Guide complet de configuration de la quarantaine du spam sur l'appliance de sécurité de la messagerie (ESA) et l'appliance de gestion de la sécurité (SMA)

Table des matières

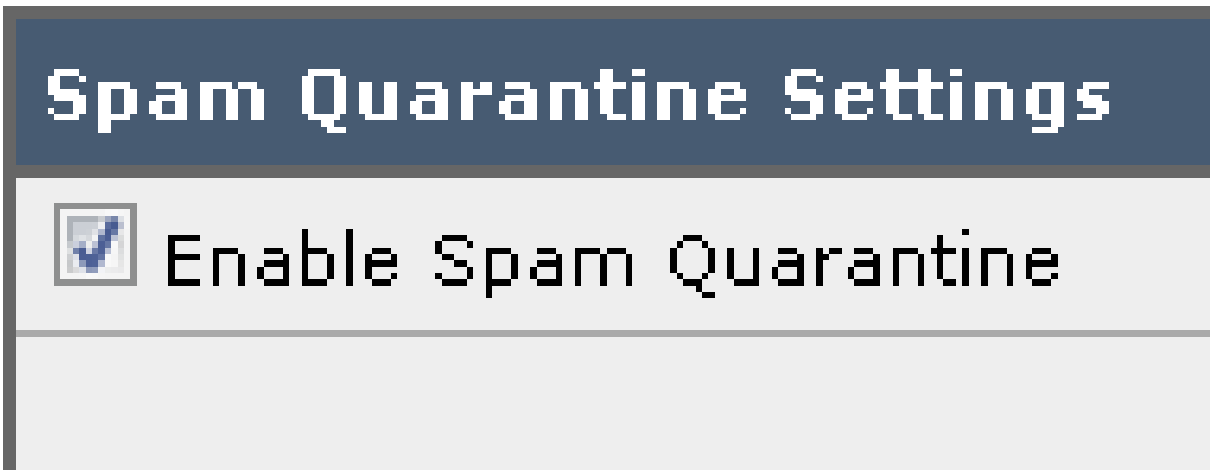
Introduction

Ce document décrit comment configurer la quarantaine du spam sur l'ESA ou SMA et les fonctionnalités associées : authentification externe avec LDAP et notification de quarantaine du spam.

Procédure

Configurer la quarantaine locale du spam sur l'ESA

1. Sur l'ESA, choisissez Monitor > Spam Quarantine.
2. Dans la section Paramètres de quarantaine du spam, cochez la case Activer la quarantaine du spam et définissez les paramètres de quarantaine souhaités.

