

Comprehensive SPA Quarantine Setup Guide over e-mail security applicatie (ESA) en security beheerapplicatie (SMA)

Inhoud

[Inleiding](#)

[Procedure](#)

[Local Spam Quarantine op ESA configureren](#)

[Quarantaine poorten inschakelen en een Quarantaine URL op de interface specificeren](#)

[Configureer de ESA om positieve spam te verplaatsen en/of spam te verdenken tot spam quarantaine](#)

[Externe spamquarantaine instellen op de SMA](#)

[Spam Quarantine-melding instellen](#)

[Wachtwoord voor eindgebruiker instellen voor quarantaine-toegang via SPA0000 Quarantine-eindgebruikersverificatie](#)

[Administratieve gebruikerstoegang instellen tot de SPM-quarantaine](#)

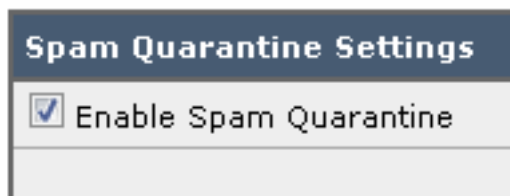
Inleiding

In dit document wordt beschreven hoe u de spamquarantaine op de ESA of SMA kunt configureren en welke functies u daarbij moet gebruiken: externe echtheidscontrole door middel van lidaf- en spamquarantainekennisgeving.

Procedure


Local Spam Quarantine op ESA configureren

1. Kies in het ESA de optie **Monitor > Spam Quarantine**.
2. In het gedeelte Wachtwoord quarantaine instellingen, controleert u het vakje **Spam Quarantine inschakelen** en stelt u de gewenste quarantaineinstellingen in.



3. Kies **Security Services > Samsm Quarantine**.
4. Zorg ervoor dat het aanvinkvakje **Externe spam Quarantine inschakelen** niet is ingeschakeld, tenzij u van plan bent om Externe spam Quarantine te gebruiken (zie paragraaf hieronder).

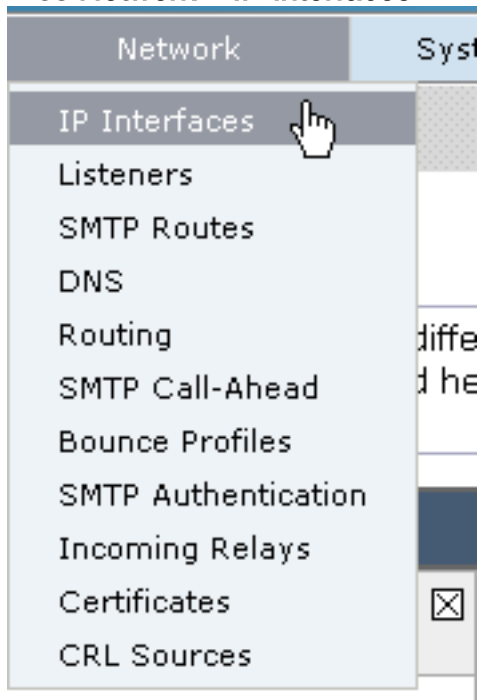
External Spam Quarantine Settings

 **Enable External Spam Quarantine**

5. Breng veranderingen in en begaan.

Quarantaine poorten inschakelen en een Quarantaine URL op de interface specificeren

1. Kies **Netwerk > IP-interfaces**.



2. Klik op de interfacenaam van de interface die u gebruikt om tot de quarantaine te toegang. In het gedeelte spamquarantaine controleert u de vinkjes en specificeert u de standaardpoorten of de gewenste wijziging: Spam Quarantine HTTP Spam Quarantine HTTPS

Spam Quarantine	
<input checked="" type="checkbox"/> Spam Quarantine HTTP	82
<input checked="" type="checkbox"/> Spam Quarantine HTTPS	83

3. Controleer **dit is de standaardinterface voor het** aanvinkvakje **Spam Quarantine**.

4. Onder "URL DIN WEERGEGEVEN IN MELDINGEN" gebruikt het apparaat standaard de systeemhostname (cli: **sethostname**), tenzij anders gespecificeerd in de tweede radioknop optie en het tekstveld. Dit voorbeeld specificeert de standaardinstelling van de

This is the default interface for Spam Quarantine
Quarantine login and notifications will originate on this interface.
URL Displayed in Notifications:
 Hostname

(examples: http://spamQ.url/, http://10.1.1.1:82/)

hostname.

U kunt

een aangepaste URL instellen om toegang te krijgen tot uw Samsm

This is the default interface for Spam Quarantine
Quarantine login and notifications will originate on this interface.
URL Displayed in Notifications:
 Hostname

(examples: http://spamQ.url/, http://10.1.1.1:82/)

Quarantine.

