

Eメールセキュリティ アプライアンス (ESA) およびセキュリティ管理アプライアンス (SMA) における包括的なスパム検疫設定ガイド

目次

[概要](#)

[手順](#)

[設定 ESA のローカル スパム検疫](#)

[検疫ポートを有効にし、インターフェイスで検疫 URL を規定して下さい](#)

[肯定的なスパムや容疑者スパムを検疫を無差別に送信するために移動するように ESA を設定して下さい](#)

[SMA の外部スパム検疫を設定して下さい](#)

[スパム検疫通知を設定して下さい](#)

[スパム検疫エンドユーザ 認証クエリによってエンドユーザ スパム検疫アクセスを設定して下さい](#)

[スパム検疫に管理上のユーザアクセスを設定して下さい](#)

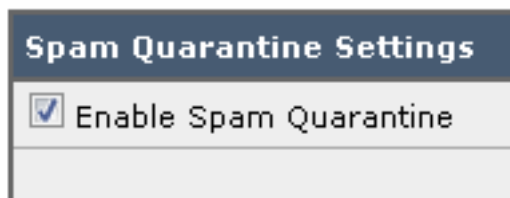
概要

この資料に ESA のスパム検疫をか SMA および関連する機能設定する方法を記述されています:
LDAP およびスパム検疫通知の外部認証。

手順

設定 ESA のローカル スパム検疫

1. ESA で、> **スパム検疫** 『Monitor』 を選択して下さい。
2. スパム検疫では設定は区分し、**イネーブル スパム検疫** チェックボックスをチェックし、望ましい検疫設定を行いました。



3. サービス > **スパム検疫** を 『Security』 を選択して下さい。
4. 外部スパム検疫を使用するために計画しなかったら、**外部スパム検疫** チェックボックスがチェックを外されるイネーブルを確認して下さい (下記の例を参照して下さい)。

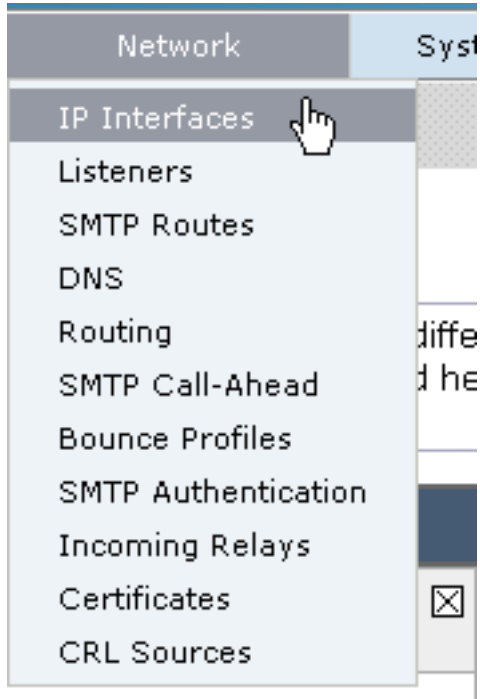
External Spam Quarantine Settings

Enable External Spam Quarantine

5. 変更を送信し、保存します。

検疫ポートを有効にし、インターフェイスで検疫 URL を規定して下さい

1. ネットワーク > IP インターフェイスを選択して下さい。



2. 検疫にアクセスするために使用するインターフェイスのインターフェイス名をクリックして下さい。スパム検疫セクションでは、チェックボックスをチェックし、デフォルトポートを規定するか、または要求に応じて変更して下さい: 検疫 HTTP を無差別に送信して下さい
検疫 HTTPS を無差別に送信して下さい

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

3. これですパム検疫チェックボックスのためのデフォルト インターフェイス チェックして下さい。

4. 「通知で」表示する URL の下でデフォルトでアプライアンスはシステム ホスト名 (cli を使用します: 第 2 オプション ボタン オプションおよびテキスト フィールドの `sethostname`) 他に特に規定がなければ。この例はデフォルトホスト名設定を規定したも

