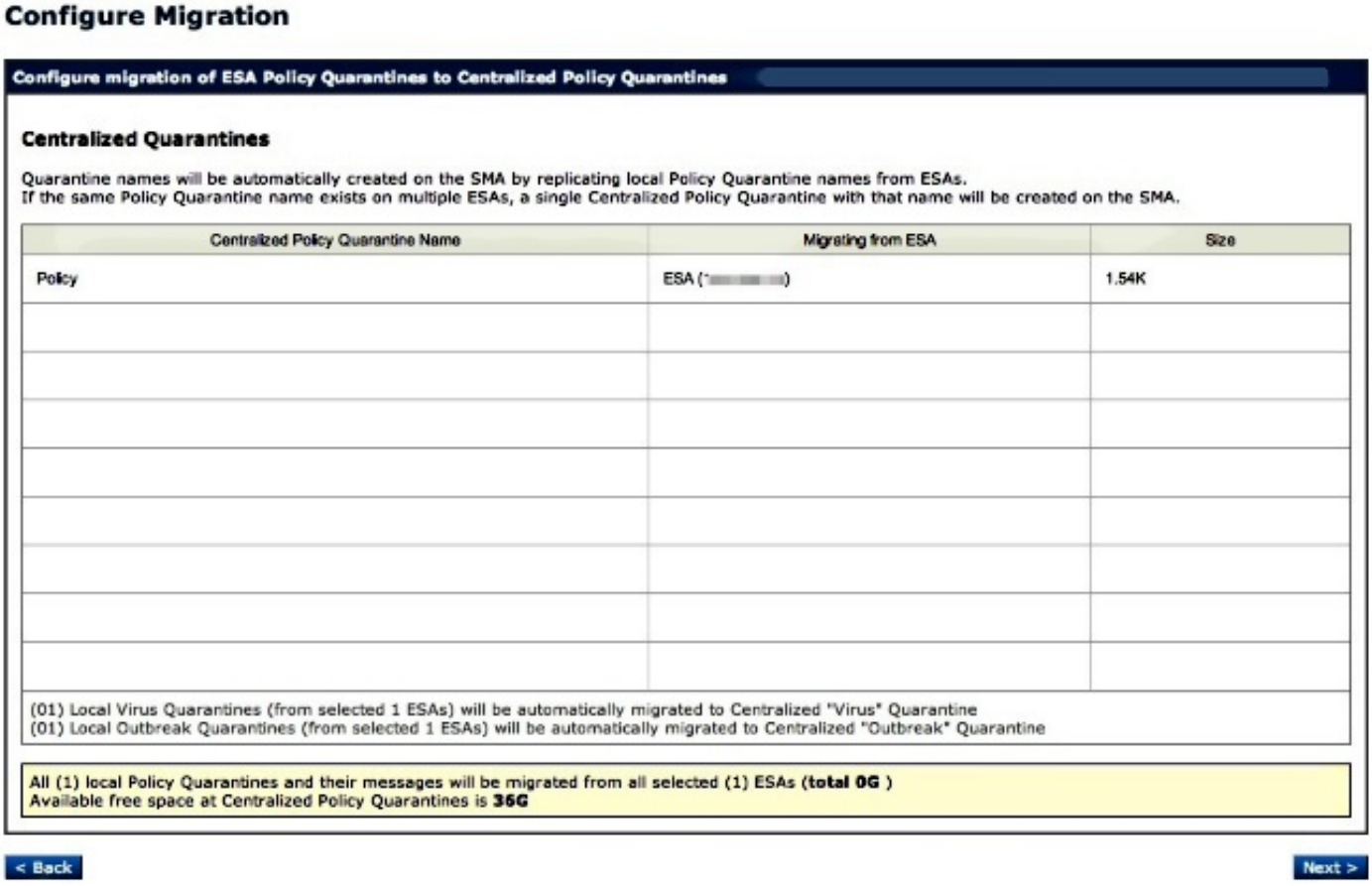
Nadat de **Commit Verandering** is voltooid, de **Wizard Start Migratie?** van stap 2 wordt actief :