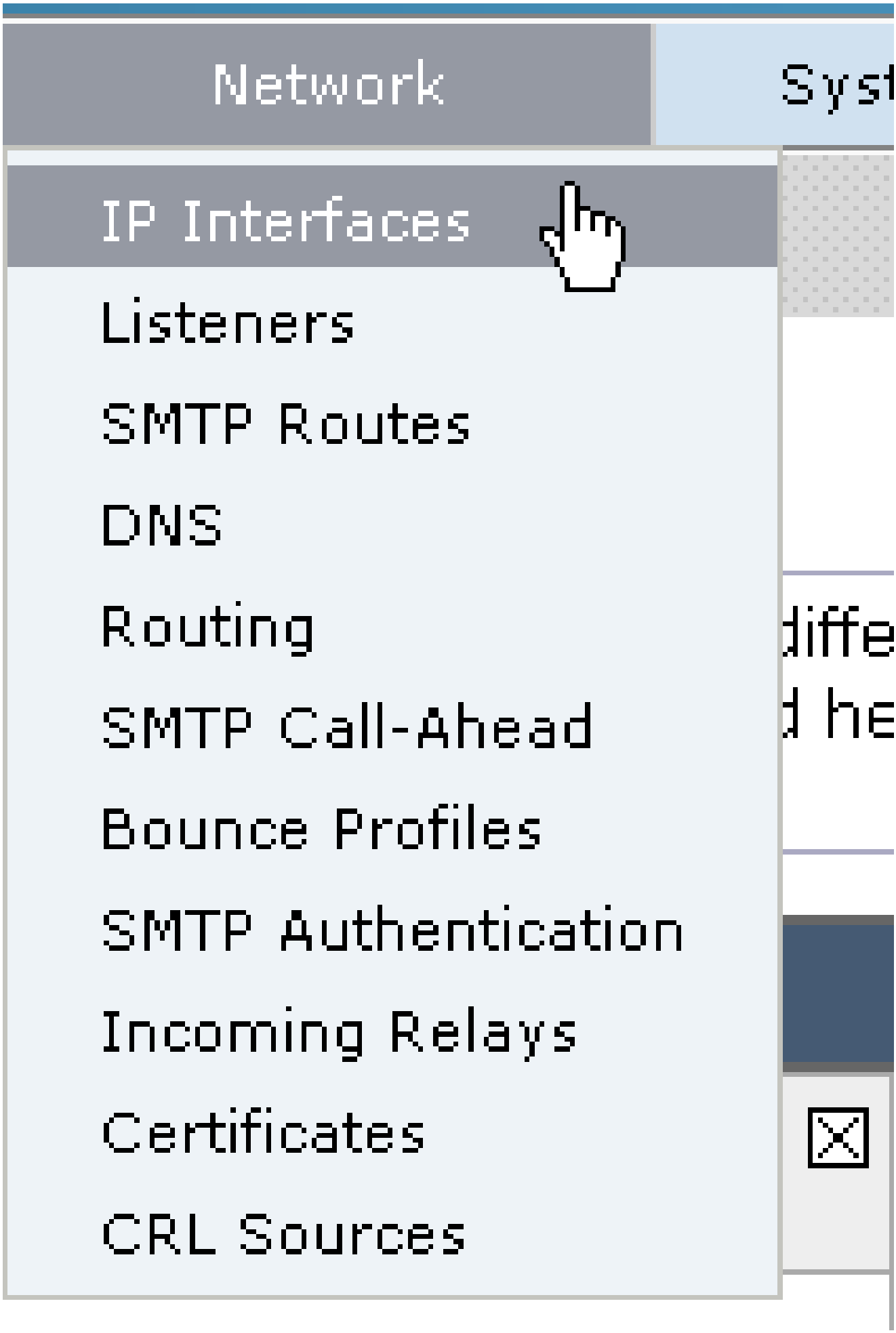


3. Choisissez Security Services > Spam Quarantine.
4. Assurez-vous que la case Enable External Spam Quarantine est décochée, sauf si vous prévoyez d'utiliser External Spam Quarantine (voir la section ci-dessous).

5. Soumettre et valider les modifications.

Activer les ports de quarantaine et spécifier une URL de quarantaine au niveau de l'interface

1. Choisissez Network > IP Interfaces.


Network
Syst
IP Interfaces
Listeners
SMTP Routes
DNS
Routing
SMTP Call-Ahead
Bounce Profiles
SMTP Authentication
Incoming Relays
Certificates
CRL Sources
diffe
d he

