Configuration de Microsoft 365 avec la messagerie sécurisée

Table des matières

Introduction

Ce document décrit les étapes de configuration pour intégrer Microsoft 365 avec Cisco Secure Email pour la remise des e-mails entrants et sortants.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Passerelle Cisco Secure Email Cloud Gateway ou passerelle en nuage
- Accès par interface de ligne de commande (CLI) à votre environnement Cisco Secure Email Cloud Gateway :
  Cisco Secure Email Cloud Gateway > Accès à l'interface de ligne de commande (CLI)
- Microsoft 365
- Protocole SMTP (Simple Mail Transfer Protocol)
- Serveur de noms de domaine ou système de noms de domaine (DNS)

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.

Informations générales

Ce document peut être utilisé pour les passerelles sur site ou les passerelles cloud Cisco.

Si vous êtes un administrateur de messagerie électronique sécurisée Cisco, votre lettre de bienvenue inclut vos adresses IP de passerelle cloud et d'autres informations pertinentes. En plus de la lettre que vous voyez ici, un e-mail chiffré vous est envoyé pour vous fournir des détails supplémentaires sur le nombre de Cloud Gateway (également appelé ESA) et Cloud Email and Web Manager (également appelé SMA) provisionnés pour votre allocation. Si vous n'avez pas reçu ou n'avez pas de copie de la lettre, contactez ces-activations@cisco.com avec vos coordonnées et votre nom de domaine en service.

Your Cisco Cloud Email Security (CES) service is ready!

Organization Name: [redacted]
Start Date: 2022-09-09 05:09:04 America/Los_Angeles

Below you will find information about your login credentials and other important information regar ding your CES. Please retain this email for future reference

MX Records for inbound email from Internet

- mx1.[redacted].iphmx.com
- mx2.[redacted].iphmx.com

Your Cisco CES portals:

Email Security
https://dh[redacted]-esa1.iphmx.com
Security Management
https://dh[redacted]-sma1.iphmx.com
End User Quarantine
https://dh[redacted]-euq1.iphmx.com

Please sign in the portals with this user ID:

Username: [redacted]
Password: [redacted]
Note: We recommend changing your password after the initial login.

Hostname and IP addresses to be whitelisted(for Microsoft/Office365 and G-Suite u sers):

Email Security:
[redacted].140.105
[redacted].150.143
[redacted].143.186
[redacted].32.98
Security Management:
[redacted].157.91

If you are using a Cloud service such as Office365, G-Suite, etc., you should direct your o utbound emails to the address below to have them scanned by Cisco Cloud Email Securit y:

Host and IP address used for outbound relay from Office365 and G-Suite:
ob1.hc[redacted].iphmx.com

Include CES host and IP address in your SPF record:

v=spf1 exists:%{i}.spf.hc[redacted].iphmx.com ~all

Chaque client dispose d’adresses IP dédiées. Vous pouvez utiliser les adresses IP ou les noms d’hôte attribués lors de la configuration de Microsoft 365.

Remarque : il est vivement recommandé de tester avant toute mise en service planifiée des messages de production, car les configurations prennent du temps à se répliquer dans la console Microsoft 365 Exchange. Attendez au moins une heure pour que toutes les modifications soient prises en compte.

Remarque : les adresses IP de la capture d'écran sont proportionnelles au nombre de passerelles cloud provisionnées pour votre allocation. Par exemple, xxx.yy.140.105 est l'adresse IP de l'interface Data 1 pour la passerelle 1 et xxx.yy.150.1143 est l'adresse IP de l'interface Data 1 pour la passerelle 2. L'adresse IP de l'interface de données 2 pour la passerelle 1 est xxx.yy.143.186 et l'adresse IP de l'interface de données 2 pour la passerelle 2 est xxx.yy.32.98. Si votre lettre de bienvenue ne contient pas d'informations sur Data 2 (IP d'interface sortante), contactez le TAC Cisco pour que l'interface Data 2 soit ajoutée à votre allocation.

Configuration de Microsoft 365 avec la messagerie sécurisée

Configurer les courriels entrants dans Microsoft 365 depuis Cisco Secure Email

Contourner la règle de filtrage des pourriels

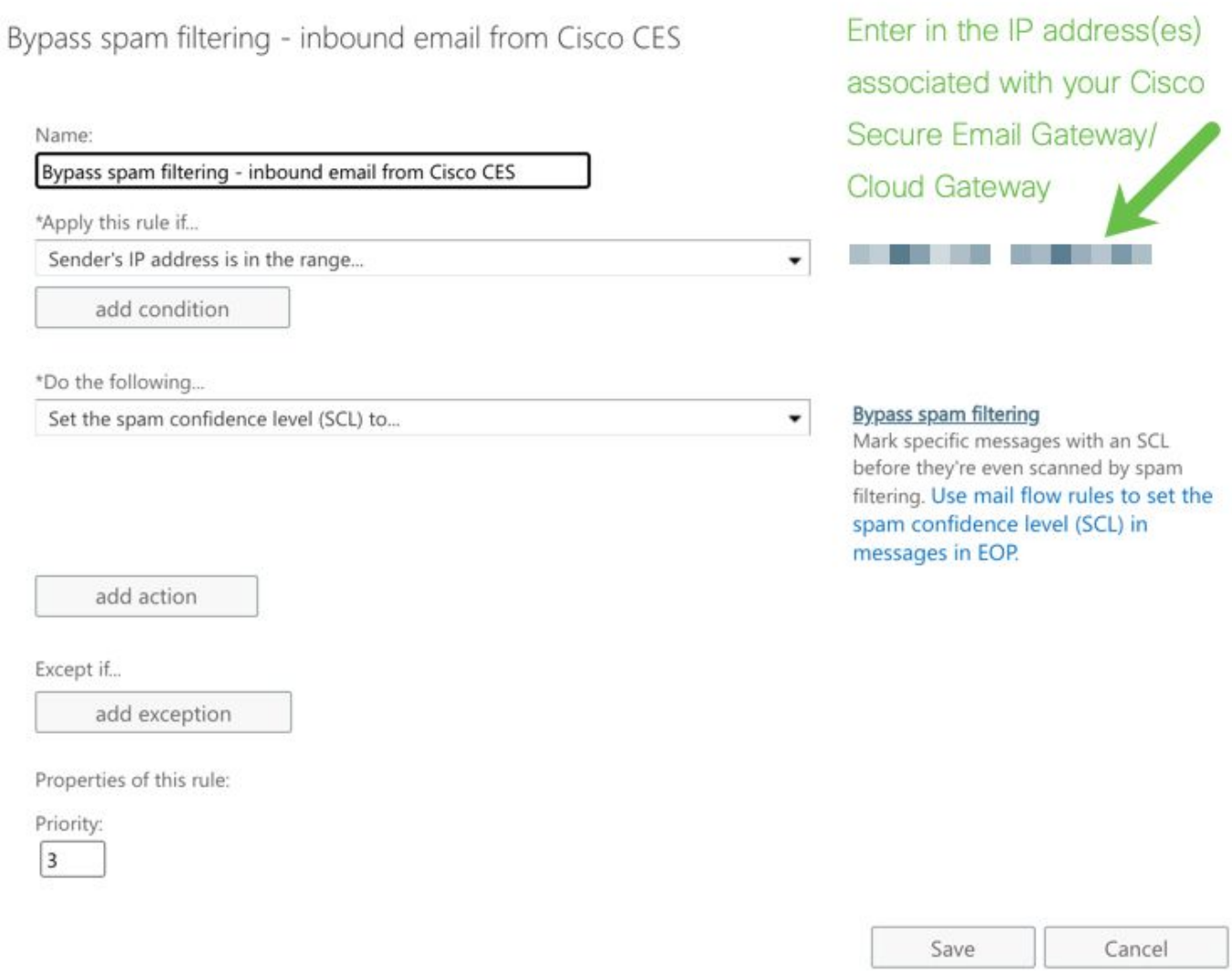
- Connectez-vous au Centre d'administration Microsoft 365 (https://portal.microsoft.com).
- Dans le menu de gauche, développez **Admin Centers**.
- Cliquer **Exchange**.
- Dans le menu de gauche, accédez à **Mail flow > Rules**.
- Cliquez ici **[+]** pour créer une nouvelle règle.
- Faites votre choix dans **Bypass spam filtering...** la liste déroulante.
- Entrez un nom pour votre nouvelle règle : **Bypass spam filtering - inbound email from Cisco CES**.
- Pour *Appliquer cette règle si..., choisissez **The sender - IP address is in any of these ranges or exactly matches**.