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/)

のです。スパム
 検疫にアクセスするためにカスタム URL を規定できます。

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

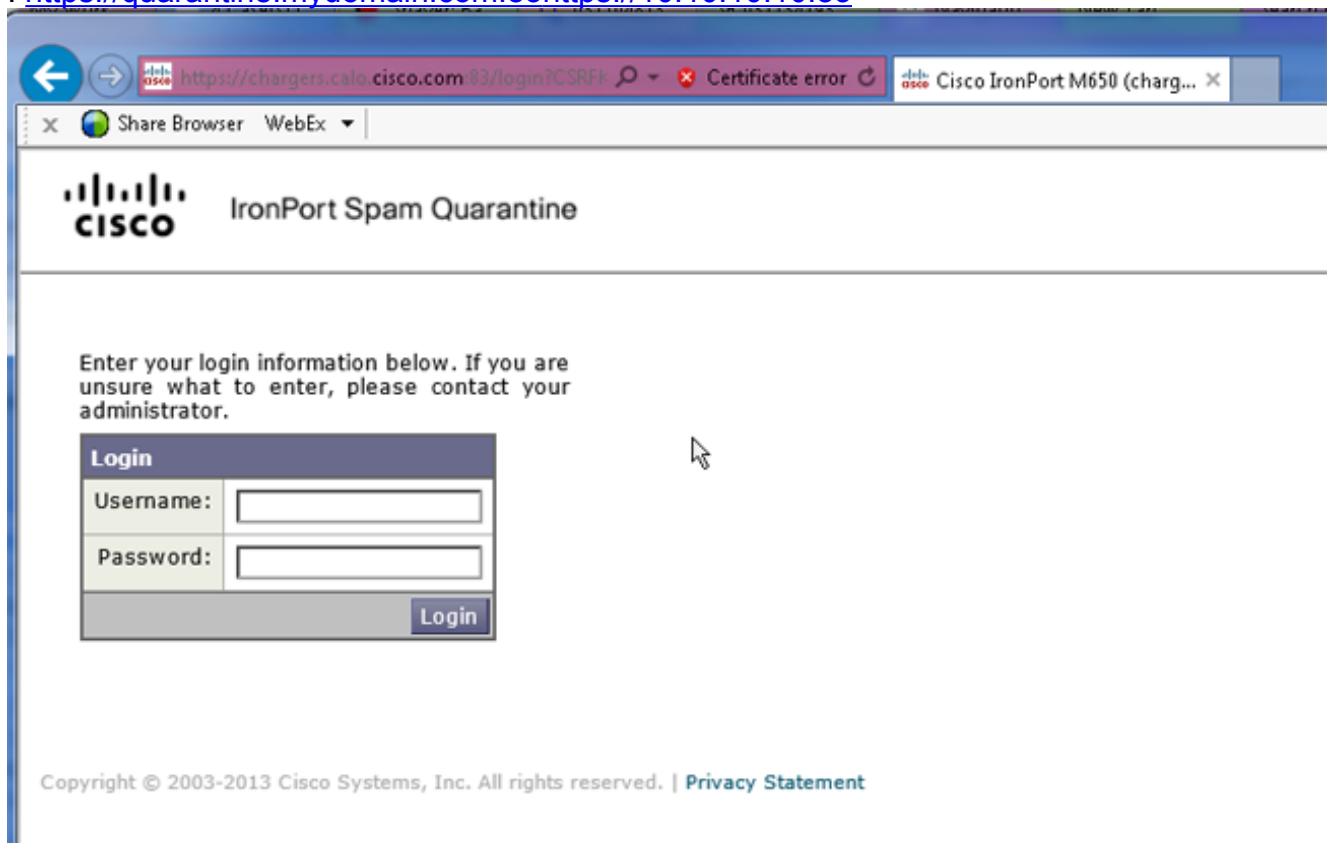
Hostname

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

注: 外部アクセ

スのための検疫を設定する場合、変換される内部 IP へのネットワークアドレスである外部 IP インターフェイスで設定された外部 IP アドレスを必要とします。ホスト名を使用しなければ-ホスト名オプション ボタンをチェックしておくことができますがまだ IP アドレスだけによって検疫にアクセスします。たとえば、<https://10.10.10.10:83>。

