# Configuration de Microsoft 365 avec la messagerie sécurisée

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- 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
    - Connecteur de réception
  - Configurer les courriels de Cisco Secure Email vers Microsoft 365
    - Contrôles de destination
    - Tableau d'accès des destinataires
    - Routes SMTP
    - Configuration DNS (enregistrement MX)
    - Tester le courrier entrant
  - Configurer les courriels sortants de Microsoft 365 vers Cisco Secure Email
    - Configuration de RELAYLIST sur la passerelle de messagerie sécurisée Cisco
    - Activer TLS
    - Configurer la messagerie de Microsoft 365 vers CES
    - Créer une règle de flux de messagerie
    - Empêcher le relais ouvert
    - Option 1: Interdire Open Relay via l'interface utilisateur graphique
    - Option 2: Interdire le relais ouvert via CLI
    - Tester le courrier sortant
- Informations connexes
  - Documentation de Cisco Secure Email Gateway
  - Documentation sur Secure Email Cloud Gateway
  - Documentation de Cisco Secure Email and Web Manager
  - Documentation sur les produits Cisco Secure


## 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.150.143 est l'adresse IP de l'interface Data 1 pour la passerelle 2. L'adresse IP de l'interface Data 2 pour la passerelle 1 est xxx.yy.143.186, et l'adresse IP de l'interface Data 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 obtenir l'interface Data 2 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

1. Connectez-vous au Centre d'administration Microsoft Exchange
2. Dans le menu de gauche, accédez à **Mail flow** > **Rules**.
3. Cliquez sur **Add a rule** pour créer une nouvelle règle.
4. Entrez un nom pour votre nouvelle règle : **Bypass spam filtering - inbound email from Cisco CES**.
5. 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**.
6. Pour *Effectuez les opérations suivantes..., sélectionnez **Modify the message properties** et choisissez l' **set the spam confidence level (SCL)**utilisation **Bypass spam filtering**.
7. Cliquer **Next**.
8. Sélectionnez **Enforce** et cliquez sur Next.
9. ET Finish.

Voici un exemple de l'aspect de votre règle :

# Bypass spam filtering - inbound email from Cisco CES

Edit rule conditions  Edit rule settings

Status: Disabled

**Enable or disable rule**

Disabled

**Rule settings**

**Rule name**

Bypass spam filtering - inbound email from Cisco CES

**Severity**

Not specified

**Senders address**

Matching Header

**For rule processing errors**

Ignore

**Mode**

Enforce

**Set date range**

Specific date range is not set

**Priority**

2

**Rule description**

**Apply this rule if**

*sender ip addresses belong to one of these ranges: '1[redacted] or '1[redacted]' or '1[redacted]'*