2. Cliquez sur le nom de l'interface que vous allez utiliser pour accéder à la quarantaine.

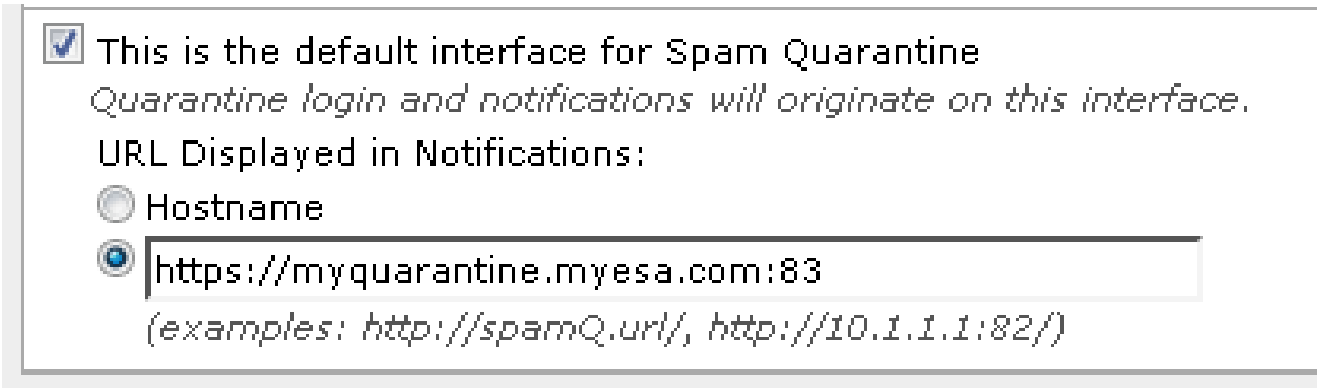
   Dans la section quarantaine du spam, cochez les cases et spécifiez les ports par défaut ou modifiez-les si nécessaire :

   - Quarantaine du spam HTTP
   - Quarantaine du spam HTTPS

3. Cochez la case Ceci est l'interface par défaut pour la quarantaine du spam.
4. Sous « URL affichée dans les notifications », par défaut, l'appliance utilise le nom d'hôte système (cli: sethostname) sauf indication contraire dans la deuxième case d'option et le champ de texte.

   Cet exemple spécifie le paramètre de nom d'hôte par défaut.

   Vous pouvez spécifier une URL personnalisée afin d'accéder à votre quarantaine du spam.



Remarque : si vous configurez la quarantaine pour l'accès externe, vous aurez besoin d'une adresse IP externe configurée sur l'interface ou d'une adresse IP externe qui est une adresse réseau traduite en une adresse IP interne.

Si vous n'utilisez pas de nom d'hôte, vous pouvez conserver la case d'option Nom d'hôte cochée, mais accéder à la quarantaine uniquement par adresse IP. Par exemple,

https://10.10.10.10:83.

5. Soumettre et valider les modifications.
6. Valider.

Si vous spécifiez un nom d'hôte pour la quarantaine du spam, assurez-vous que le nom d'hôte peut être résolu via le système de noms de domaine (DNS) interne ou externe. Le service DNS convertit le nom d'hôte en votre adresse IP.