1. Dans la fenêtre contextuelle Spécifier les plages d'adresses IP, ajoutez les adresses IP fournies dans votre lettre de bienvenue Cisco Secure Email.
2. Cliquer **OK**.

- Pour *Effectuez les opérations suivantes..., la nouvelle règle a été présélectionnée : **Set the spam confidence level (SCL) to... - Bypass spam filtering**.

- Cliquer **Save**.

Voici un exemple de l'aspect de votre règle :



Connecteur de réception

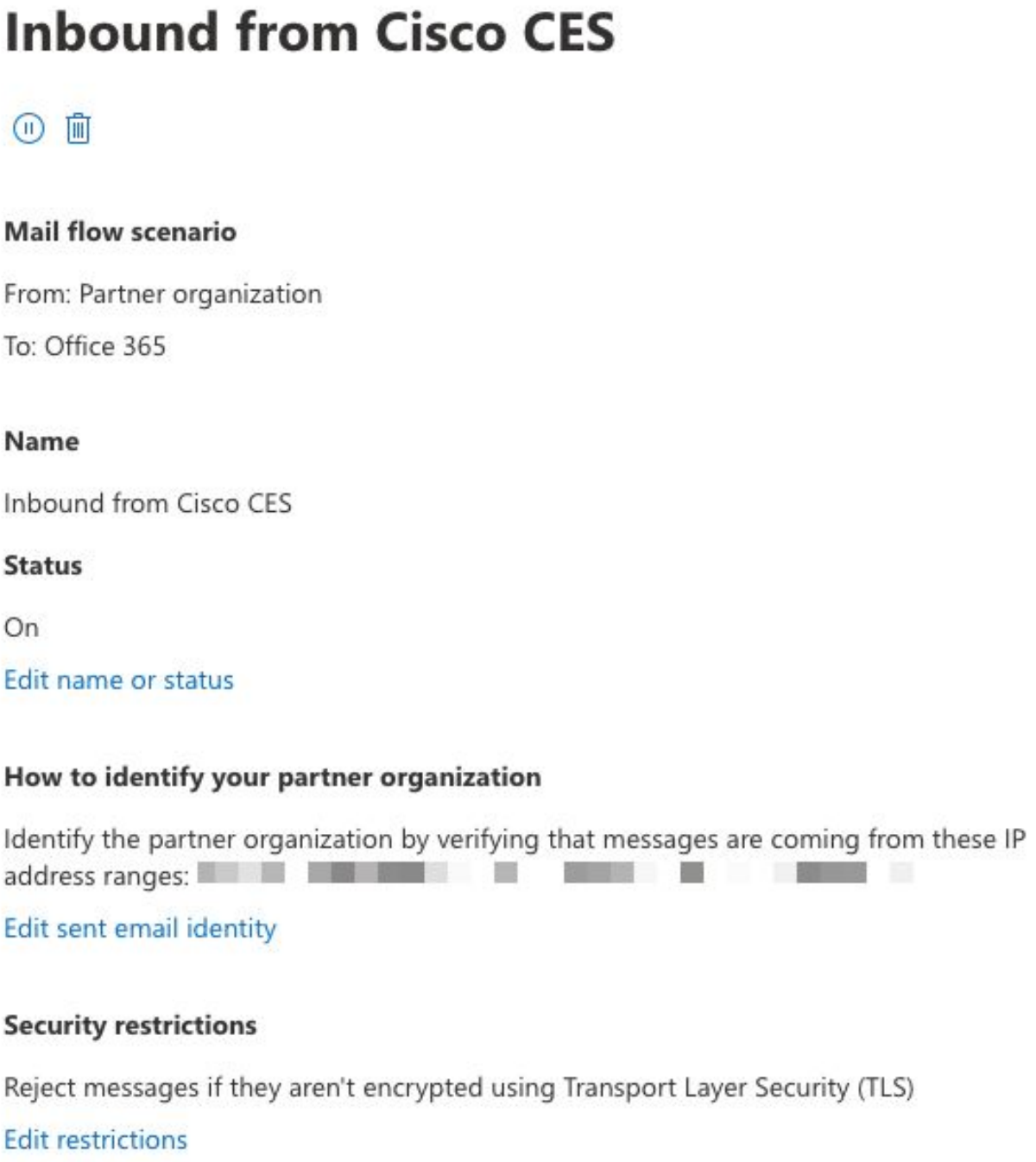
- Restez dans le Centre d'administration Exchange.
- Dans le menu de gauche, accédez à **Mail flow > Connectors**.
- Cliquez sur **[+]** pour créer un nouveau connecteur.
- Dans la fenêtre contextuelle Sélectionner votre scénario de flux de messagerie, sélectionnez :

1. From (de) : Partner organization

    - Par : **Office365**

- Cliquer **Next**.
- Entrez un nom pour votre nouveau connecteur : **Inbound from Cisco CES**.
- Saisissez une description, si vous le souhaitez.
- Cliquer **Next**.
- Cliquer **Use the sender's IP address**.
- Cliquer **Next**.
- Cliquez sur **[+]** et saisissez les adresses IP indiquées dans votre lettre de bienvenue Cisco Secure Email.
- Cliquer **Next**.
- Choisir **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- Cliquer **Next**.
- Cliquer **Save**.

Voici un exemple de la configuration de votre connecteur :



Configurer les courriels de Cisco Secure Email vers Microsoft 365

Contrôles de destination

Imposez une auto-limitation à un domaine de remise dans vos contrôles de destination. Bien sûr, vous pouvez supprimer l'accélérateur plus tard, mais ce sont de nouvelles IP à Microsoft 365, et vous ne voulez pas de limitation par Microsoft en raison de sa réputation inconnue.

- Connectez-vous à votre modem routeur.
- Naviguez jusqu'à **Mail Policies > Destination Controls**.
- Cliquer **Add Destination**.

- Utilisation:

1. Destination : saisissez votre nom de domaine

2. Concurrent Connections (connexions simultanées) : **10**

   - Maximum Messages Per Connection (nombre maximal de messages par connexion) : **20**
   - TLS Support (soutien TLS) : **Preferred**

- Cliquer **Submit**.
- Cliquez sur **Commit Changes** en haut à droite de l'interface utilisateur pour enregistrer vos modifications de configuration.