**Do the following**

*Set the spam confidence level (SCL) to '-1'*

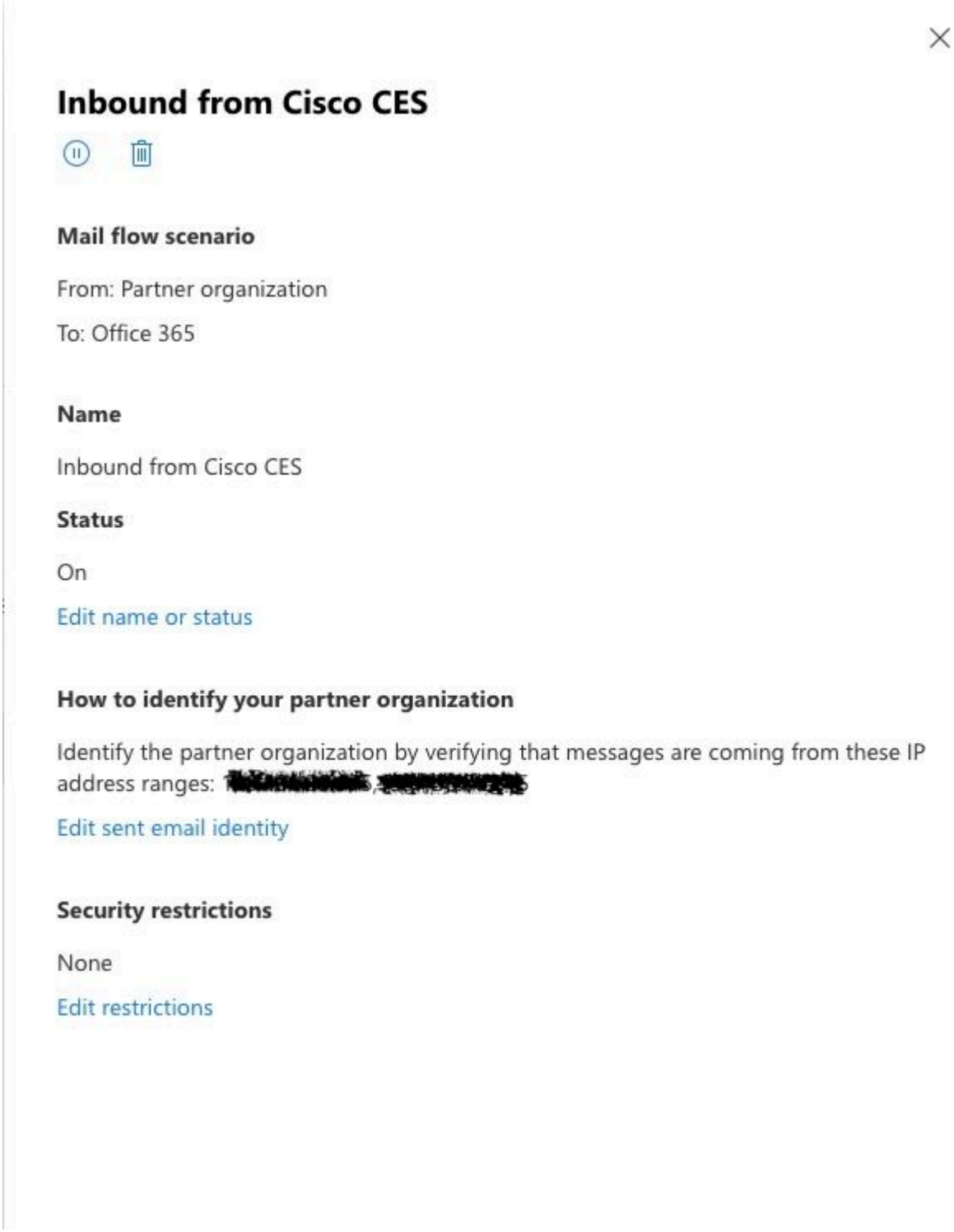
**Rule comments**

Règle de contournement

Connecteur de réception

1. Restez dans le Centre d'administration Exchange.
2. Dans le menu de gauche, accédez à **Mail flow** > **Connectors**.
3. Cliquez sur **[+ Add a connector]** pour créer un nouveau connecteur.
4. Dans la fenêtre contextuelle Sélectionner votre scénario de flux de messagerie, sélectionnez :
    1. From (de) : Partner organization
    2. Par : **Office365**
5. Cliquer **Next**.
6. Entrez un nom pour votre nouveau connecteur : **Inbound from Cisco CES**.
7. Saisissez une description (facultatif).
8. Cliquer **Next**.
9. Sélectionner **By verifying that the IP address of the sending...**
10. Cliquez sur **[+]** et ajoutez les adresses IP fournies dans la lettre de bienvenue et utilisées dans la règle de filtrage Ignorer le spam.
11. Cliquer **Next**.
12. Choisir **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
13. Cliquer **Next**.
14. Cliquer **Save**.

