

Всестороннее карантинное руководство по установке спама на Email Security Appliance (ESA) и устройстве управления безопасностью (SMA)

Содержание

[Введение](#)

[Процедура](#)

[Настройте локальный карантин спама на ESA](#)

[Включите карантинные порты и задайте карантинный URL в интерфейсе](#)

[Настройте ESA для Перемещения Положительного Спама Спама и/или Подозреваемого для Спама Карантина](#)

[Настройте внешний карантин спама на SMA](#)

[Настройте карантинное уведомление спама](#)

[Настройте Карантинный Доступ Спама Конечного пользователя через Карантинный Запрос Аутентификации Конечного пользователя Спама](#)

[Настройте доступ административного пользователя к карантину спама](#)

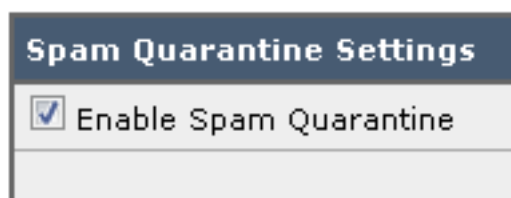
Введение

Этот документ описывает, как настроить карантин спама на ESA или SMA и привязанных функциях: внешняя проверка подлинности с LDAP и спамом изолирует уведомление.

Процедура


Настройте локальный карантин спама на ESA

1. На ESA выберите **Monitor> Spam Quarantine**.
2. В Карантинном разделе Параметров настройки Спама проверьте флажок **Enable Spam Quarantine** и установите желаемые карантинные параметры настройки.



3. Выберите **Security Services> Spam Quarantine**.
4. Гарантируйте, что флажок **Enable External Spam Quarantine** неконтролируем, пока вы не планируете использовать Внешний Карантин Спама (см. раздел ниже).

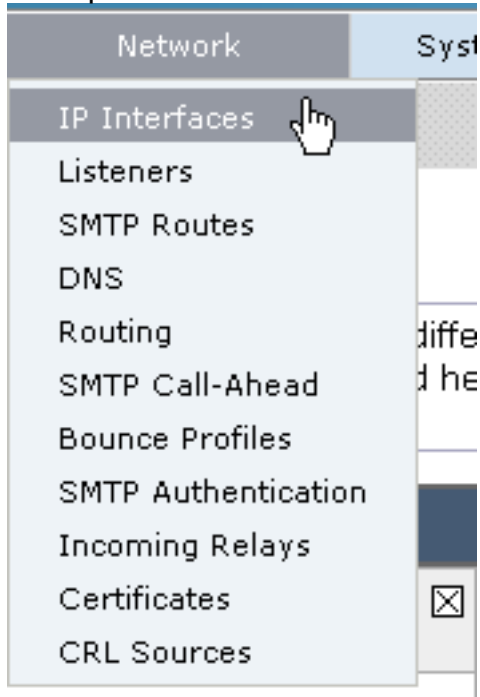
External Spam Quarantine Settings

 **Enable External Spam Quarantine**

5. Отправьте и передайте изменения.

Включите карантинные порты и задайте карантинный URL в интерфейсе

1. Выберите **Network > IP Interfaces**.



2. Нажмите имя интерфейса интерфейса, который вы будете использовать для доступа к карантину. В карантинном разделе спама проверьте флажки и задайте порты по умолчанию или изменение как требуется: Карантинный HTTP спама Карантинный HTTPS спама

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

3. Проверьте, что Это является интерфейсом по умолчанию для флажка **Spam Quarantine**.

4. Под "URL, Отображенным в Уведомлениях", по умолчанию устройство использует системное имя хоста (cli: **sethostname**), пока иначе не задано во втором параметре переключателей и текстовом поле. Данный пример задает значение имени хоста по

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/)

умолчанию.

Мо

жно задать пользовательский URL для доступа к Карантину

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/)