Exemple de présentation de votre table de contrôle des destinations :

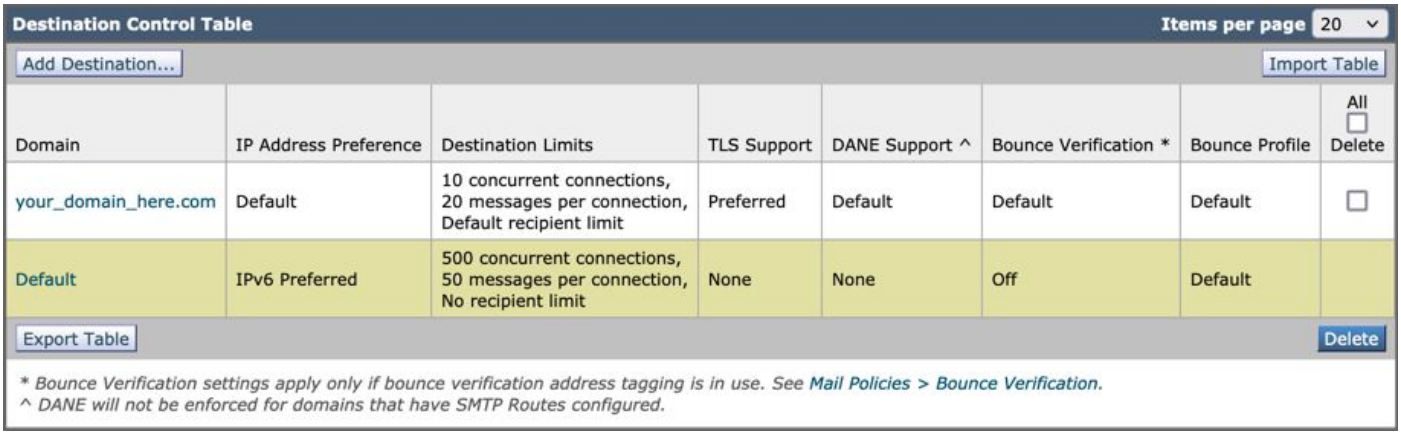


Tableau d’accès des destinataires

Ensuite, définissez le tableau d’accès des destinataires (RAT) pour qu’il accepte les courriels de vos domaines :

- Naviguez jusqu'à **Mail Policies > Recipient Access Table (RAT)**.

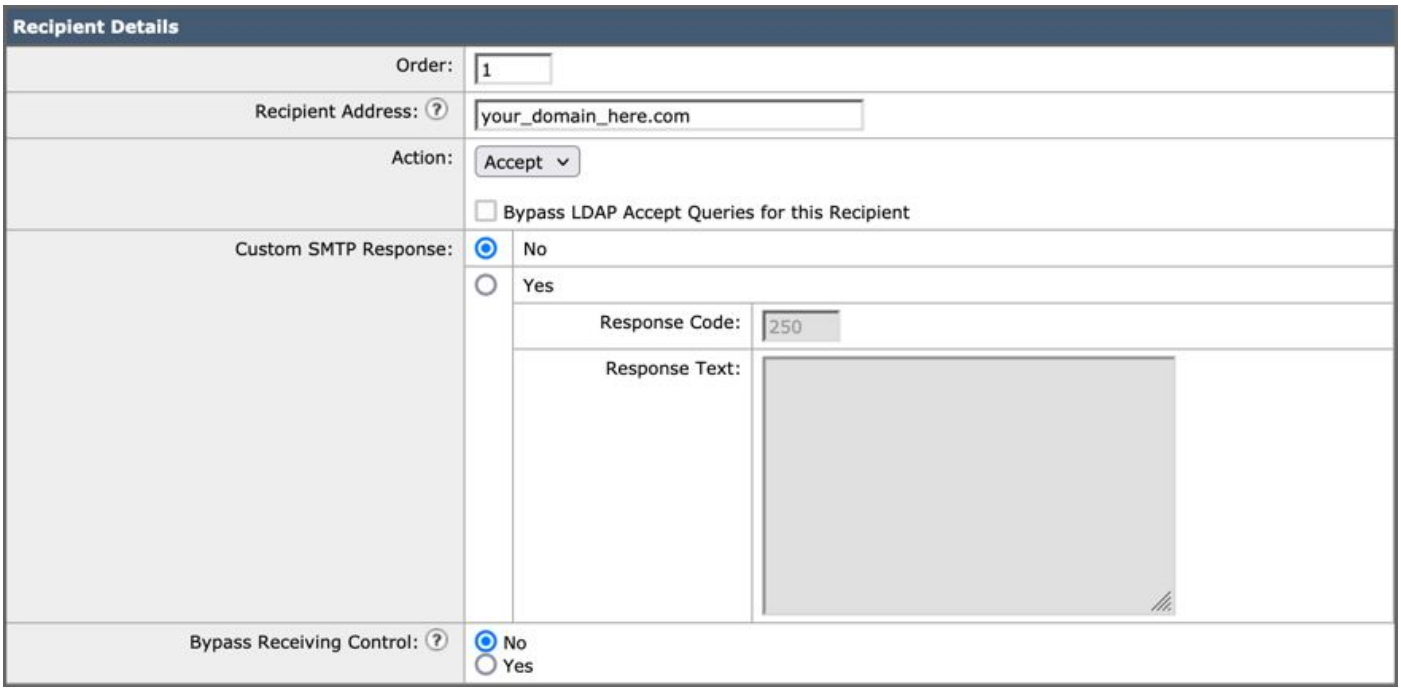
Remarque : assurez-vous que l'écouteur est destiné à l'écouteur entrant, à IncomingMail ou à MailFlow, en fonction du nom réel de l'écouteur pour votre flux de messagerie principal.

- Cliquer **Add Recipient**.
- Ajoutez vos domaines dans le champ Adresse du destinataire.
- Sélectionnez l'action par défaut de **Accept**.

- Cliquer **Submit**.

- Cliquez sur **Commit Changes** en haut à droite de l'interface utilisateur pour enregistrer vos modifications de configuration.

Voici un exemple de l'apparence de votre entrée RAT :



Routes SMTP

Définissez le routage SMTP pour la remise du courrier électronique sécurisé Cisco à votre domaine Microsoft 365 :

- Naviguez jusqu'à **Network > SMTP Routes**.

- Cliquer **Add Route...**

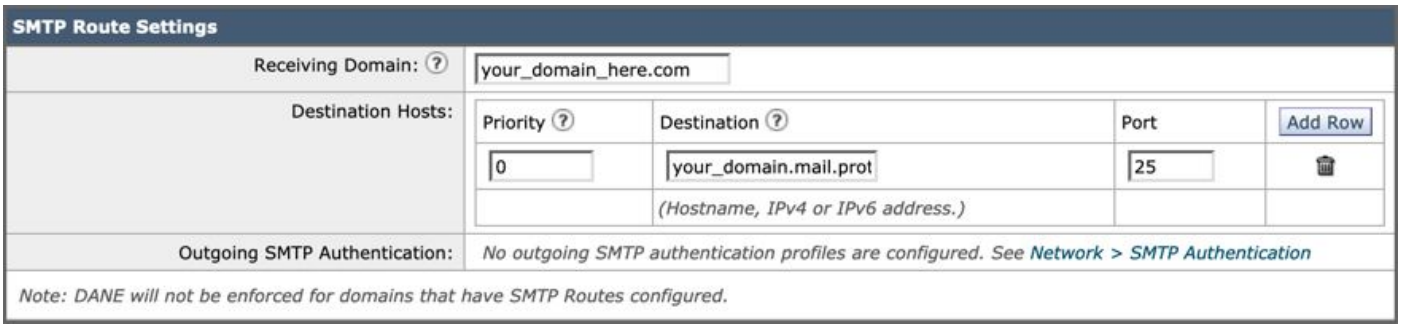
- Receiving Domain : saisissez votre nom de domaine.

- Hôtes de destination : ajoutez votre enregistrement Microsoft 365 MX d'origine.

- Cliquer **Submit**.

- Cliquez sur **Commit Changes** en haut à droite de l'interface utilisateur pour enregistrer vos modifications de configuration.