Op

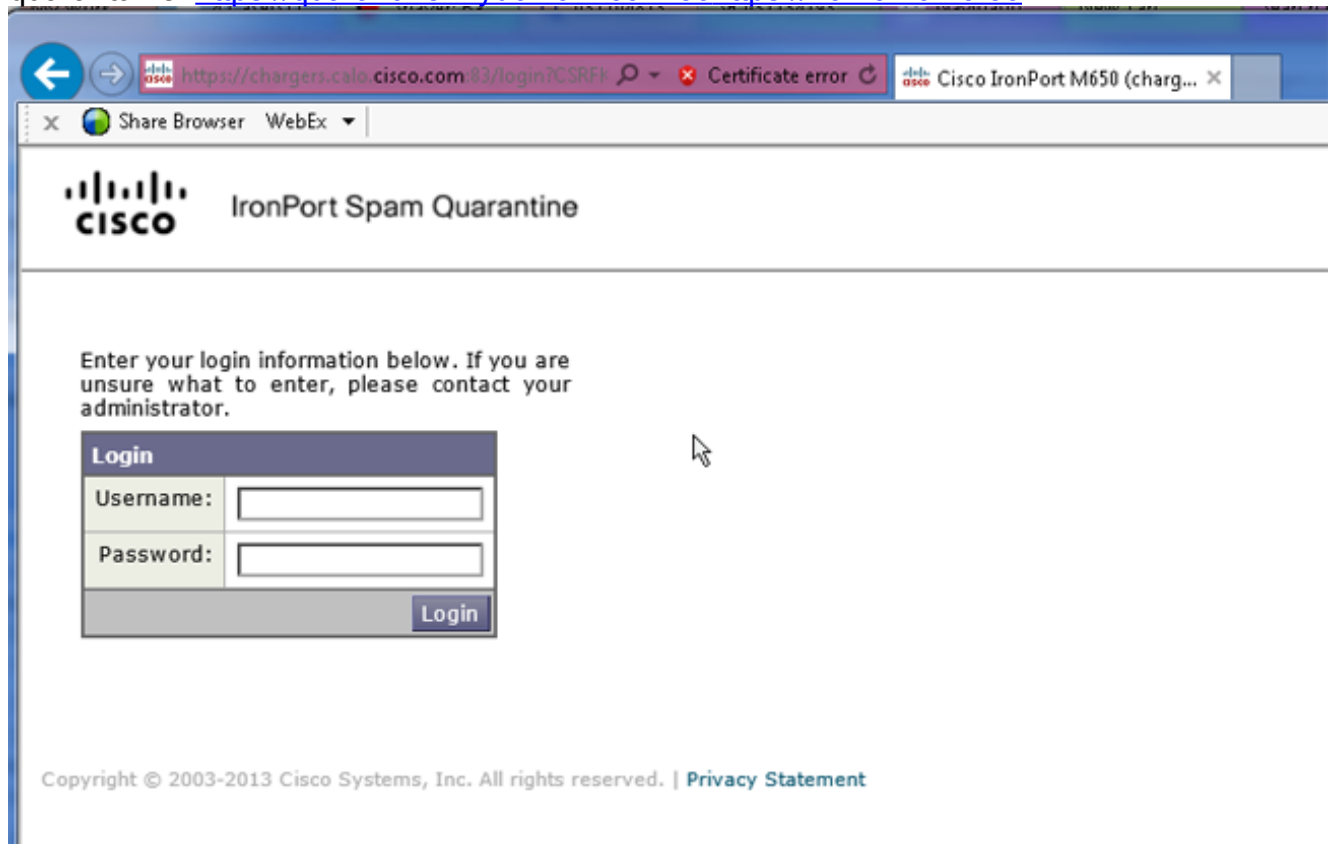
merking: Als u de quarantaine voor externe toegang configureren hebt u een extern IP-adres nodig dat op de interface is geconfigureerd of een extern IP dat een netwerkadres is dat is vertaald in een interne IP. Als u geen hostname gebruikt, kunt u de Hostname-radioknop controleren maar nog steeds alleen via IP-adres toegang tot de quarantaine hebben.

Bijvoorbeeld, <https://10.10.10.10:83>.

