Configurer la passerelle de messagerie sécurisée pour la & de quarantaine Microsoft 365 Notifications

Table des matières

Introduction

Informations générales

Conditions préalables

- Exigences
- Composants utilisés

Configuration de Microsoft 365 (O365)

- Activer les notifications de quarantaine dans Microsoft Exchange Online
- Créer une règle de flux de messagerie

Configurer la messagerie sécurisée Cisco

Vérifier

Dépannage

Introduction

Ce document décrit les étapes de configuration requises pour intégrer Cisco Secure Email (CES) à la quarantaine Microsoft 365.

Informations générales

Dans une infrastructure de messagerie moderne, plusieurs couches de sécurité sont généralement déployées, ce qui peut entraîner la mise en quarantaine des messages par différents systèmes. Afin d'améliorer l'expérience utilisateur et de maintenir des workflows de notification cohérents, il est recommandé de centraliser la gestion de la quarantaine au sein d'une plate-forme unique.
Ce guide décrit le processus de redirection des messages indésirables, tels que les courriers indésirables et les messages gris, détectés par Cisco CES vers la quarantaine des utilisateurs Microsoft 365.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Un locataire actif dans la passerelle CES

- Un locataire actif dans Microsoft Exchange en ligne
- Accès aux services Microsoft 365 (O365)
- Une licence Microsoft 365 Defender (requise pour configurer les stratégies de quarantaine et les notifications)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration de Microsoft 365 (O365)

Commencez par configurer Microsoft 365 afin de recevoir et de gérer les messages mis en quarantaine.

Activer les notifications de quarantaine dans Microsoft Exchange Online

Plusieurs options de configuration permettent de contrôler la manière dont les messages sont dirigés vers la quarantaine Microsoft 365.
Si l'objectif est d'empêcher les utilisateurs finaux d'accéder aux messages mis en quarantaine ou de recevoir des notifications de quarantaine, cela peut être réalisé en implémentant une règle de flux de messagerie (transport) qui redirige les messages directement vers la quarantaine.

Inversement, si les utilisateurs finaux doivent recevoir des notifications de quarantaine et être en mesure de libérer des messages, la configuration de la règle doit être modifiée en conséquence. Dans ce scénario, la valeur SCL (Spam Confidence Level) doit être définie sur 9, ce qui désigne le message comme courrier indésirable hautement confidentiel et active les notifications de l'utilisateur et la fonctionnalité de libération.

Ces configurations sont détaillées dans la documentation officielle de Microsoft ; Configuration de la notification de quarantaine Microsoft.

L'exemple illustre la configuration qui permet aux utilisateurs finaux de recevoir des notifications de quarantaine et des messages de libération.

Créer une règle de flux de messagerie

Une fois les notifications actives, configurez une règle qui redirige les messages marqués par la passerelle CES vers la quarantaine hébergée par Microsoft.

1. Ouvrez le Centre d'administration Microsoft Exchange.
2. Dans le menu de gauche, accédez à Flux de messages > Règles.
3. Cliquez sur Add a rule, puis choisissez Create a new rule.
4. Définissez le nom de la règle sur Règle de quarantaine CSE.

5. Sous Apply this rule if, choisissez The message header, puis choisissez matches text patterns.
6. Dans le nom de l'en-tête, entrez X-CSE-Quarantine, et définissez la valeur sur true.
7. Sous Effectuer les opérations suivantes, choisissez Modifier les propriétés du message, Définir le niveau de confiance du spam, puis 9.
8. Enregistrez la configuration.
9. Après l'enregistrement, assurez-vous que la règle est activée.

Dans l'image, vous pouvez voir à quoi ressemble la règle.