Exemple de l'apparence de vos paramètres de routage SMTP :



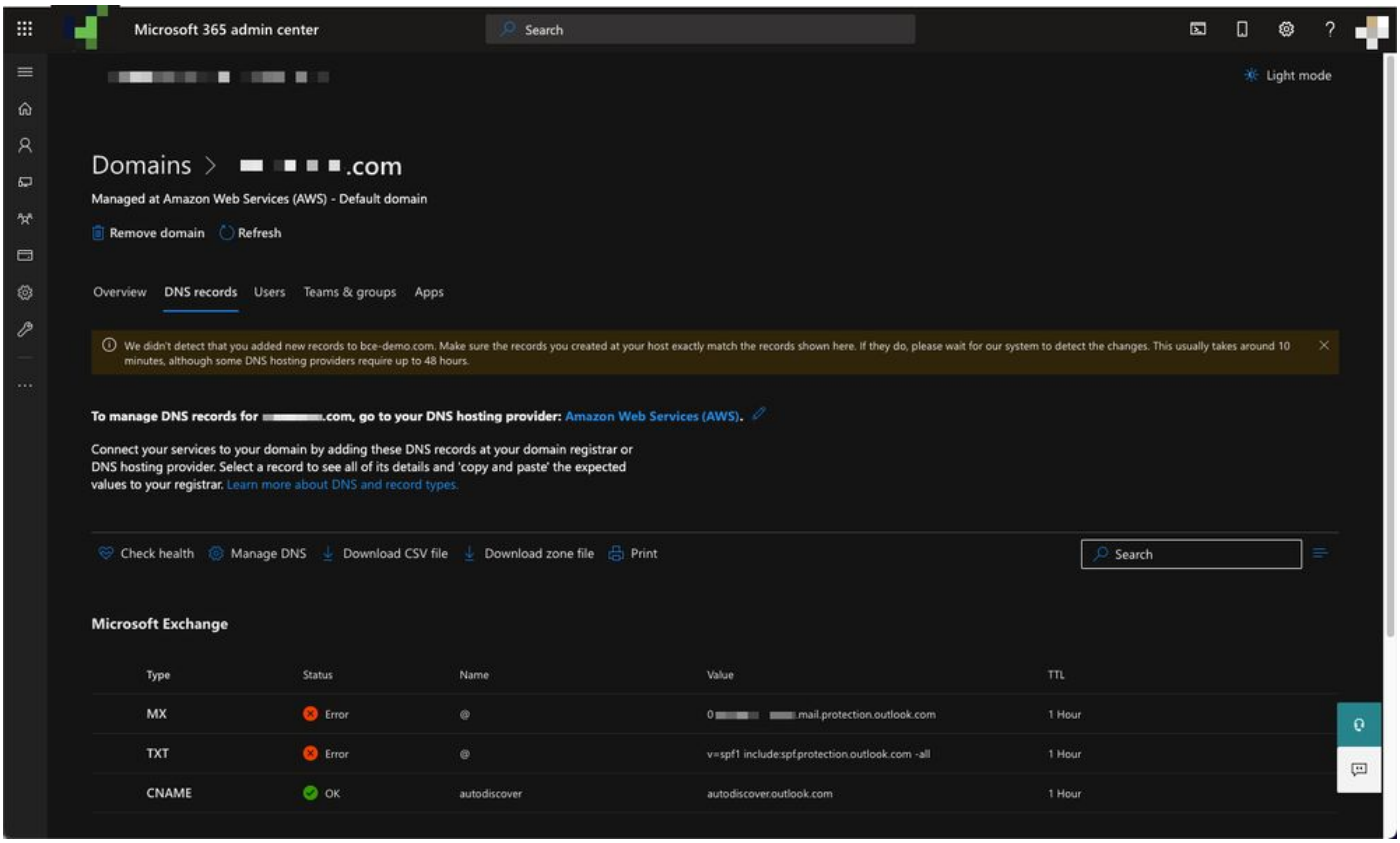
Configuration DNS (enregistrement MX)

Vous êtes prêt à couper le domaine via une modification d'enregistrement MX (Mail Exchange). Travaillez avec votre administrateur DNS pour résoudre vos enregistrements MX en adresses IP pour votre instance Cisco Secure Email Cloud, comme indiqué dans votre lettre de bienvenue Cisco Secure Email.

Vérifiez également la modification apportée à l'enregistrement MX à partir de votre console Microsoft 365 :

- Connectez-vous à la console Admin de Microsoft 365 (https://admin.microsoft.com).
- Naviguez jusqu'à **Home > Settings > Domains**.
- Choisissez votre nom de domaine par défaut.
- CliquerCheck Health.

Cette section fournit les enregistrements MX actuels de la façon dont Microsoft 365 recherche vos enregistrements DNS et MX associés à votre domaine :



Remarque : dans cet exemple, le DNS est hébergé et géré par Amazon Web Services (AWS). En tant qu'administrateur, attendez-vous à voir un avertissement si votre DNS est hébergé n'importe où en dehors du compte Microsoft 365. Vous pouvez ignorer des avertissements comme : "Nous n'avons pas détecté que vous avez ajouté de nouveaux enregistrements à your_domain_here.com. Assurez-vous que les enregistrements que vous avez créés sur votre hôte correspondent à ceux affichés ici..." Les instructions détaillées réinitialisent les enregistrements MX à ce qui a été initialement configuré pour la redirection vers votre compte Microsoft 365. La passerelle de messagerie sécurisée Cisco est ainsi supprimée du flux de trafic entrant.

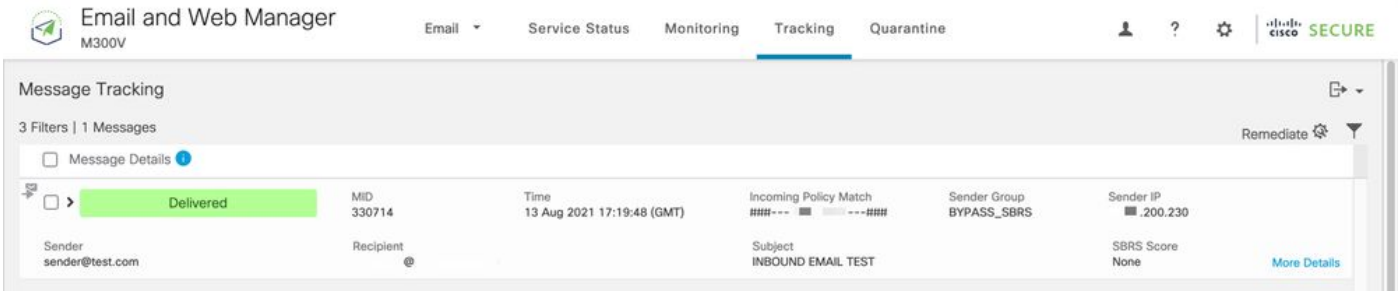
Tester le courrier entrant

Testez le courrier entrant vers votre adresse de messagerie Microsoft 365. Vérifiez ensuite qu'il arrive dans votre boîte de réception de messagerie Microsoft 365.

Validez les journaux de messagerie dans Message Tracking sur votre Cisco Secure Email and Web Manager (également appelé SMA) fourni avec votre instance.