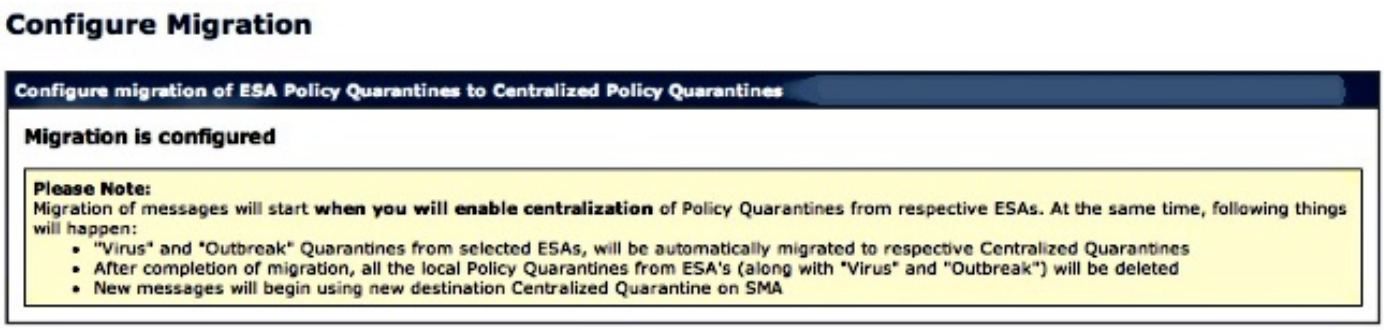
Selecteer **de wizard Migratie starten** en ga als volgt verder:



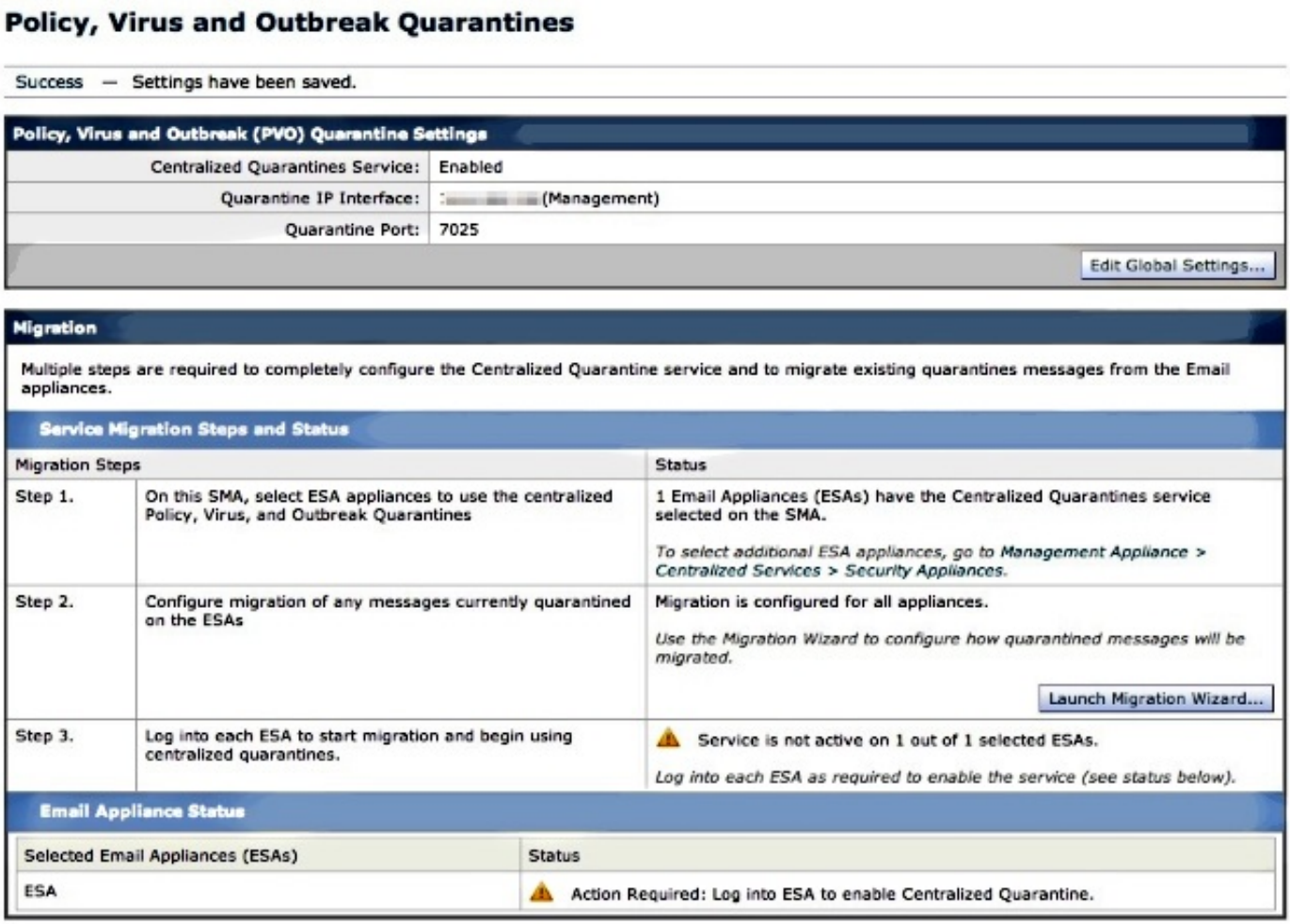
Als u slechts een bepaalde quarantaine wilt migreren, kiest u **Aangepast**. In dit voorbeeld gaan we verder met **Automatic**, waardoor ELKE/ALLE beleidslijnen van het ESA naar SMA zullen worden gemigreerd. Let op dat de gespecificeerde naam die tijdens het ESA werd gekozen, eerder vermeld wordt, gevolgd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