CSE Quarantine

Edit rule conditions Edit rule settings

Status: Enabled

Enable or disable rule

Enabled

Rule settings

Rule name
CSE Quarantine

Mode
Enforce

Severity
Not specified

Set date range
Specific date range is not set

Senders address
Matching Header

Priority
1

For rule processing errors
Ignore

Rule description

Apply this rule if

'X-CSE-Quarantine' header matches the following patterns: 'true'

Do the following

Set the spam confidence level (SCL) to '9'

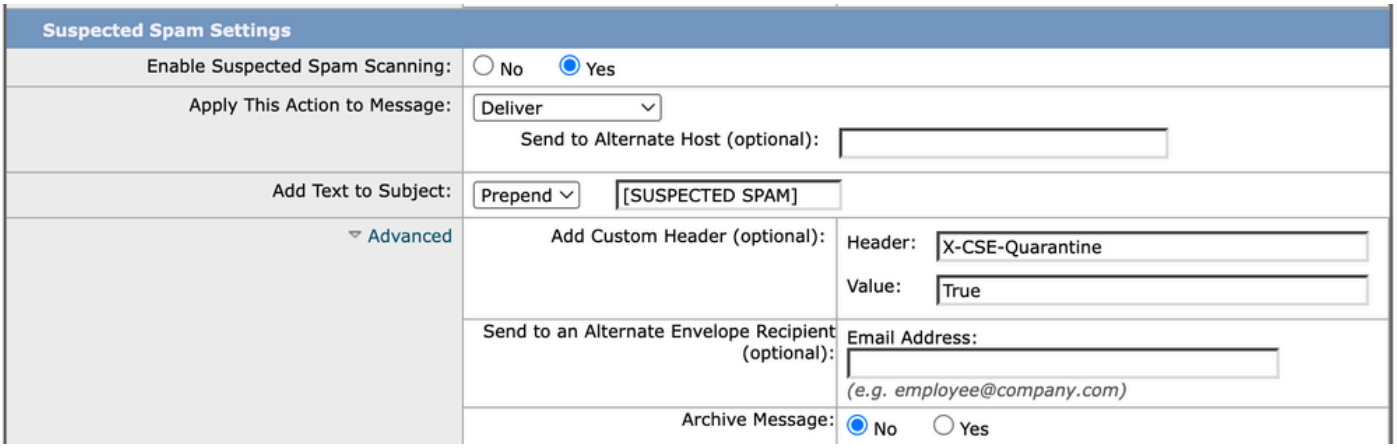
Rule comments

Configurer la messagerie sécurisée Cisco

Dans Cisco CES, un en-tête personnalisé (X-CSE-Quarantine : true) peut être ajouté à tout message qui doit être redirigé vers la quarantaine de Microsoft. Ces messages peuvent être marqués par n'importe quel filtre ou moteur de contenu dans CES. Dans cet exemple, il est configuré pour les messages de spam suspecté.

1. Ouvrez la console Cisco Secure Email Management.
2. Accédez à Politiques de messagerie > Politiques de messages entrants.
3. Modifiez les stratégies que vous souhaitez modifier (par exemple, choisissez la stratégie par défaut).
4. Cliquez sur les paramètres de spam pour la stratégie choisie.
5. Sous Suspect Spam, remplacez l'action Quarantine par Deliver.
6. Cliquez sur Avancé et ajoutez un en-tête personnalisé :
    - Nom d'en-tête : X-CSE-Quarantine
    - Valeur: true (même valeur utilisée dans la règle Microsoft)
7. Cliquez sur Submit, puis sur Commit Changes afin d'appliquer la configuration.

Dans l'image, vous pouvez voir à quoi ressemble la configuration.