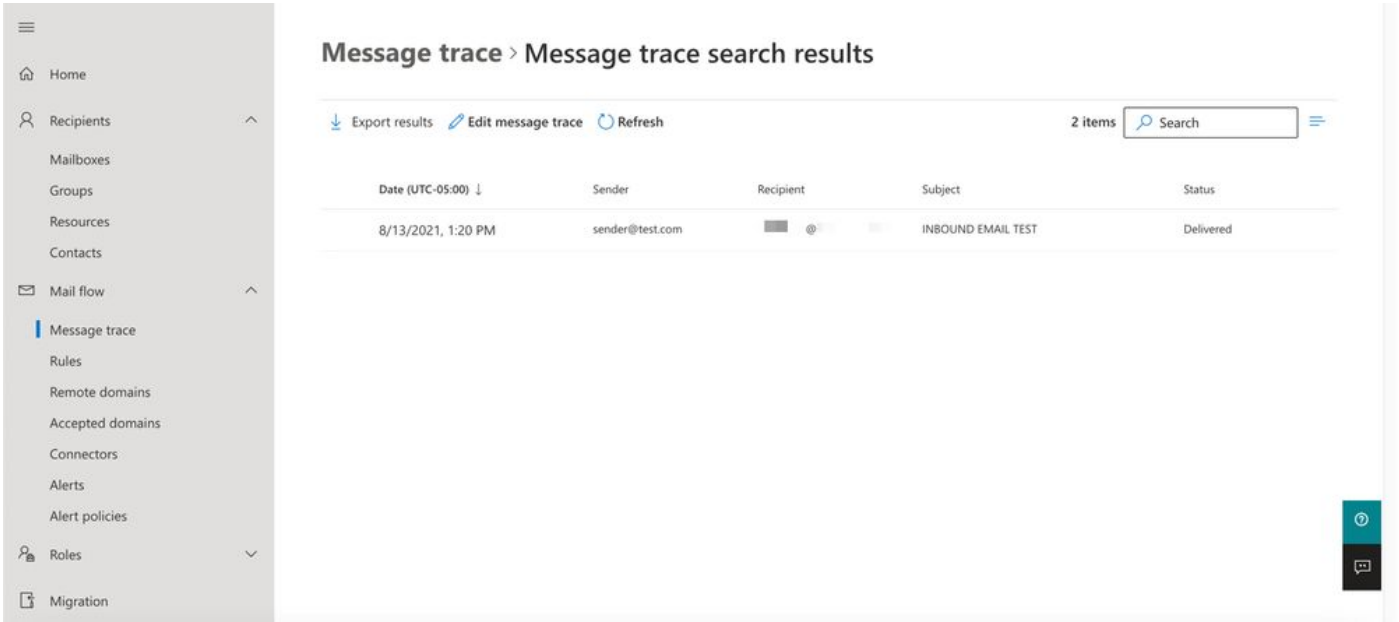
Pour afficher les journaux de messagerie sur votre SMA :

- Connectez-vous à votre SMA (https://sma.iphmx.com/ng-login)
- Cliquer **Tracking**.
- Entrez les critères de recherche requis et cliquez sur **Search**; et attendez-vous à voir ces résultats :



Pour afficher les journaux de messagerie dans Microsoft 365 :

- Connectez-vous au Centre d'administration Microsoft 365 (https://admin.microsoft.com).
- Accroissement **Admin Centers**.
- Cliquer **Exchange**.
- Naviguez jusqu'à **Mail flow > Message trace**.
- Microsoft fournit des critères de recherche par défaut. Par exemple, choisissez **Messages received by my primary domain in the last day** de lancer votre requête de recherche.
- Entrez les critères de recherche requis pour les destinataires et cliquez sur **Search** et attendez-vous à voir les résultats similaires à :



Configurer les courriels sortants de Microsoft 365 vers Cisco Secure Email

Configurer RELAYLIST sur la passerelle Cisco Secure Email Gateway

Reportez-vous à votre lettre de bienvenue Cisco Secure Email. En outre, une interface secondaire est spécifiée pour les messages sortants via votre modem routeur.

- Connectez-vous à votre modem routeur.

- Naviguez jusqu'à **Mail Policies > HAT Overview**.

Remarque : assurez-vous que l'écouteur est pour Outgoing Listener, OutgoingMail ou MailFlow-Ext, en fonction du nom réel de votre écouteur pour votre flux de courrier externe/sortant.

- Cliquer **Add Sender Group...**

- Configurez le groupe d’expéditeurs comme suit :

1. Nom : RELAY_O365

2. Comment (commentaire) : <<enter a comment if you wish to notate your sender group>>

3. Stratégie : RELAYÉE

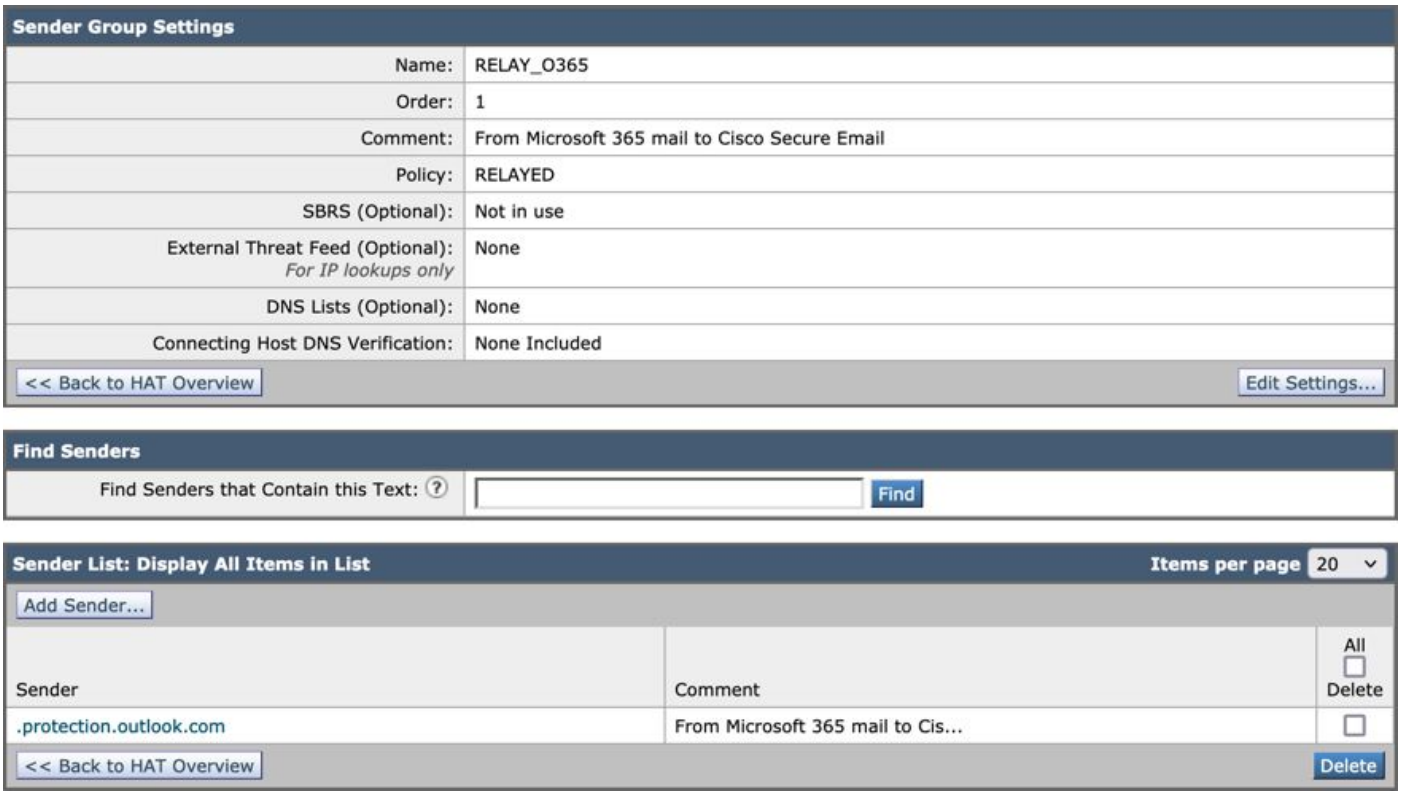
4. Cliquer **Submit and Add Senders**.

- Expéditeur : **.protection.outlook.com**

Remarque : la **.** (point) au début du nom de domaine de l'expéditeur est obligatoire.

- Cliquer **Submit**.
- Cliquez sur **Commit Changes** en haut à droite de l'interface utilisateur pour enregistrer vos modifications de configuration.