5. 変更を送信し、保存します。
6. 検証します。スパム検疫のためのホスト名を規定する場合、ホスト名をです内部 Domain Name System (DNS) か外部 DNS によって解決可能確認して下さい。DNS は IP アドレスにホスト名を解決します。結果を得ない場合、ネットワーク管理者とチェックし、ホストが DNS に出て来るまで前例のような IP アドレスによって検疫にアクセスし続けて下さい。
 >nslookup quarantine.mydomain.com検疫にアクセスできること検証するために Webブラウザで前もって設定される URL にナビゲートして下さい
 : <https://quarantine.mydomain.com:83><https://10.10.10.10:83>



肯定的なスパムや容疑者スパムを検疫を無差別に送信するために移動するように ESA を設定して下さい

疑わしいスパムや肯定的に識別されたスパム メッセージを検疫するために、これらのステップを完了して下さい:

1. 次に ESA で、メール「Policies」> デフォルトポリシーのための着信メール「Policies」および反スパム カラムをクリックして下さい。
2. 変更して下さいスパム検疫に送信 する肯定的に識別されたスパムまたは容疑者スパムの操作を」。

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. 外部スパム検疫のために設定するかもしれない他のどの ESA のためのプロセスも繰り返して下さい。 クラスタの他のアプライアンスへの変更が propogated のでクラスタでこの変更 に水平にそれを繰り返す必要がないために。
4. 変更を送信し、保存します。
5. この時点で、別の方法で渡されるか、または廃棄されたメールは検疫されて得ます。

設定 SMA の外部スパム検疫

SMA の外部スパム検疫を設定するステップは少数の例外を除く前のセクションと同じです:

1. ESA のそれぞれで、ローカル検疫をディセーブルにする必要があります。 > 検疫 『Monitor』 を選択して下さい。
2. ESA で、サービス>スパム検疫を『Security』 を選択し、外部スパム検疫を『Enable』 をクリックして下さい。
3. ESA を SMA の IP アドレスを指し、使用するために望むポートを規定して下さい。 デフォルトはポート 6025 です。

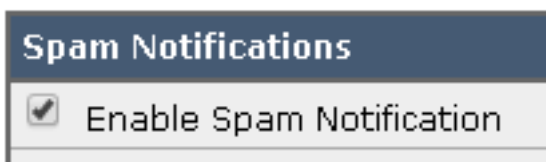
External Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable External Spam Quarantine	
Name:	aggies_spam_quarantine <small>(e.g. spam_quarantine)</small>
IP Address:	14.2.30.104
Port:	6025
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature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

Cancel Submit

- ポート 6025 を ESA から SMA に開いています確認して下さい。このポートは検疫されたメッセージの配信のためからの ESA > SMA です。これはポート 6025 の ESA の CLI からの telnet テストでによって検証することができます。接続がおよび開けば開いた滞在設定する必要があります。tarheel.rtp> telnet 14.2.30.116 6025
Trying 14.2.30.116...
Connected to steelers.rtp.
Escape character is '^]'.
220 steelers.rtp ESMTTP
- 「イネーブル検疫ポートののようなスパム検疫に、アクセスし、インターフェイスで検疫 URL を」規定するために設定しました IP/hostname を-確認して下さい。
- メッセージが ESA からのスパム検疫に着くことを確認して下さい。スパム検疫がメッセージを表示しない場合、ESA > ポート 6025 の SMA 接続においての問題がからのあるかもしれませぬ (前の手順を参照して下さい) 。