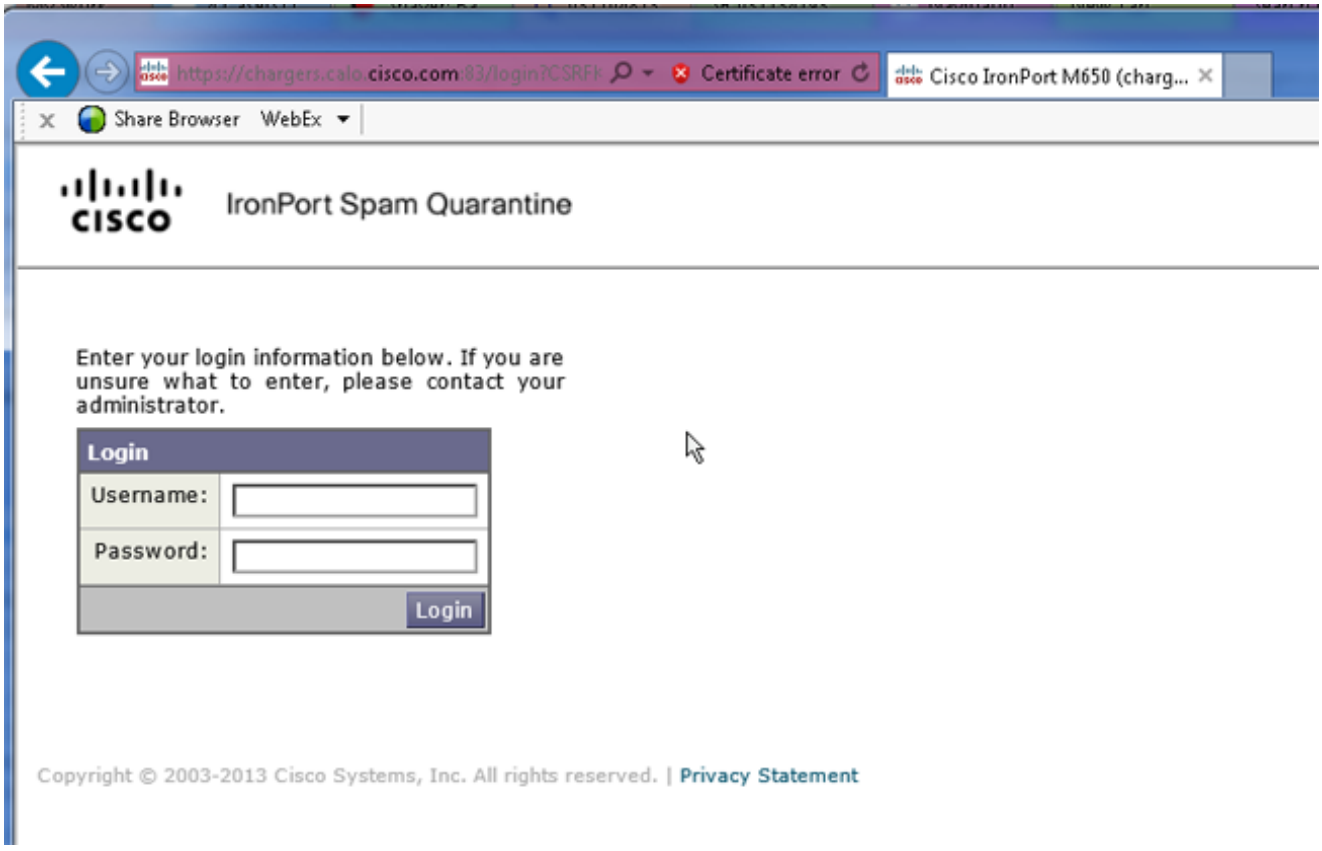
Si vous n'obtenez pas de résultat, vérifiez auprès de votre administrateur réseau et continuez à accéder à la quarantaine par adresse IP comme dans l'exemple précédent jusqu'à ce que l'hôte apparaisse dans le DNS.

> nslookup quarantine.mydomain.com

Accédez à votre URL configurée précédemment dans un navigateur Web afin de valider que vous pouvez accéder à la quarantaine :