Voici un exemple de l'apparence de vos paramètres de groupe d'expéditeurs :



Activer TLS

- Cliquer **<<Back to HAT Overview**.
- Cliquez sur la politique de flux de messagerie nommée : **RELAYED**.
- Faites défiler vers le bas et recherchez dans la **Security Features** section **Encryption and Authentication**.
- Pour TLS, sélectionnez : **Preferred**.
- Cliquer **Submit**.
- Cliquez sur **Commit Changes** en haut à droite de l'interface utilisateur pour enregistrer vos modifications de configuration.

Exemple de configuration de votre stratégie de flux de messagerie :

Configurer la messagerie de Microsoft 365 vers CES

- Connectez-vous au Centre d'administration Microsoft 365 (https://admin.microsoft.com).
- Accroissement **Admin Centers**.

- Cliquer **Exchange**.
- Naviguez jusqu'à **Mail flow > Connectors**.
- Cliquez sur [+] pour créer un nouveau connecteur.
- Dans la fenêtre contextuelle Sélectionner votre scénario de flux de messagerie, sélectionnez :

    1. From (de) : Office365
        - Par :Partner organization

- Cliquer **Next**.
- Entrez un nom pour votre nouveau connecteur : **Outbound to Cisco CES**.
- Saisissez une description, si vous le souhaitez.
- Cliquer **Next**.
- Pour Quand voulez-vous utiliser ce connecteur ? :

    1. Choisissez : **Only when I have a transport rule set up that redirects messages to this connector**.
        - Cliquer **Next**.

- Cliquer **Route email through these smart hosts**.
- Cliquez sur **[+]** et saisissez les adresses IP sortantes ou les noms d'hôte fournis dans votre lettre de bienvenue CES.
- Cliquer **Save**.
- Cliquer **Next**.
- Pour savoir comment Office 365 doit-il se connecter au serveur de messagerie de votre organisation partenaire ?

    1. Choisissez : **Always use TLS to secure the connection (recommended)**.
        - ChoisissezAny digital certificate, including self-signed certificates.
        - Cliquer **Next**.

- L'écran de confirmation s'affiche.
- Cliquer **Next**.
- Utilisez **[+]** pour saisir une adresse e-mail valide et cliquez sur **OK**.
- Cliquez sur **Validate** et laissez la validation s'exécuter.
- Une fois terminé, cliquez sur **Close**.
- CliquerSave.

Voici un exemple de l'apparence de votre connecteur sortant :

Outbound to Cisco CES

Mail flow scenario

From: Office 365

To: Partner organization

Name

Outbound to Cisco CES

Status

On

Edit name or status

Use of connector

Use only when I have a transport rule set up that redirects messages to this connector.

Edit use

Routing

Route email messages through these smart hosts: [redacted].iphmx.com

Edit routing

Security restrictions

Always use Transport Layer Security (TLS) and connect only if the recipient's email server has a digital certificate.

Edit restrictions

Validation

Last validation result: Validation successful

Last validation time: 10/5/2020, 9:08 AM

Validate this connector

Créer une règle de flux de messagerie

1. Pour la fenêtre contextuelle Sélectionner l'emplacement de l'expéditeur, sélectionnez : **Inside the organization**.

    - Cliquer **OK**.

- Cliquer **More options...**
- Cliquez sur **add condition** le bouton et insérez une deuxième condition :

    1. Choisir **The recipient...**

        - Choisissez : **Is external/internal**.
        - Pour la fenêtre contextuelle Sélectionner l'emplacement de l'expéditeur, sélectionnez : **Outside the organization** .
        - Cliquer **OK**.

- Pour *Effectuez les opérations suivantes..., choisissez : **Redirect the message to...**

    1. Sélectionnez : **le connecteur suivant**.
    2. Et sélectionnez votre connecteur **Outbound to Cisco CES**.
    3. Click OK.

- Revenez à "*Effectuez les opérations suivantes..." et insérez une deuxième action :

    1. Choisissez : **Modify the message properties...**

        - Choisissez : **set the message header**
        - Définissez l’en-tête du message : **X-OUTBOUND-AUTH**.
        - Cliquer **OK**.
        - Définissez la valeur : **mysecretkey**.

- Cliquer **OK**.

- Cliquer **Save**.

Remarque : pour empêcher les messages non autorisés de Microsoft, un en-tête x secret peut être estampillé lorsque les messages quittent votre domaine Microsoft 365 ; cet en-tête est évalué et supprimé avant d'être remis sur Internet.

Exemple de configuration du routage Microsoft 365 :

Outbound to Cisco CES

Name:

Outbound to Cisco CES

*Apply this rule if...

✖ The sender is located... — Inside the organization

and

✖ The recipient is located... — Outside the organization

add condition

*Do the following...

✖ Set the message header to this value... — Set the message header 'X-OUTBOUND-AUTH' to the value 'mysecretkey'

and

✖ Use the following connector... — Outbound to Cisco CES

add action

Except if...

add exception

Properties of this rule:

Priority:

0

☐ Audit this rule with severity level:

Not specified

Choose a mode for this rule:

◉ Enforce
○ Test with Policy Tips
○ Test without Policy Tips

☐ Activate this rule on the following date:

Fri 8/13/2021 1:30 PM

☐ Deactivate this rule on the following date:

Fri 8/13/2021 1:30 PM

☐ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message:

Header

☐ Add to DLP policy

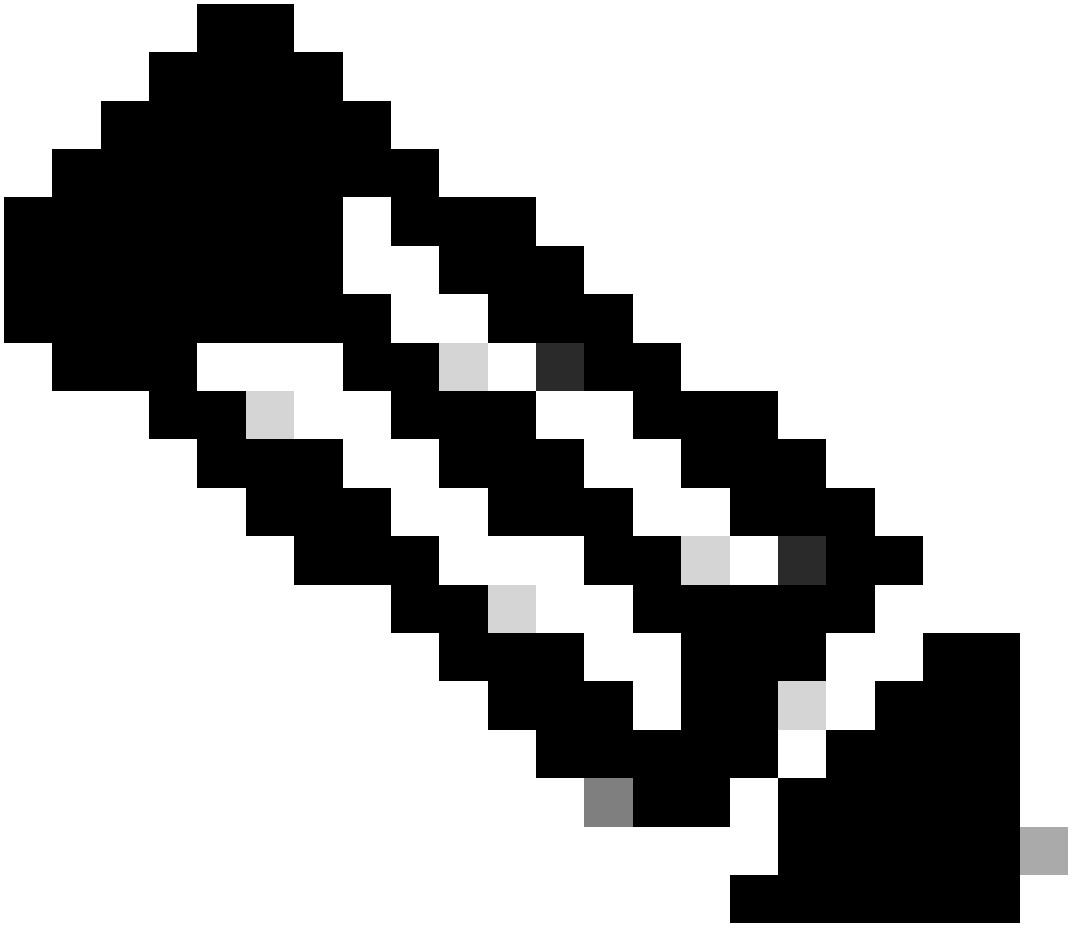
PCI

Comments:

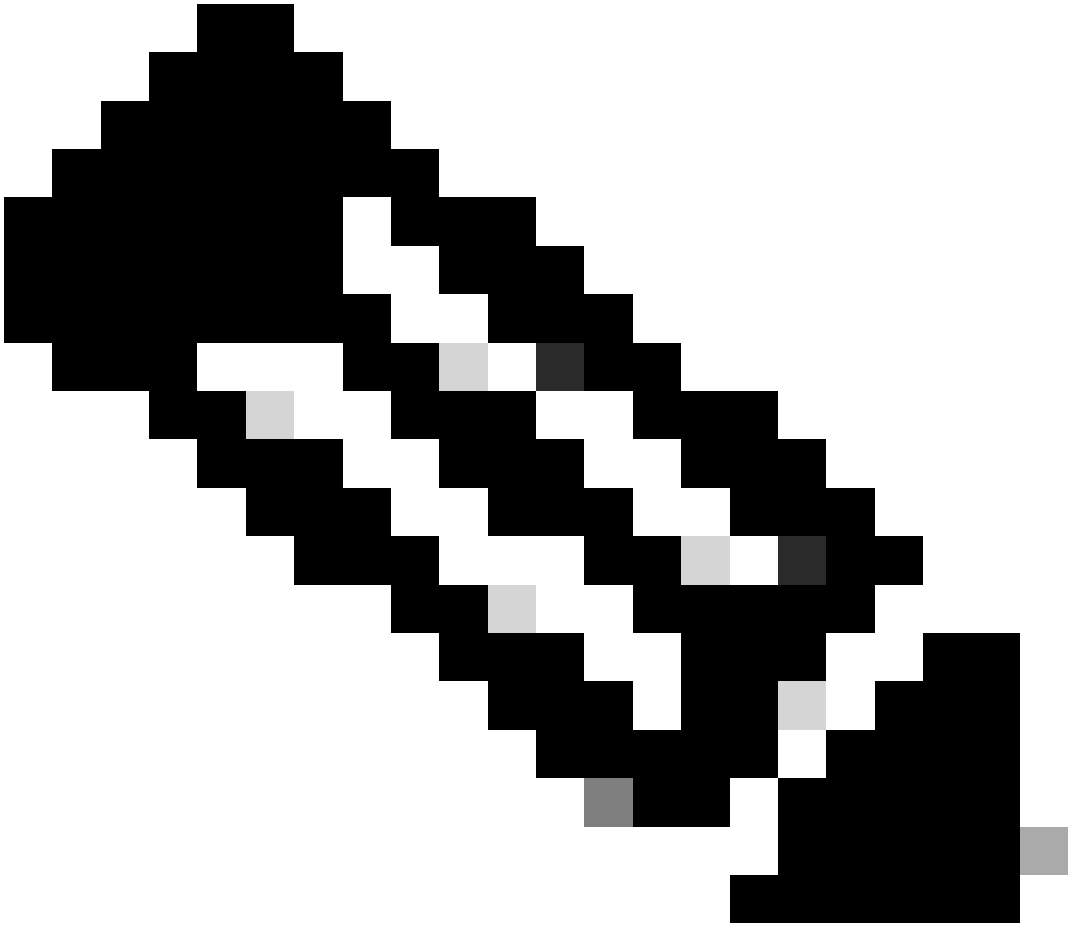
ℹ Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

```
office365_outbound: if sendergroup == "RELAYLIST" {
if header("X-OUTBOUND-AUTH") == "^mysecretkey$" {
strip-header("X-OUTBOUND-AUTH");
} else {
drop();
}
}
```

- Appuyez une fois sur Return pour créer une nouvelle ligne vide.
- Entrez **[.]** sur la nouvelle ligne pour terminer votre nouveau filtre de messages.
- Cliquez **return** une fois pour quitter le menu Filtres.
- Exécutez la **Commit** commande pour enregistrer les modifications apportées à votre configuration.



Remarque : évitez les caractères spéciaux pour la clé secrète. Les caractères ^ et $ affichés dans le filtre de message sont des caractères regex et sont utilisés comme indiqué dans l'exemple.



Remarque : vérifiez le nom de la configuration de RELAYLIST. Il peut être configuré avec un autre nom ou vous pouvez avoir un nom spécifique basé sur votre stratégie de relais ou votre fournisseur de messagerie.

Tester le courrier sortant

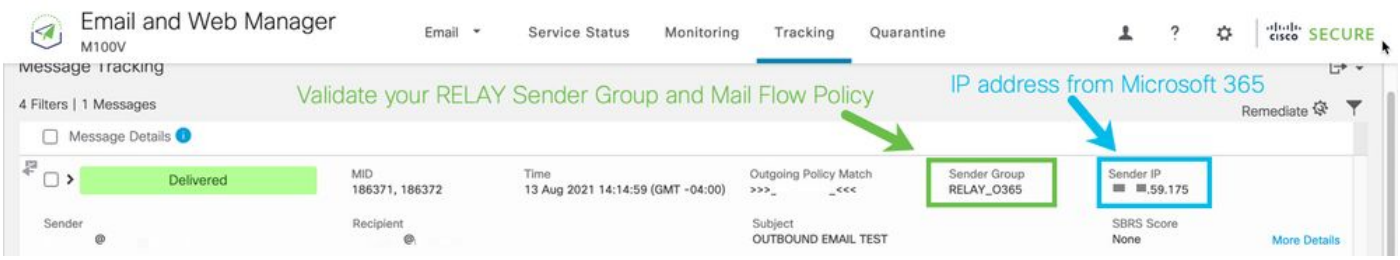
Testez le courrier sortant de votre adresse de messagerie Microsoft 365 vers un destinataire de domaine externe. Vous pouvez vérifier le suivi des messages depuis votre Cisco Secure Email and Web Manager pour vous assurer qu'il est correctement acheminé vers l'extérieur.