5. Breng veranderingen in en begaan.

6. Bevestig. Als u een hostname voor de spamquarantaine specificeert, zorg er dan voor dat de hostname kan worden opgelost via het interne Domain Name System (DNS) of externe DNS. DNS lost de hostname op aan uw IP-adres. Als u geen resultaat hebt, raadpleegt u uw netwerkbeheerder en blijft u toegang tot de quarantaine via IP-adres, zoals in het vorige voorbeeld, totdat de host zich in DNS bevindt. >nslookup quarantine.mydomain.com
Navigeer naar uw URL die eerder in een web browser is ingesteld om te bevestigen dat u toegang hebt tot de

quarantaine: <https://quarantine.mydomain.com:83><https://10.10.10.10:83>



Configureer de ESA om positieve spam te verplaatsen en/of spam te verdenken tot spam quarantaine

Voltooi de volgende stappen om uw verdachte spam-berichten in quarantaine te plaatsen en/of

positief geïdentificeerde spam-berichten te plaatsen:

1. Klik in het ESR op **Mail Policies > Inkomend Mail beleid** en vervolgens op anti-spam kolom voor Default Policy.
2. Wijzig de actie van ofwel de positief geïdentificeerde Spam of verdachte Spam om naar de Spam Quarantine te sturen."

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine ▼ <small>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</small>
Add Text to Subject:	Prepend ▼ [SPAM]
▶ Advanced	Optional settings for custom header and message delivery.

Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Spam Quarantine ▼ <small>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</small>
Add Text to Subject:	Prepend ▼ [SUSPECTED SPAM]
▶ Advanced	Optional settings for custom header and message delivery.

3. Herhaal het proces voor elke andere ESA's die u eventueel hebt ingesteld voor Externe Spam Quarantine. Als u deze verandering op het clusterniveau aanbrengt, hoeft u deze niet te herhalen, aangezien de wijziging wordt voorgesteld aan de andere apparaten in het cluster.
4. Breng veranderingen in en beëindig.
5. Op dit moment wordt post die anders zou zijn afgeleverd of ingetrokken in quarantaine geplaatst.

Externe spamquarantaine instellen op de SMA

De stappen om Externe Spam Quarantine op SMA te configureren zijn dezelfde als de voorgaande sectie met een paar uitzonderingen:

1. Op elk van uw ESA's moet u de lokale quarantaine uitschakelen. Kies **monitor > Quarantines**.
2. Kies op uw ESA, **Security Services > Spam Quarantine** en klik op **Enable Externe Spam Quarantine**.
3. Punt het ESA aan het IP adres van uw SMA en specificeer de haven die u wilt gebruiken. De standaardinstelling is Port 6025.

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable External Spam Quarantine	
Name:	aggies_spam_quarantine <small>(e.g. spam_quarantine)</small>
IP Address:	14.2.30.104
Port:	6025
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature Blocklist Action: Quarantine ▼

Cancel Submit

4. Zorg ervoor dat poort 6025 open is van de ESA naar de SMA. *Deze haven is bestemd voor*

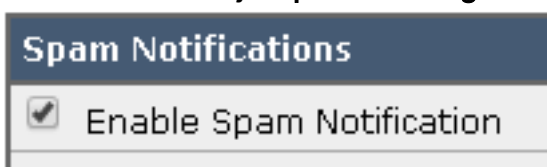
de levering van quarantaine-berichten van ESA > SMA. Dit kan worden gevalideerd met een telnettest van de CLI op de ESA in poort 6025. Als er een verbinding wordt geopend en open blijft, dient u deze in te stellen.

```
tarheel.rtp> telnet 14.2.30.116 6025
Trying 14.2.30.116...
Connected to steelers.rtp.
Escape character is '^]'.
220 steelers.rtp ESMTTP
```

5. Zorg ervoor dat u de IP/hostname hebt ingesteld om toegang te krijgen tot de spamquarantaine, zoals in "Enable Quarantine Ports en Specificeer een Quarantine URL op de interface".
6. Controleer dat er berichten in de spamquarantaine komen van uw ESA's. Als de spamquarantaine geen berichten laat zien, kan er een probleem zijn met connectiviteit van ESA > SMA op poort 6025 (zie voorgaande stappen).

Spam Quarantine-melding instellen

1. Kies in het ESA de optie **Monitor > Spam Quarantine**.
2. In het SMA navigeert u naar de instellingen van de Spam Quarantine om de zelfde stappen uit te voeren.
3. Klik op **Spam Quarantine**.
4. Controleer het vakje **Spam-melding inschakelen**.



5. Kies uw waarschuwing schema.

Notification Schedule:

Monthly (Sent the 1st of each month at 12am)

Weekly (Sent at 12am)

Mon Tue Wed Thu Fri Sat Sun

12 1 2 3 4 5 6 7 8 9 10 11 AM

12 1 2 3 4 5 6 7 8 9 10 11 PM

6. Breng veranderingen in en begraan.

Wachtwoord voor eindgebruiker instellen voor quarantaine-toegang via SPA0000 Quarantine-eindgebruikersverificatie

1. Kies in het SMA of ESA **stysteembeheer > LDAP**.
2. Open uw LDL-serverprofiel.
3. Om te controleren of u met een Active Directory-account kunt authenticeren, controleer dan of de Spam Quarantine End-User Accounting Query is ingeschakeld.
4. Controleer de optie **Aanwijzen als actieve zoekopdracht**.