https://quarantine.mydomain.com:83

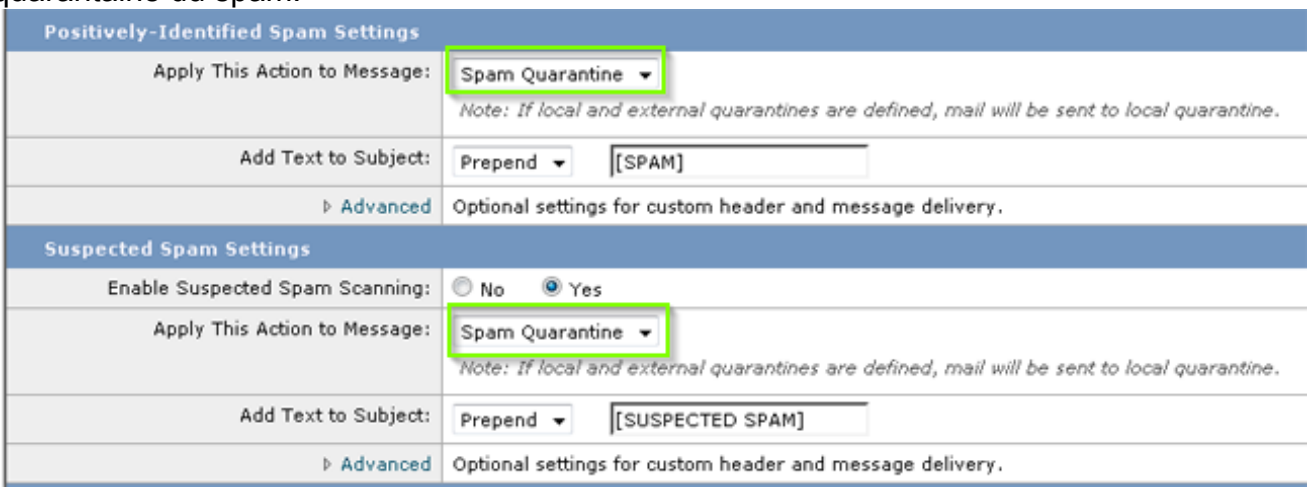
https://10.10.10.10:83



Configurer ESA pour placer le spam positif et/ou le spam suspecté en quarantaine du spam

Afin de mettre en quarantaine vos messages de spam suspecté et/ou de spam identifié positivement, procédez comme suit :

1. Sur l'ESA, cliquez sur Politiques de messagerie > Politiques de messages entrants, puis sur la colonne anti-spam pour la Stratégie par défaut.
2. Modifier l'action du spam identifié positivement ou du spam suspecté à envoyer à la quarantaine du spam."



3. Répétez le processus pour tous les autres ESA que vous avez configurés pour la quarantaine du spam externe. Si vous avez effectué cette modification au niveau de la grappe, vous n'aurez pas à la répéter car elle sera propagée aux autres appliances de la grappe.
4. Soumettre et valider les modifications.
5. À ce stade, les messages qui auraient autrement été remis ou abandonnés sont mis en quarantaine.

Configurer la quarantaine du spam externe sur le SMA

Les étapes de configuration de la quarantaine du spam externe sur le SMA sont les mêmes que dans la section précédente, à quelques exceptions près :

1. Sur chacun de vos ESA, vous devez désactiver la quarantaine locale. Choisissez Monitor > Quarantines.
2. Sur votre ESA, choisissez Security Services > Spam Quarantine et cliquez sur Enable External Spam Quarantine.
3. Pointez l'ESA vers l'adresse IP de votre SMA et spécifiez le port que vous souhaitez utiliser. La valeur par défaut est Port 6025.

4. Assurez-vous que le port 6025 est ouvert du ESA au SMA. Ce port est destiné à la remise

des messages mis en quarantaine depuis ESA > SMA.

Cela peut être validé par un test Telnet à partir de l'interface de ligne de commande sur le ESA sur le port 6025. Si une connexion s'ouvre et reste ouverte, vous devez la définir.

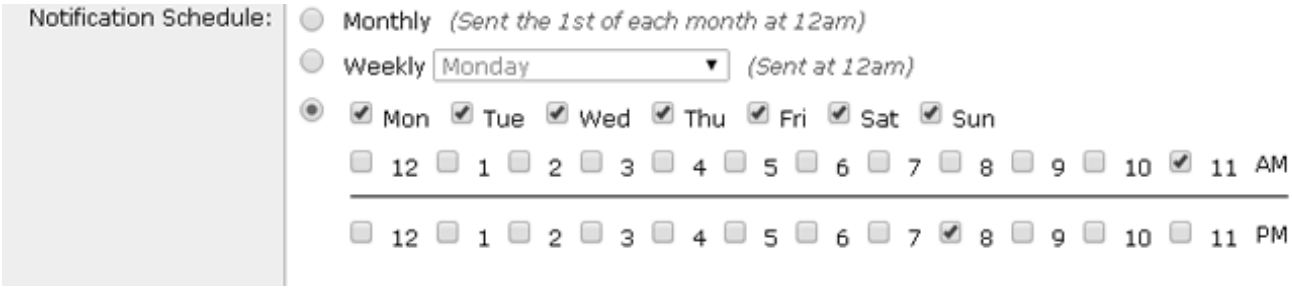
```
tarheel.rtp> telnet 14.2.30.116 6025
Trying 14.2.30.116...
Connected to steelers.rtp.
Escape character is '^]'.
220 steelers.rtp ESMTP
```