スパム検疫通知を設定して下さい

- ESA で、> スパム検疫 『Monitor』 を選択して下さい。
- 同じステップを実行するために SMA でスパム検疫設定にナビゲート します。
- スパム検疫をクリックして下さい。
- イネーブル スパム 通知 チェックボックスをチェックして下さい。



- 通知スケジュールを選択して下さい。

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

- 変更を送信し、保存します。

スパム検疫エンドユーザ 認証クエリによってエンドユーザ スパム検疫アクセスを設定して下さい

- SMA か ESA で、システム 管理 > LDAP を選択して下さい。
- LDAPサーバ プロファイルを開いて下さい。
- 確認するためにアクティブ ディレクトリ アカウントと認証ことチェックしますスパム検疫 エンドユーザをできて下さい認証クエリが有効になる。
- アクティブな Query チェックボックスとして指定をチェックして下さい。

✓ 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. クエリをテストするために『Test』をクリックして下さい。認証が正常だったことを肯定的意味します一致する

:

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. 変更を送信し、保存します。
7. ESA で、> **スパム検疫** 『Monitor』 を選択して下さい。 SMA で、同じステップを実行するためにスパム検疫設定にナビゲートして下さい。
8. **スパム検疫** をクリックして下さい。
9. **イネーブル エンドユーザ検疫アクセスチェック** チェック ボックスをチェックして下さい。
10. エンドユーザ 認証 ドロップダウン リストから **LDAP** を選択して下さい。

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 messages. To configure an End User Authentication...</i>
Hide Message Bodies:	<input type="checkbox"/> Do not display message bodies to end-u

- 変更を送信し、保存します。
- 外部認証が ESA/SMA にあること検証して下さい。
- 検疫にアクセスできること検証するために Webブラウザで前もって設定される URL にナビゲートして下さい: <https://quarantine.mydomain.com:83>
<https://10.10.10.10:83>
- LDAP アカウントのログイン。これが失敗した場合、外部認証 LDAP プロファイルをチェックし、エンドユーザ検疫アクセスをイネーブルにして下さい (前の手順を参照して下さい)。

スパム検疫に管理上のユーザアクセスを設定して下さい

これらのロールの管理上のユーザをスパム検疫のメッセージを管理することを許可するためにこのセクションでプロシージャを使用して下さい: オペレータ、読み取り専用オペレータ、ヘルプデスク、または Guestroles およびスパム検疫にアクセスを含むカスタム ユーザの役割。

デフォルト管理者ユーザが含まれ、管理者ユーザを E-メールを送る管理者レベル ユーザはスパム検疫に常にアクセスでき、このプロシージャを使用してスパム検疫機能と関連付けられる必要はありません。

注: 非管理者レベル ユーザはスパム検疫のメッセージにアクセスできますが検疫設定を編集できません。管理者レベル ユーザはメッセージにアクセスし、設定を編集できます。

スパムのメッセージを管理する完全なアドミニストレーター特権がない管理上のユーザを有効にするためにこれらのステップを検疫して下さい、完了して下さい:

- ユーザを作成し、スパム検疫にアクセスとそれらにユーザの役割を割り当てるために確かめて下さい。
- セキュリティ マネジメント アプライアンスで、**管理 アプライアンス > 中央 集中型 サービス > スパム検疫**を選択して下さい。
- スパム検疫設定セクションの**設定**を『Enable』をクリックするか、または編集して下さい。
- スパム検疫設定の管理上の利用者域ではローカルユーザ、外部に 認証済みユーザ、またはカスタム ユーザの役割への選択リンクを区分して下さい、クリックして下さい。
- 対するアクセス権の付与に表示したいと思い、スパムのメッセージを管理するために検疫しなさいユーザを選択して下さい。
- [OK] をクリックします。
- セクション (ローカルユーザ、外部に 認証済みユーザ、かカスタム ユーザの役割) にもし

必要なら繰り返して下さい。リストされている管理上のユーザの他の型のそれぞれのために
8. 変更を送信し、確定します。