Klik op **Volgende** en ga verder:

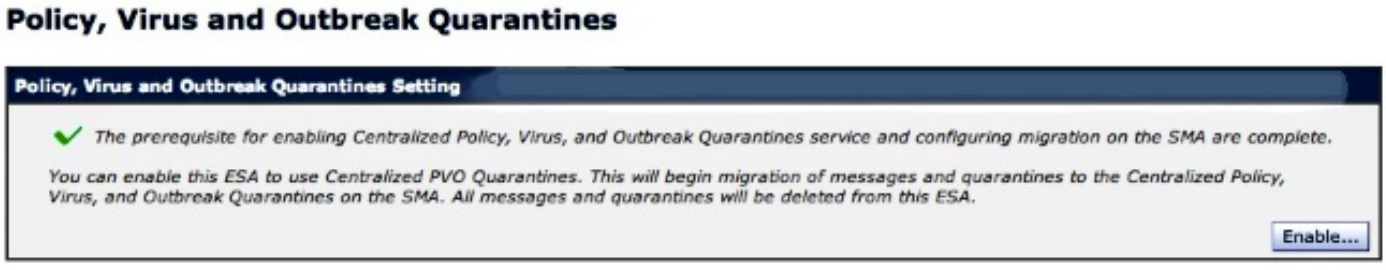


Klik tot slot op **Inzenden** en het bericht "Succes" wordt weergegeven:

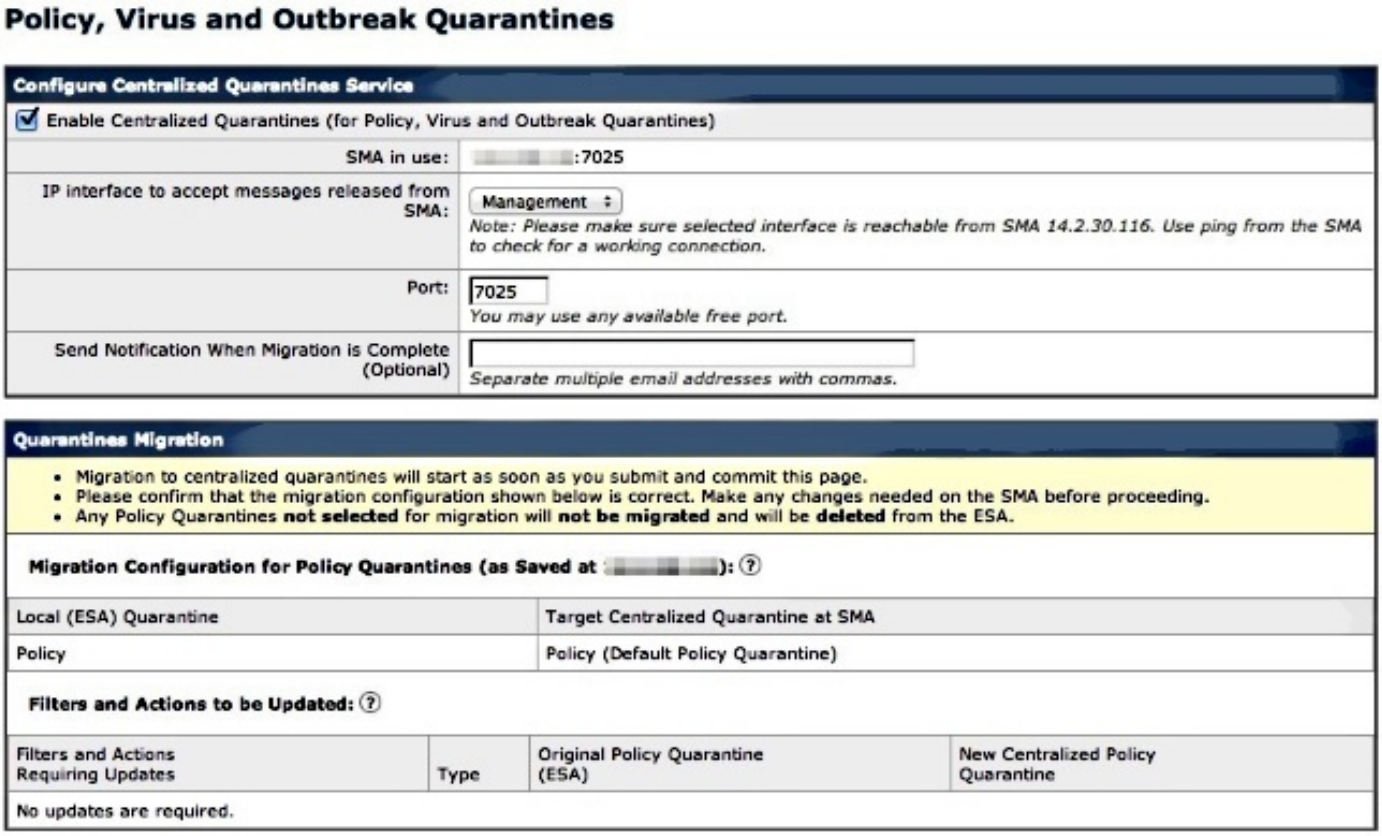


Doe je wijzigingen in de VS.

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



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

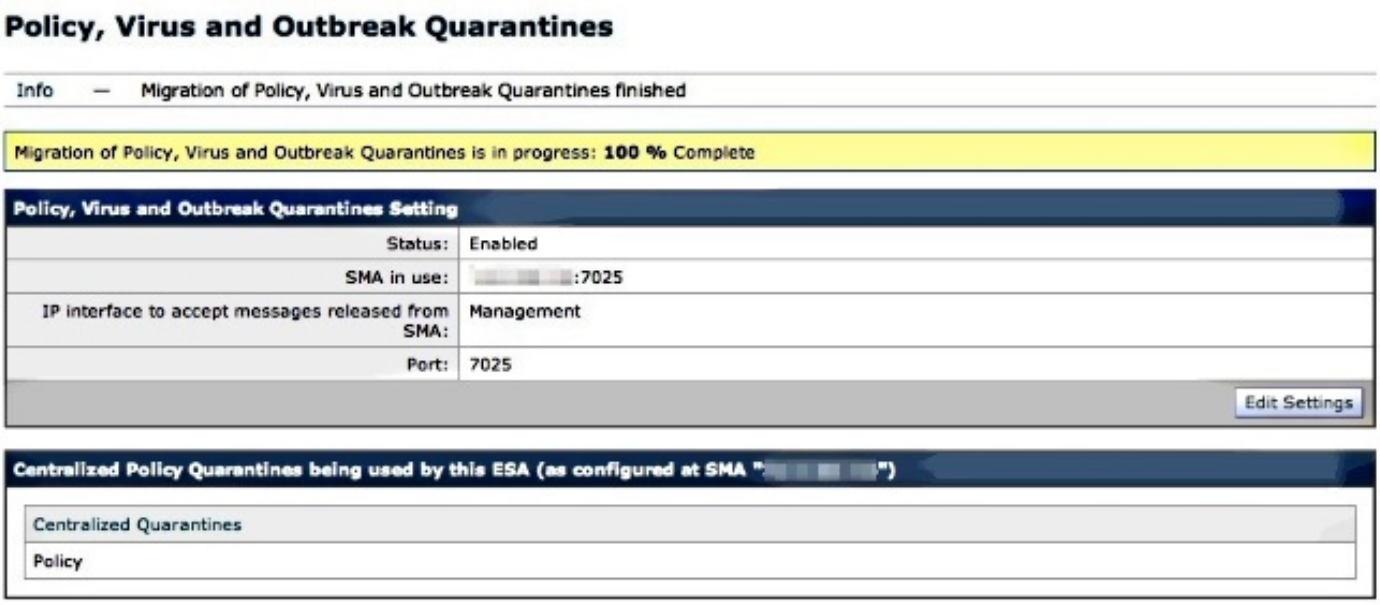


Merk op dat hier opnieuw de juiste poort wordt gebruikt voor communicatie. Deze moeten overeenkomen en indien ACL-firewall/netwerk in gebruik is, moeten deze worden geopend om een goede migratie tussen ESA en SMA mogelijk te maken.