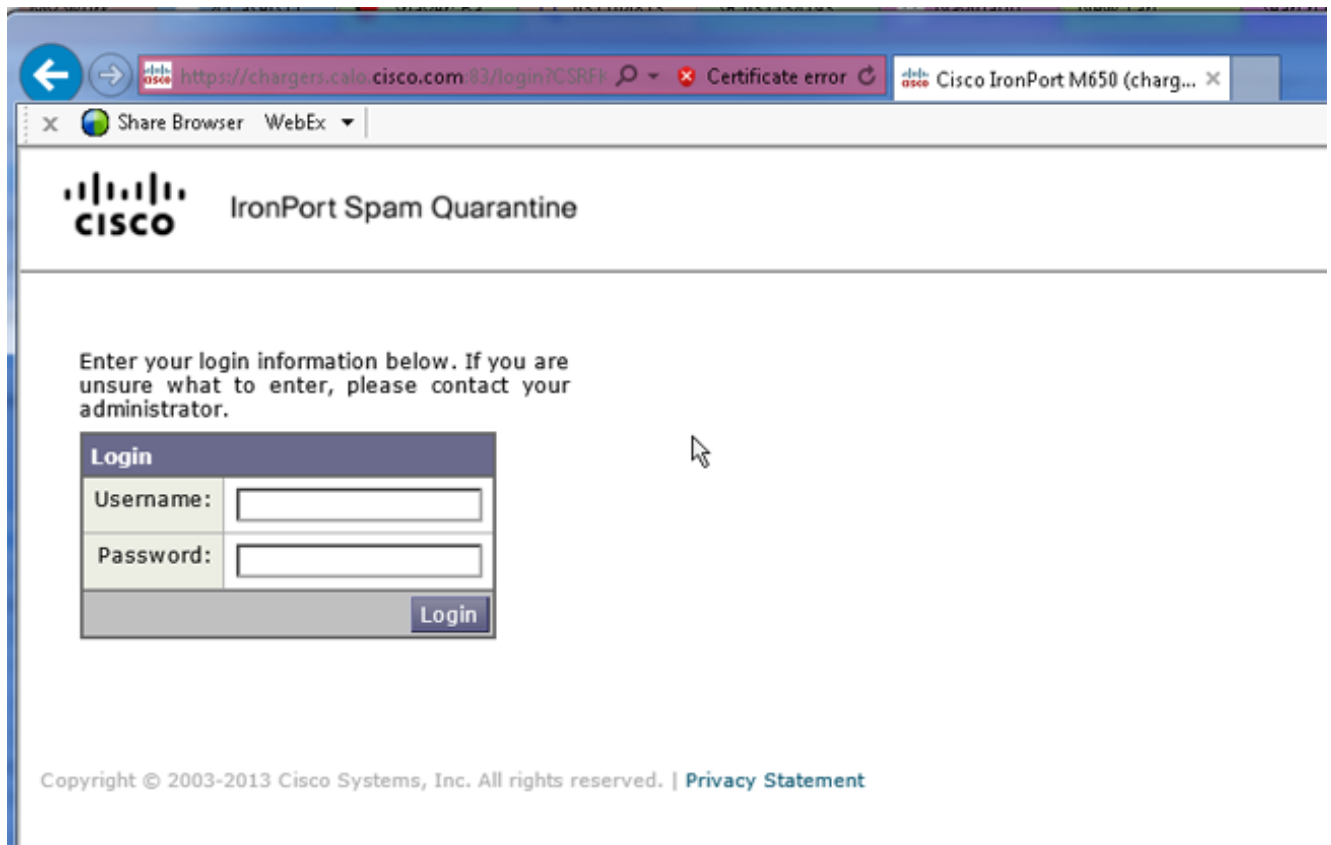
Спама.

Приме

чание: При настройке карантина на внешний доступ вам будет нужен внешний IP - адрес, настроенный на интерфейсе или внешнем IP, который является Сетевым адресом, Преобразованным во внутреннего IP. Если вы не используете имя хоста, можно поддержать кнопку с зависимой фиксацией Hostname проверенной, но все еще обратиться к карантину IP-адресом только. Например, <https://10.10.10.10:83>.

5. Отправьте и передайте изменения.

6. Проверить. Если вы задаете имя хоста для карантина спама, гарантируете, что имя хоста разрешимо через внутреннюю Систему доменных имен (DNS) или внешний DNS. DNS решит имя хоста к вашему IP-адресу. Если вы не получаете результат, сверяйтесь с вашим Администратором сети и продолжаете обращаться к Карантину IP-адресом как предыдущий пример, пока хост не обнаруживается в DNS. >nslookup quarantine.mydomain.com
 Перейдите к своему URL, настроенному ранее в web-браузере, чтобы проверить, что можно обратиться к карантину: <https://карантин.mydomain.com:83>
<https://10.10.10.10:83>



Настройте ESA для Перемещения Положительного Спам Спам и/или Подозреваемого для Спам Карантина

Для изоляции Подозрительного Спам и/или Положительно Определенных сообщений Спам, выполните эти шаги:

1. На ESA нажмите **Mail Policies > Incoming Mail Policies** и затем столбец для защиты от спама для Политики по умолчанию.
2. Измените действие или Положительно Определенного Спам Спам или Подозреваемого для передачи к Карантину Спам."

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. Повторите процесс для любых других ESA, которые вы, возможно, настроили для Внешнего Карантина Спам. При внесении этого изменения на кластерном уровне, вы не должны будете повторять его, поскольку изменение будет prorogated к другим устройствам в кластере.
4. Отправьте и передайте изменения.
5. На этом этапе почта, которая была бы иначе отправлена или отброшена, будет

изолирована.