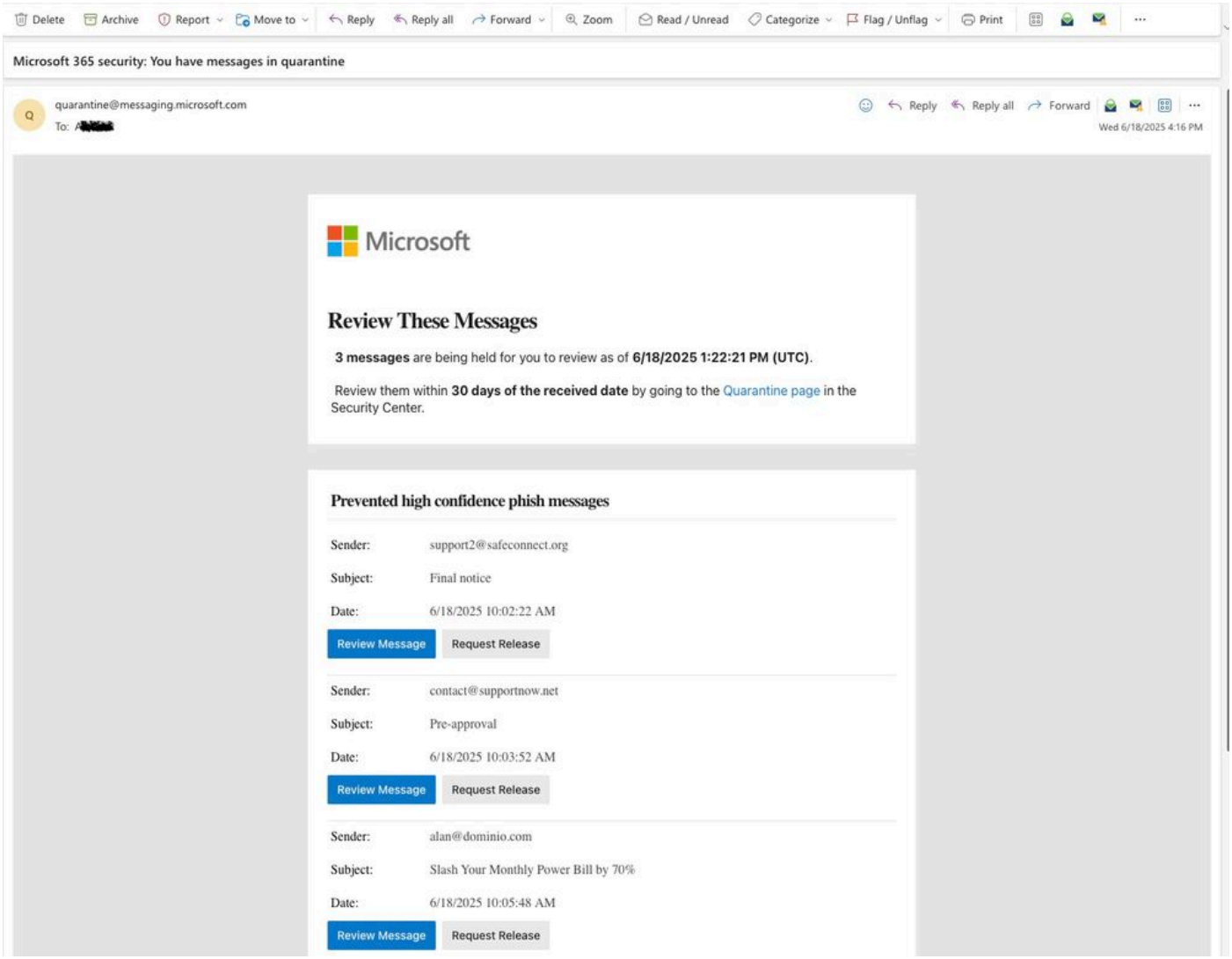


configuration CES

Vérifier

À partir de ce moment, les e-mails identifiés par Cisco CES comme des spams potentiels seront marqués avec l'en-tête personnalisé. Microsoft 365 détecte cette balise et redirige le message vers la quarantaine Microsoft.

Les utilisateurs vont recevoir des notifications de quarantaine selon la configuration Microsoft 365.