Voici un exemple de la configuration de votre connecteur :




Connecteur entrant

## 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.

1. Connectez-vous à votre modem routeur.
2. Naviguez jusqu'à **Mail Policies** > **Destination Controls**.
3. Cliquer **Add Destination**.
4. Utilisation:
    1. Destination : Entrez votre nom de domaine
    2. Concurrent Connections (connexions simultanées) : **10**
    3. Maximum Messages Per Connection (nombre maximal de messages par connexion) : **20**
    4. TLS Support (soutien TLS) : **Preferred**
5. Cliquer **Submit**.
6. 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 :

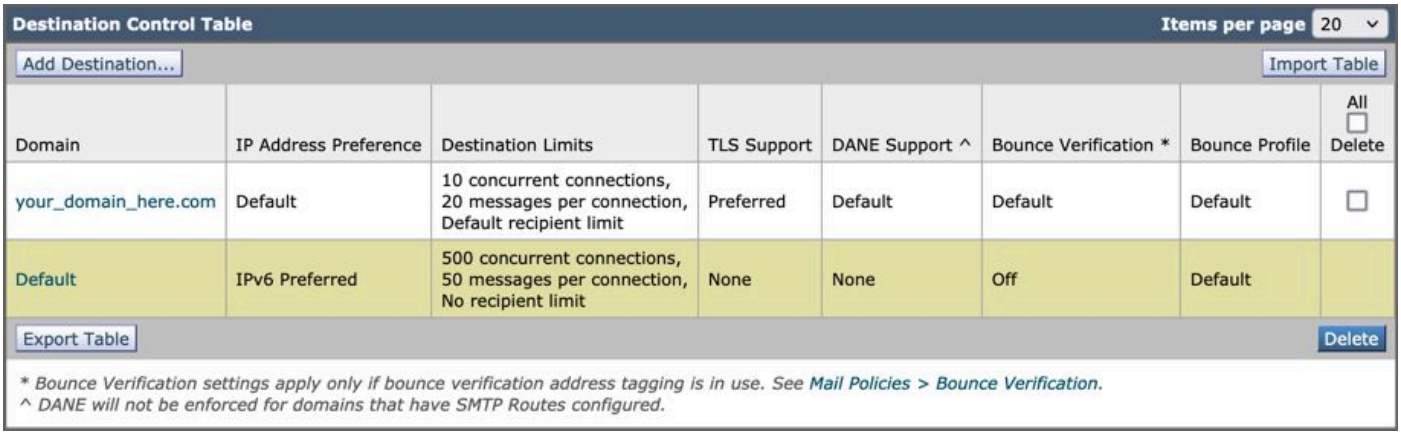



Tableau d’accès des destinataires

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

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

---

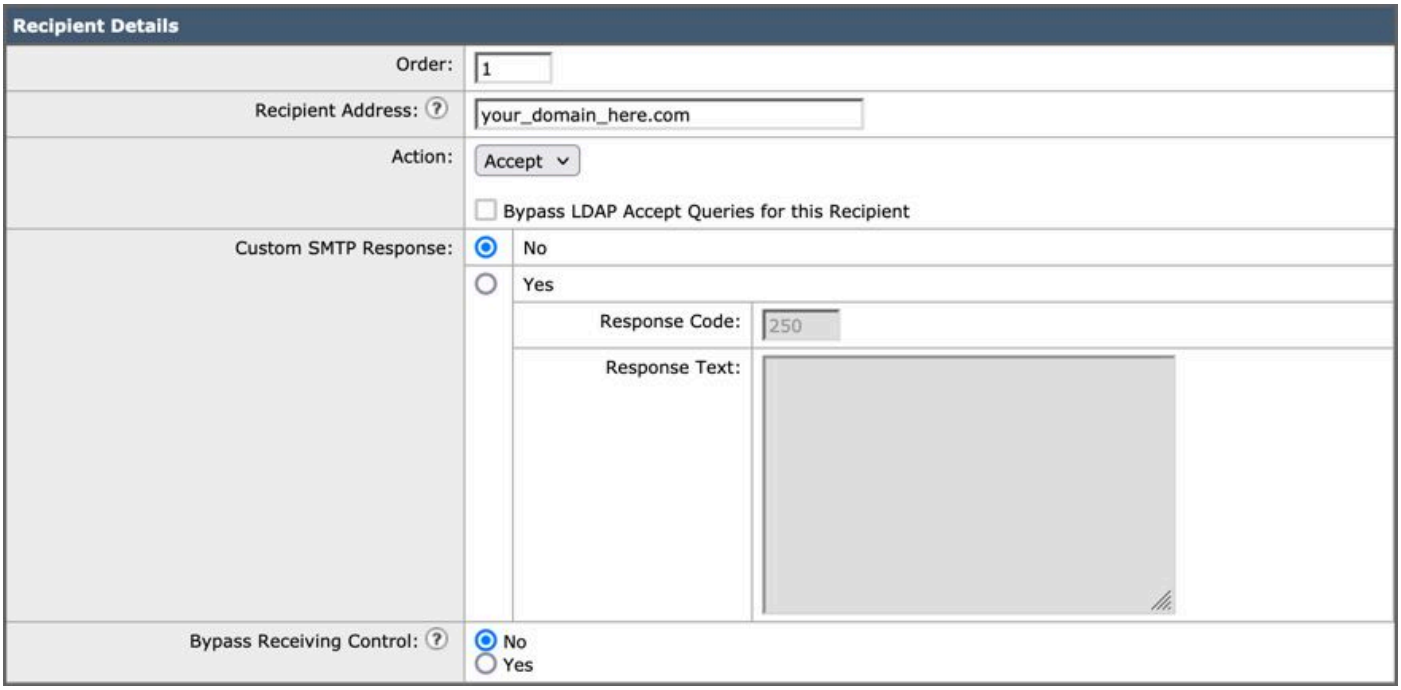
Remarque : Assurez-vous que l'écouteur est destiné à l'écouteur entrant, à IncomingMail ou à MailFlow, en fonction du nom réel de l'écouteur pour votre flux de messagerie principal.