5. Vérifiez que vous avez configuré le nom d'hôte/IP pour accéder à la quarantaine du spam, comme dans « Activer les ports de quarantaine et spécifier une URL de quarantaine au niveau de l'interface ».
6. Vérifiez que les messages arrivent dans la quarantaine du spam à partir de vos ESA. Si la quarantaine du spam n'affiche aucun message, il peut y avoir un problème de connectivité de ESA > SMA sur le port 6025 (voir les étapes précédentes).

Configurer la notification de quarantaine du spam

1. Sur l'ESA, choisissez Monitor > Spam Quarantine.
2. Sur le SMA, vous accédez aux paramètres de quarantaine du spam afin d'effectuer les mêmes étapes.
3. Cliquez sur Quarantaine du spam.
4. Cochez la case Enable Spam Notification.

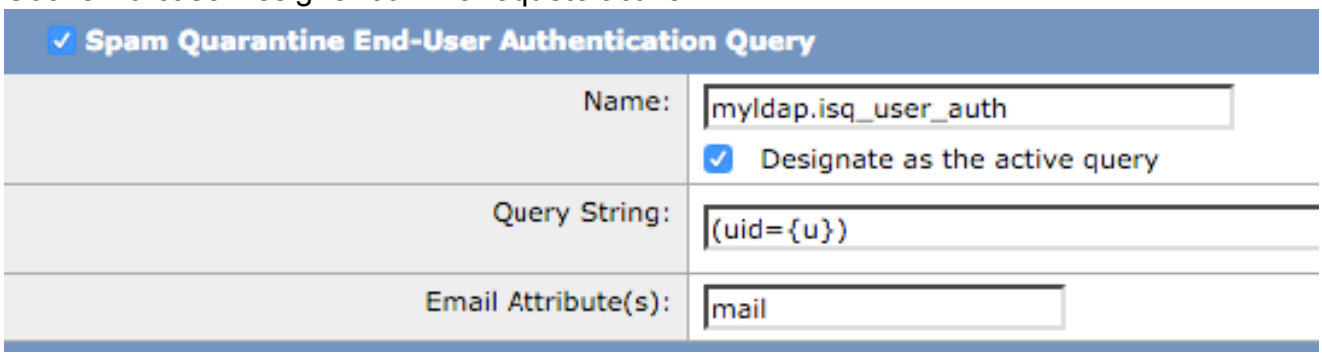
5. Sélectionnez votre calendrier de notification.