Remarque : vérifiez votre configuration TLS (**Administration système > Configuration SSL**) sur le modem routeur et les

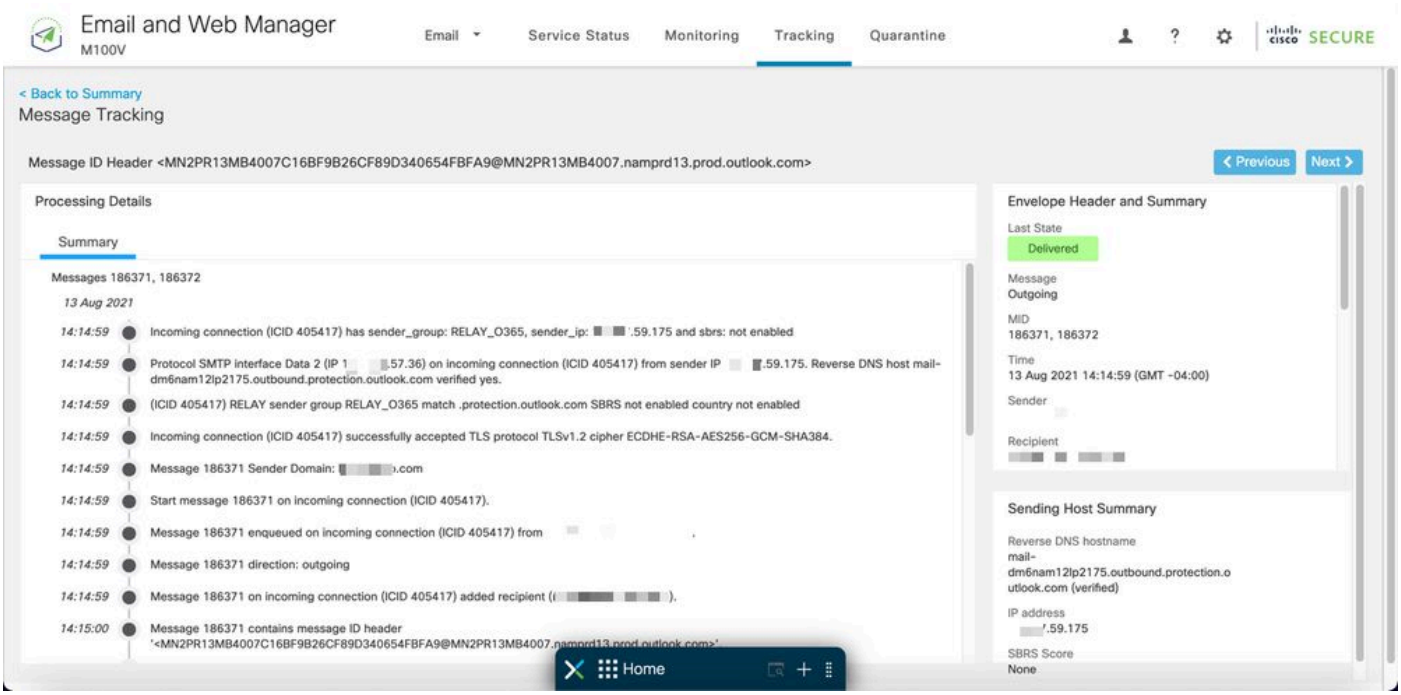
chiffrements utilisés pour le protocole SMTP sortant. Les Méthodes Recommandées de Cisco recommandent :

HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SS

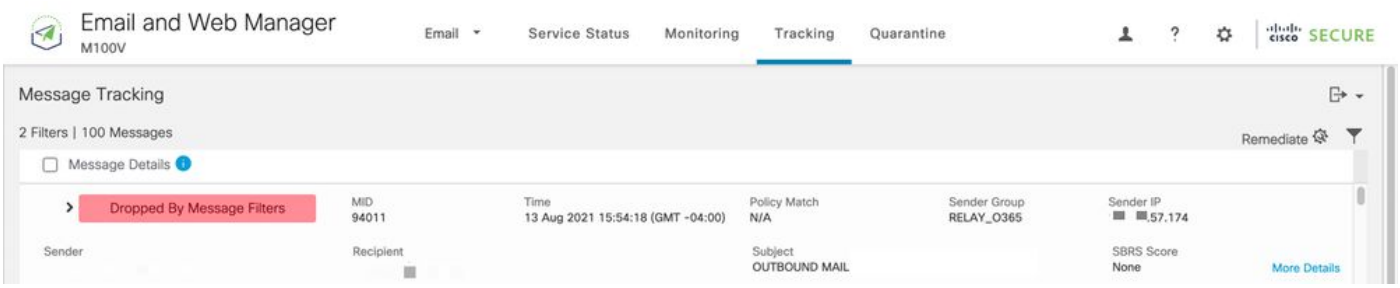
Exemple de suivi avec une livraison réussie :

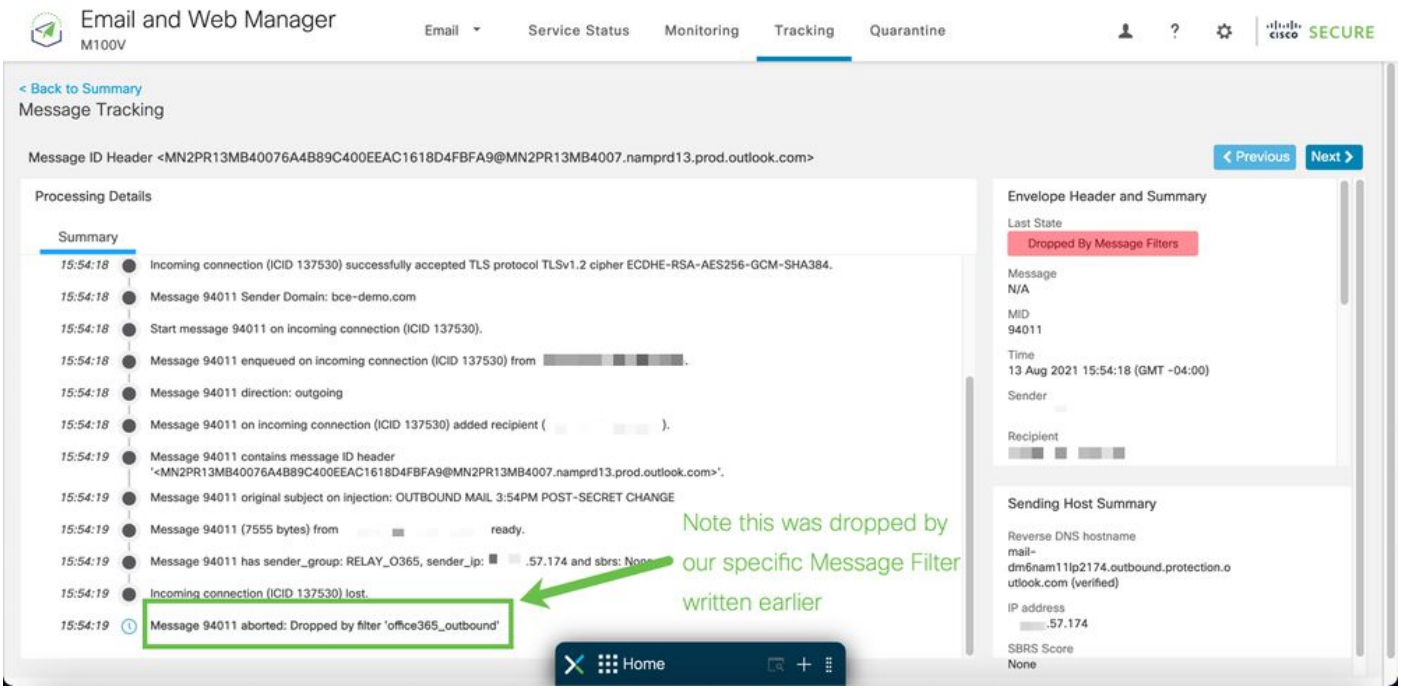


Cliquez ici **More Details** pour afficher les détails complets du message :



Exemple de suivi des messages où l'en-tête x ne concorde pas :





Informations connexes

Documentation de Cisco Secure Email Gateway

- notes de version
- Guide de l’utilisateur
- Guide de référence CLI
- Guides de programmation d'API pour Cisco Secure Email Gateway
- Open Source utilisé dans Cisco Secure Email Gateway
- Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco (inclut vESA)

Documentation sur Secure Email Cloud Gateway

- notes de version
- Guide de l’utilisateur

Documentation de Cisco Secure Email and Web Manager

- Notes de version et matrice de compatibilité

    - Guide de l’utilisateur
- Guides de programmation API pour Cisco Secure Email and Web Manager
- Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco (inclut vSMA)

Documentation sur les produits Cisco Secure

- Architecture d'attribution de noms Cisco Secure

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.