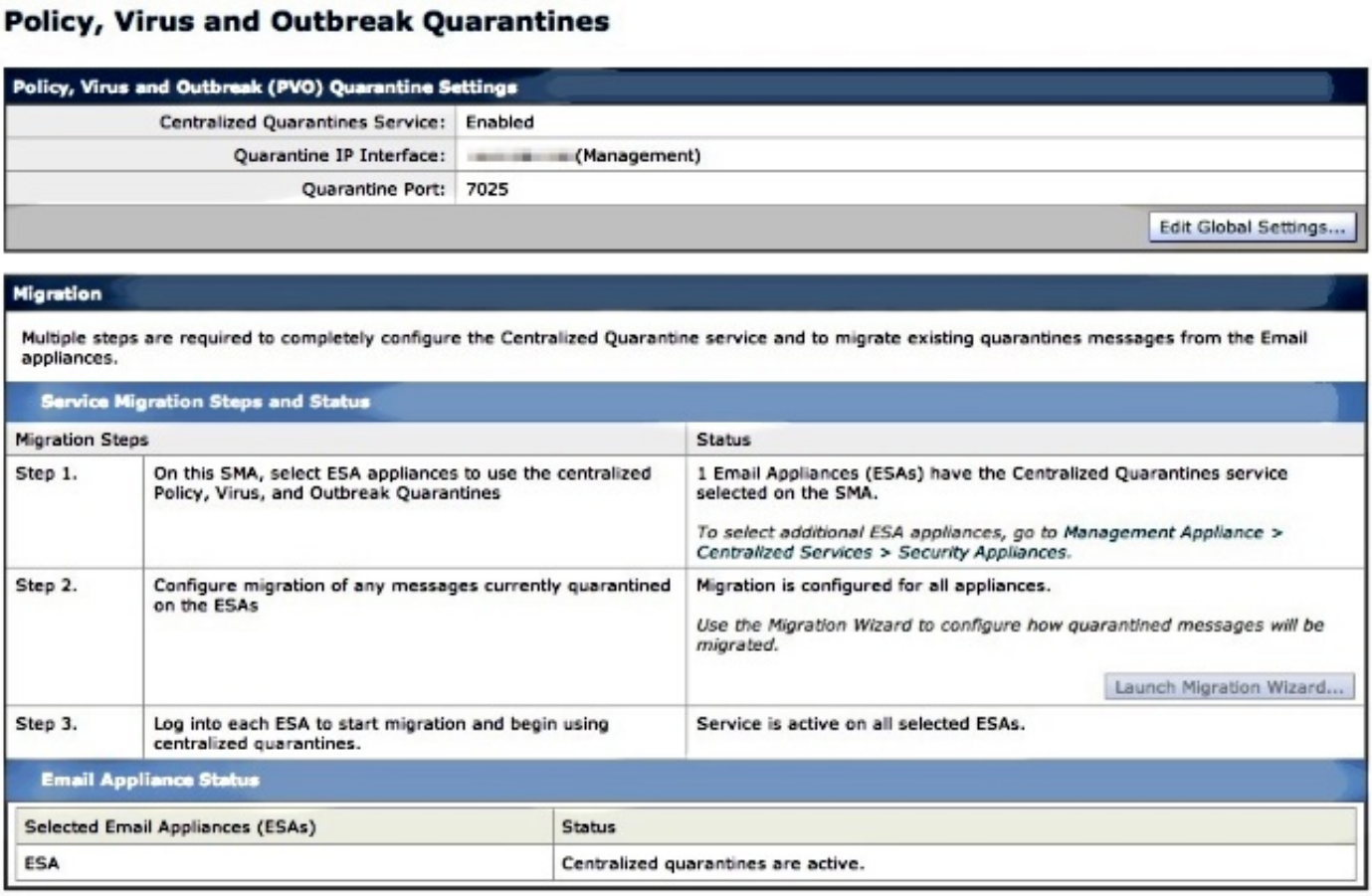
> **Opmerking**: Als je beleid, virus en quarantaine-uitbraken hebt ingesteld op een ESA, begint de migratie van quarantaine en al hun berichten zodra je deze verandering geëngageerd hebt.