Настройте внешний карантин спама на SMA

Шаги для настройки Внешнего Карантина Спама на SMA совпадают с предыдущим разделом за немногим исключением:

1. На каждом из ваших ESA необходимо будет отключить локальный карантин. Выберите **Monitor> Quarantines**.
2. На вашем ESA выберите **Security Services> Spam Quarantine** и нажмите **Enable External Spam Quarantine**.
3. Укажите ESA к IP-адресу вашего SMA и задайте порт, который требуется использовать. По умолчанию является портом 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

4. Гарантируйте, что порт 6025 открыт от ESA до SMA. *Этот порт для предоставления изолированных сообщений от ESA> SMA. Это может быть проверено с тестом telnet от CLI на ESA на порту 6025. Если соединение открывается и остается открытым, вы должны быть установлены.*

```
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. Гарантируйте настройку IP/имени хоста для доступа к карантину спама, такой, поскольку во "Включают Карантинные порты и Задают Карантинный URL в Интерфейсе".
6. Проверьте, что сообщения поступают в карантин спама от ваших ESA. Если карантин спама не показывает сообщений, могла бы быть проблема с подключением от ESA> SMA на порту 6025 (см. предыдущие шаги).

Настройте карантинное уведомление спама

1. На ESA выберите **Monitor> Spam Quarantine**.
2. На SMA вы перешли бы к Карантинным параметрам настройки Спама для выполнения тех же шагов.
3. Нажмите **Spam Quarantine**.
4. Проверьте флажок **Enable Spam Notification**.

Spam Notifications

Enable Spam Notification

5. Выберите свое уведомление Список.

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. Отправьте и передайте изменения.

Настройте Карантинный Доступ Слама Конечного пользователя через Карантинный Запрос Аутентификации Конечного пользователя Слама

1. На SMA или ESA, выберите **System Administration > LDAP**.
2. Откройте свой Профиль Сервера LDAP.
3. Чтобы проверить, что вы в состоянии аутентифицироваться с Учетной записью Active Directory, проверить, что включен ваш Карантинный Запрос Аутентификации Конечного пользователя Слама.
4. Проверьте **Определение как флажок Active Query**.

<input checked="" type="checkbox"/> 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. Нажмите **Test** для тестирования запроса. Совпадение Положительный, означает, что аутентификация была успешна:

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. Отправьте и передайте изменения.
7. На ESA выберите **Monitor> Spam Quarantine**. На SMA перейдите к Карантинным параметрам настройки Спاما для выполнения тех же шагов.
8. Нажмите **Spam Quarantine**.
9. Установите **Разрешать Карантинный флажок Проверки доступа Конечного пользователя**.
10. Выберите **LDAP** из выпадающего списка Аутентификации Конечного пользователя.

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-user

11. Отправьте и передайте изменения.
12. Проверьте ту Внешнюю проверку подлинности, находится на ESA/SMA.
13. Перейдите к своему URL, настроенному ранее в web-браузере, чтобы проверить, что можно обратиться к карантину: <https://карантин.mydomain.com:83>
<https://10.10.10.10:83>
14. Войдите со своей учетной записью LDAP. Если это отказывает, проверьте, что LDAP Внешней проверки подлинности представляет и включает Карантинный Доступ Конечного пользователя (см. предыдущие шаги).

Настройте доступ административного пользователя к карантину спама

Используйте процедуру в этом разделе, чтобы позволить административным пользователям с этими ролями управлять сообщениями в Карантине Спам: Оператор, Оператор Только для чтения, Справочный стол, или Guestroles и пользовательские роли пользователя, которые включают доступ к Карантину Спам.

Пользователи уровня администратора, среди которых пользователь с правами администратора по умолчанию и Почтовые Администраторы, могут всегда обращаться к Карантину Спам и не должны привязываться к Карантинной функции Спам с помощью этой процедуры.

Примечание: Пользователи неуровня администратора могут обратиться к сообщениям в Карантине Спам, но они не могут отредактировать карантинные параметры настройки. Пользователи уровня администратора могут обратиться к сообщениям и отредактировать параметры настройки.

Чтобы включить административным пользователям, которые не имеют прав полного администратора для управления сообщениями в Карантине Спам, выполняют эти шаги:

1. Удостоверьтесь, что вы создали пользователей и назначили их роль пользователя с доступом к Карантину Спам.
2. На устройстве Управления системой безопасности выберите **Management Appliance> Centralized Services> Spam Quarantine**.
3. Нажмите **Enable** или **Edit Settings** в Карантинном разделе Параметров настройки Спам.
4. В области Administrative Users Карантинного раздела Параметров настройки Спам щелкните по ссылке выбора для Локальных пользователей, Внешне Проверенных пользователей или Пользовательских Ролей пользователя.

5. Выберите пользователей, которым вы хотите предоставить доступ, чтобы просмотреть и управлять сообщениями в Карантине Спам.
6. **Нажмите кнопку ОК.**
7. Повторитесь в случае необходимости для каждого из других типов Административных пользователей, перечисленных в разделе (Локальные пользователи, Внешне Проверенные пользователи или Пользовательские Роли пользователя).
8. Отправьте и передайте свои изменения.