✓ Spam Quarantine End-User Authentication Query	
Name:	<input type="text" value="myldap.isq_user_auth"/> <input checked="" type="checkbox"/> Designate as the active query
Query String:	<input type="text" value="(uid={u})"/>
Email Attribute(s):	<input type="text" value="mail"/>

5. Klik op **Test** om de query te testen. Overeenkomend Positief betekent dat de echtheidscontrole succesvol was:

Test Query ✕

Spam Quarantine End-User Authentication Query

Query Definition and Attributes*

Query String:

Email Attribute(s):

**These items will be updated when the Update button below is clicked.*

Test Parameters

User Login:

User Password:

Connection Status

Query results for host:192.168.170.101

Query (uid=sbayer) to server myldap (192.168.170.101:389)
email_attributes: [mail] emails: sbayer@cisco.com
Query (uid=sbayer) lookup success, (192.168.170.101:389) returned 1 results
first stage smtp auth succeeded. query: myldap.isq_user_auth results:
['cn=Stephan Bayer,ou=user,dc=sbayer,dc=cisco']
Bind attempt to server myldap (192.168.170.101:389)
BIND (uid=sbayer) returned True result
second stage smtp auth succeeded. query: myldap.isq_user_auth
Success: Action: match positive.

6. Breng veranderingen in en beaan.
7. Kies in het ESA de optie **Monitor > Spam Quarantine**. Navigeer in het SMA naar de instellingen voor Spam Quarantine om dezelfde stappen uit te voeren.
8. Klik op **Spam Quarantine**.
9. Controleer het vakje **Toegang voor eindgebruiker quarantine inschakelen**.
10. Kies **LDAP** uit de vervolgkeuzelijst Eindgebruikersverificatie.

End-User Quarantine Access	
<input checked="" type="checkbox"/> Enable End-User Quarantine Access	
End-User Authentication: ?	LDAP <i>End users will be authenticated against LDAP. Login without credentials can be configured in messages. To configure an End User Authentication...</i>
Hide Message Bodies:	<input type="checkbox"/> Do not display message bodies to end-u

11. Breng veranderingen in en begaan.
12. Bevestig dat Externe Verificatie plaatsvindt via ESA/SMA.
13. Navigeer naar uw URL die eerder in een web browser is ingesteld om te valideren dat u toegang hebt tot de quarantaine: <https://quarantine.mydomain.com:83>
<https://10.10.10.10:83>
14. Meld u aan met uw LDAP-account. Als dit mislukt, controleert u het externe authenticatie LDAP-profiel en schakelt u de toegang tot de eindgebruiker Quarantine in (zie vorige stappen).

Administratieve gebruikerstoegang instellen tot de SPM-quarantaine

Gebruik de procedure in dit gedeelte om administratieve gebruikers met deze rollen toe te staan om berichten in de Spam Quarantine te beheren: Exploitant, alleen-lezen, Help-functie of Guestrollen, en aangepaste gebruikersrollen die toegang tot de Spam-quarantaine omvatten.

Gebruikers op beheerniveau, die de standaardinstelling van de beheerder en gebruikers van de e-mail beheerder gebruiken, kunnen altijd toegang krijgen tot de Spam Quarantine en hoeven met deze procedure niet gekoppeld te worden aan de Spam Quarantine-functie.

Opmerking: Gebruikers op het niveau van de niet-beheerder kunnen berichten in de quarantaine openen maar ze kunnen de quarantaine-instellingen niet bewerken. Gebruikers op administratieniveau kunnen meldingen benaderen en de instellingen bewerken.

Voltooi de volgende stappen om beheergebruikers die geen volledige Administrator-rechten hebben, in staat te stellen om meldingen in de Spam Quarantine te beheren:

1. Zorg ervoor dat u gebruikers hebt gemaakt en hen een gebruikersrol met toegang tot de Spam Quarantine toegewezen.
2. Kies in het Security Management-apparaat **applicatie > Gecentraliseerde services > Spam Quarantine**.
3. Klik op **Instellingen inschakelen of bewerken** in het gedeelte Wachtwoord quarantaine-instellingen.
4. In het gedeelte Administratieve gebruikers van het gedeelte Wachtwoord quarantaine-instellingen klikt u op de selectieknop voor lokale gebruikers, extern gewaarmerkte gebruikers of aangepaste gebruikersrollen.
5. Kies de gebruikers aan wie u toegang wilt verlenen tot weergave en beheer van berichten in de Spam Quarantine.

6. Klik op **OK**.
7. Herhaal indien nodig voor elk van de andere types van Administratieve Gebruikers die in de sectie vermeld worden (Lokale gebruikers, Extern gewaarmerkte gebruikers, of Aangepaste gebruikersrollen).
8. Indienen en je wijzigingen begaan.