> **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:

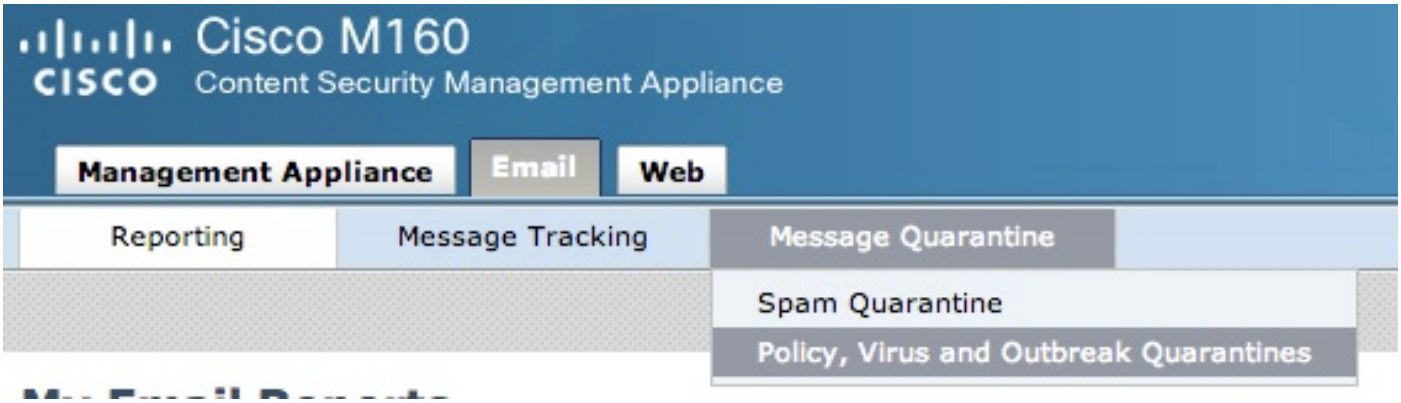


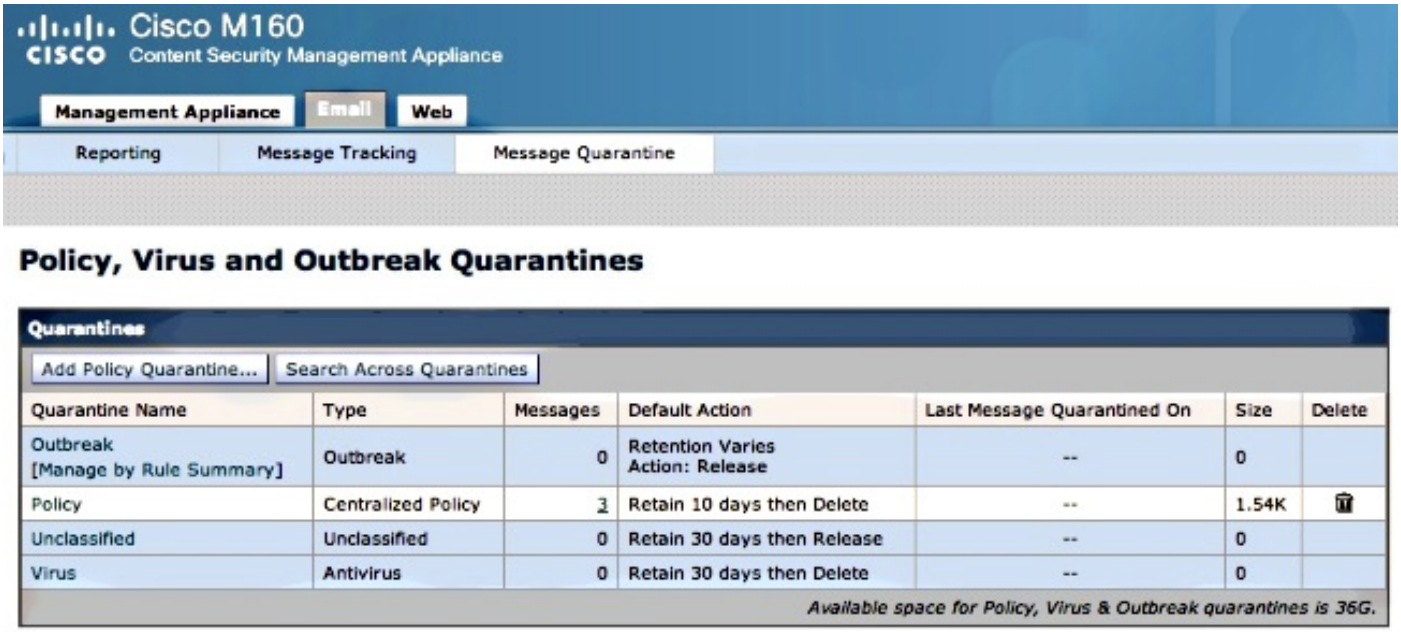
Controleer de **startvertraging** en navigeer naar **applicatie > Gecentraliseerde services > Wachtwoord voor beleid, virus en uiteinde**. De migratiestappen worden nu uitgevoerd:



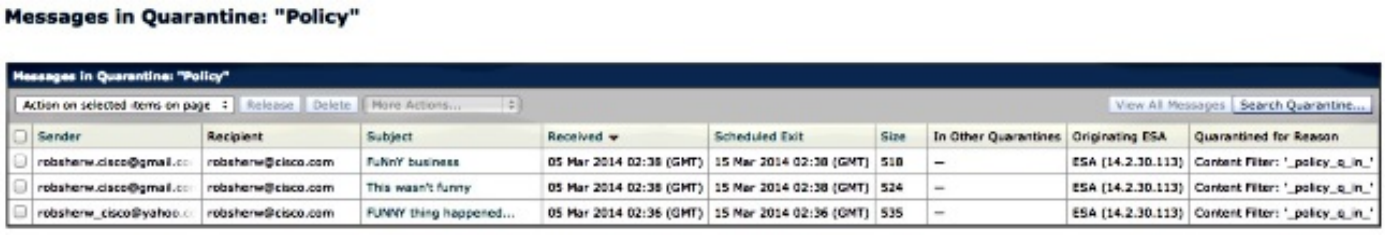
Verificatie

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:





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



Als je kijkt naar de mail_logs van de ESA, zal de migratie van de eigenlijke berichten worden gepresenteerd:

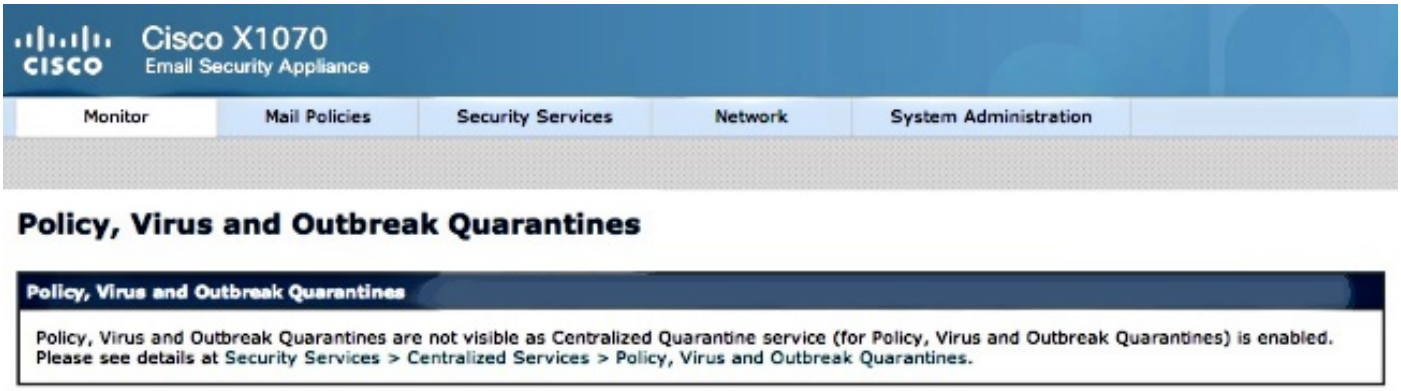
> **Opmerking**: Let op het gebruik van communicatie tussen de ESA (XX.X.XX.XXX) en SMA (YY.Y.YY.YYY) via poort 7025.

```
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:



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"

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]