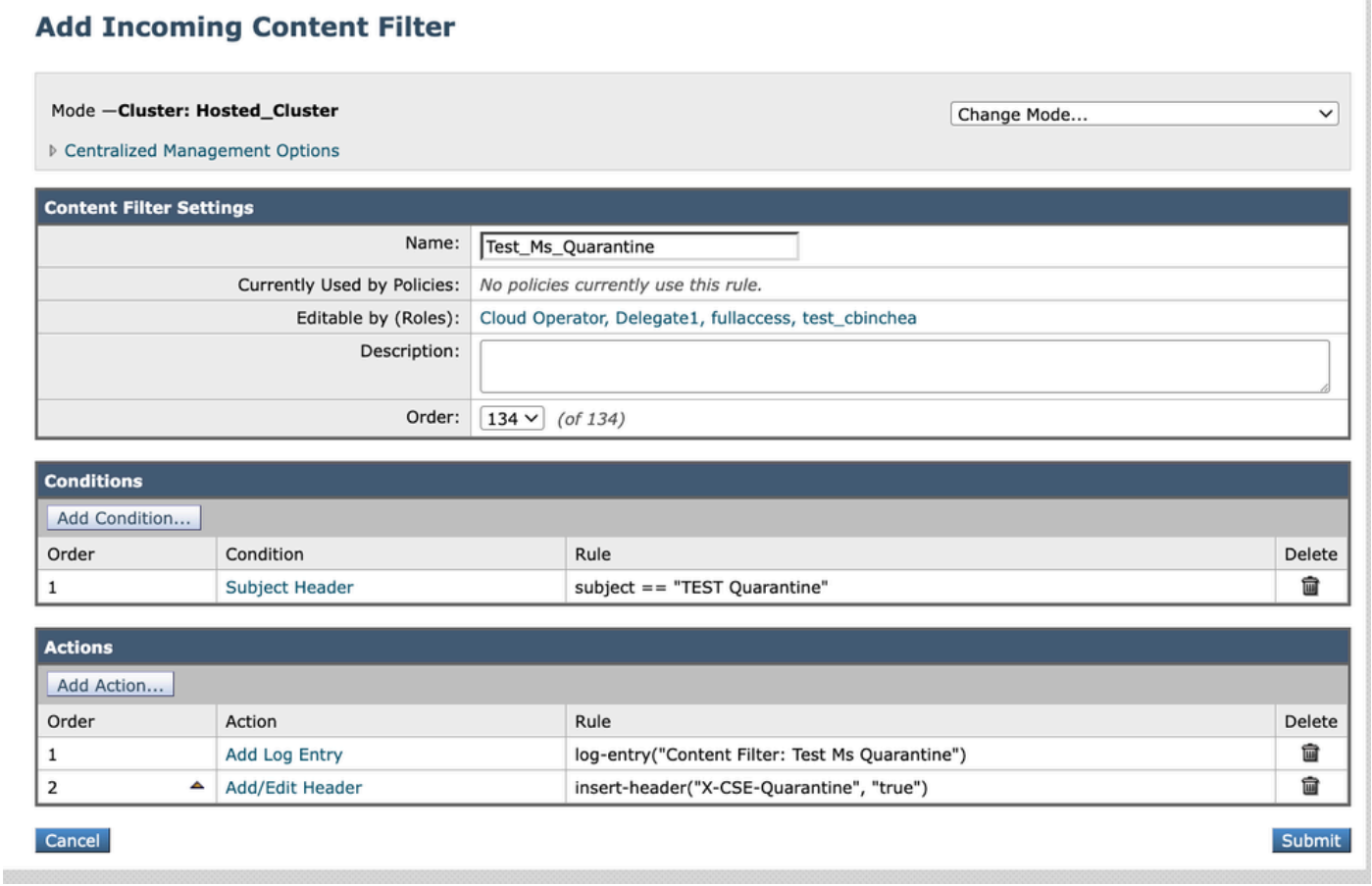


Dépannage

Afin de valider l'efficacité de la configuration et de confirmer que Microsoft achemine le message vers la quarantaine prévue, un filtre de contenu entrant peut être créé pour insérer le même en-tête lorsque l'objet du message correspond à un mot clé ou à un modèle spécifique.

En implémentant ce filtre, la passerelle de messagerie sécurisée (SEG) ajoute l'en-tête désigné, ce qui permet à Microsoft 365 de traiter le message selon sa logique antispam standard, en répliquant efficacement le comportement qui peut se produire si l'en-tête est injecté par le moteur de filtrage antispam natif.

Voici un exemple de filtre de contenu :



Test du filtre de contenu

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.