6. Soumettre et valider les modifications.

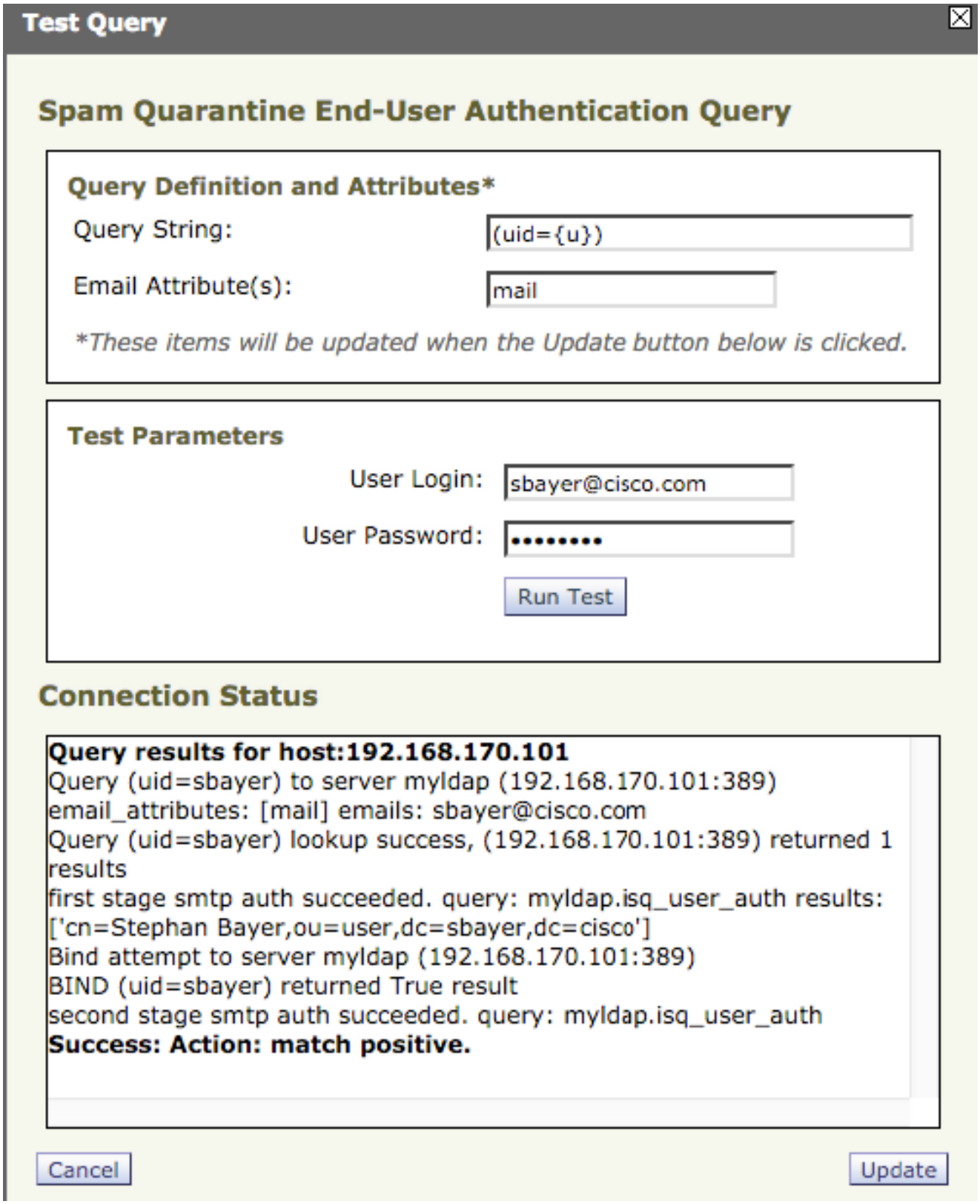
Configuration de la quarantaine du spam de l'utilisateur final Accès via la quarantaine du spam Requête d'authentification de l'utilisateur final

1. Sur le SMA ou ESA, choisissez Administration système > LDAP.
2. Ouvrez votre profil de serveur LDAP.
3. Afin de vérifier que vous êtes en mesure de vous authentifier avec un compte Active Directory, vérifiez que votre requête d'authentification de l'utilisateur final de la quarantaine du spam est activée.
4. Cochez la case Désigner comme requête active.



5. Cliquez sur Test afin de tester la requête.

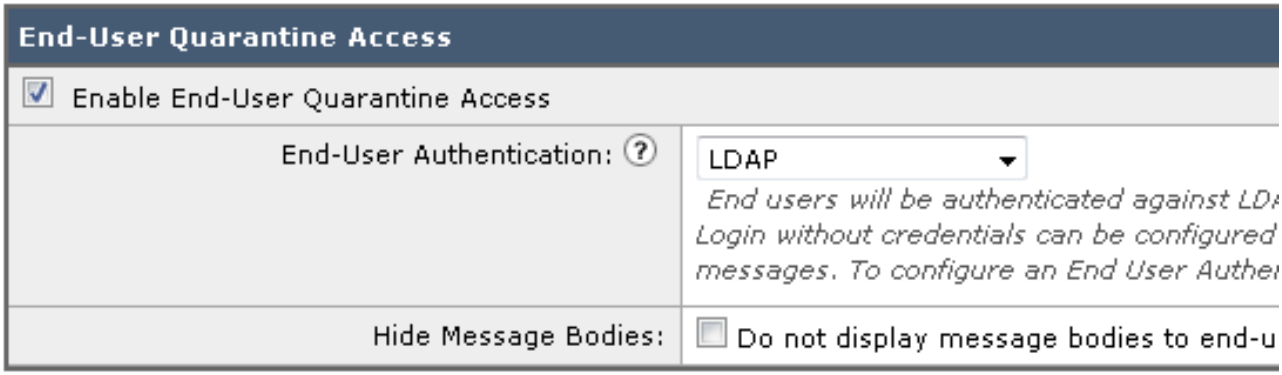
   Match Positive signifie que l'authentification a réussi :



6. Soumettre et valider les modifications.
7. Sur l'ESA, choisissez Monitor > Spam Quarantine.

   Sur le SMA, accédez aux paramètres de quarantaine du spam afin d'effectuer les mêmes étapes.

8. Cliquez sur Quarantaine du spam.
9. Cochez la case Enable End-User Quarantine Access .
10. Sélectionnez LDAP dans la liste déroulante End-User Authentication.



11. Soumettre et valider les modifications.
12. Vérifiez que l'authentification externe est sur ESA/SMA.
13. Accédez à votre URL configurée précédemment dans un navigateur Web afin de valider que vous pouvez accéder à la quarantaine :

    https://quarantine.mydomain.com:83
    https://10.10.10.10:83

14. Connectez-vous avec votre compte LDAP. En cas d'échec, vérifiez le profil LDAP d'authentification externe et activez l'accès de quarantaine de l'utilisateur final (voir les étapes précédentes).

Configurer l'accès administrateur à la quarantaine du spam

Suivez la procédure décrite dans cette section afin de permettre aux utilisateurs administratifs dotés de ces rôles de gérer les messages dans la quarantaine du spam : Opérateur, Opérateur en lecture seule, Centre d'assistance ou Guestroles, et les rôles d'utilisateur personnalisés qui incluent l'accès à la quarantaine du spam.

Les utilisateurs de niveau administrateur, qui incluent l'utilisateur administrateur par défaut et les utilisateurs Administrateur de messagerie, peuvent toujours accéder à la quarantaine du spam et n'ont pas besoin d'être associés à la fonctionnalité de quarantaine du spam à l'aide de cette procédure.

> Remarque : les utilisateurs non-administrateurs peuvent accéder aux messages de la quarantaine du spam, mais ils ne peuvent pas modifier les paramètres de quarantaine. Les utilisateurs de niveau administrateur peuvent accéder aux messages et modifier les paramètres.

Afin d'activer les utilisateurs administratifs qui n'ont pas des privilèges d'administrateur complets pour gérer les messages dans la quarantaine du spam, complétez ces étapes :

1. Assurez-vous que vous avez créé des utilisateurs et leur avez attribué un rôle d'utilisateur avec accès à la quarantaine du spam.
2. Sur l'appliance de gestion de la sécurité, choisissez Appliance de gestion > Centralized Services > Spam Quarantine.

3. Cliquez sur Activer ou Modifier les paramètres dans la section Paramètres de quarantaine du spam.
4. Dans la zone Administrative Users de la section Spam Quarantine Settings, cliquez sur le lien de sélection pour Local Users, Externally Authenticated Users ou Custom User Roles.
5. Sélectionnez les utilisateurs auxquels vous souhaitez accorder l'accès pour afficher et gérer les messages dans la quarantaine du spam.
6. Click OK.
7. Répétez l'opération si nécessaire pour chacun des autres types d'utilisateurs administratifs répertoriés dans la section (Utilisateurs locaux, Utilisateurs authentifiés en externe ou Rôles d'utilisateurs personnalisés).
8. Envoyez et validez vos modifications.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.