---

1. Cliquer **Add Recipient**.
2. Ajoutez votre ou vos domaines dans le champ Adresse du destinataire.
3. Sélectionnez l'action par défaut de **Accept**.

4. Cliquer **Submit**.
5. Cliquez **Commit Changes** dans le coin supérieur droit de l'interface utilisateur pour enregistrer vos modifications de configuration.

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

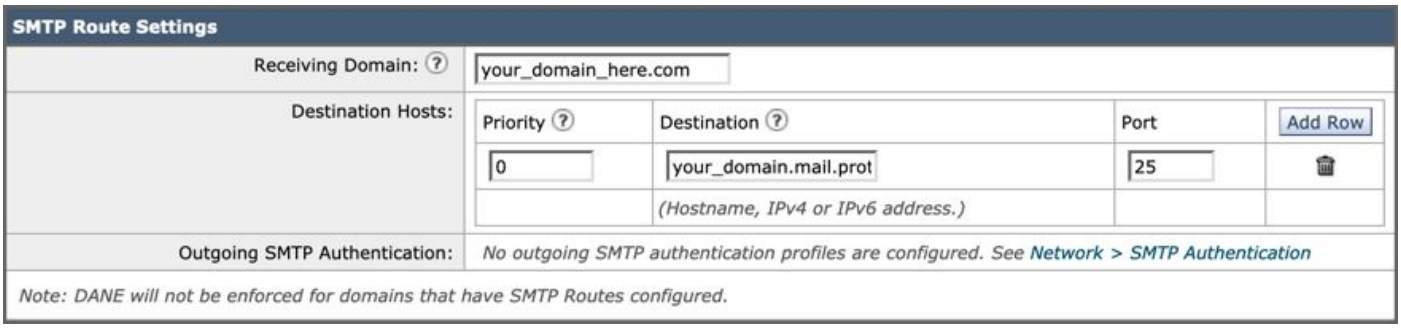



Routes SMTP

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

1. Naviguez jusqu'à **Network** > **SMTP Routes**.
2. Cliquer **Add Route...**
3. Receiving Domain (domaine de réception) : Entrez votre nom de domaine.
4. Destination Hosts (hôtes de destination) : Ajoutez votre enregistrement MX Microsoft 365 d'origine.
5. Cliquer **Submit**.
6. Cliquez **Commit Changes** dans le coin supérieur droit de l'interface utilisateur pour enregistrer vos modifications de configuration.

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



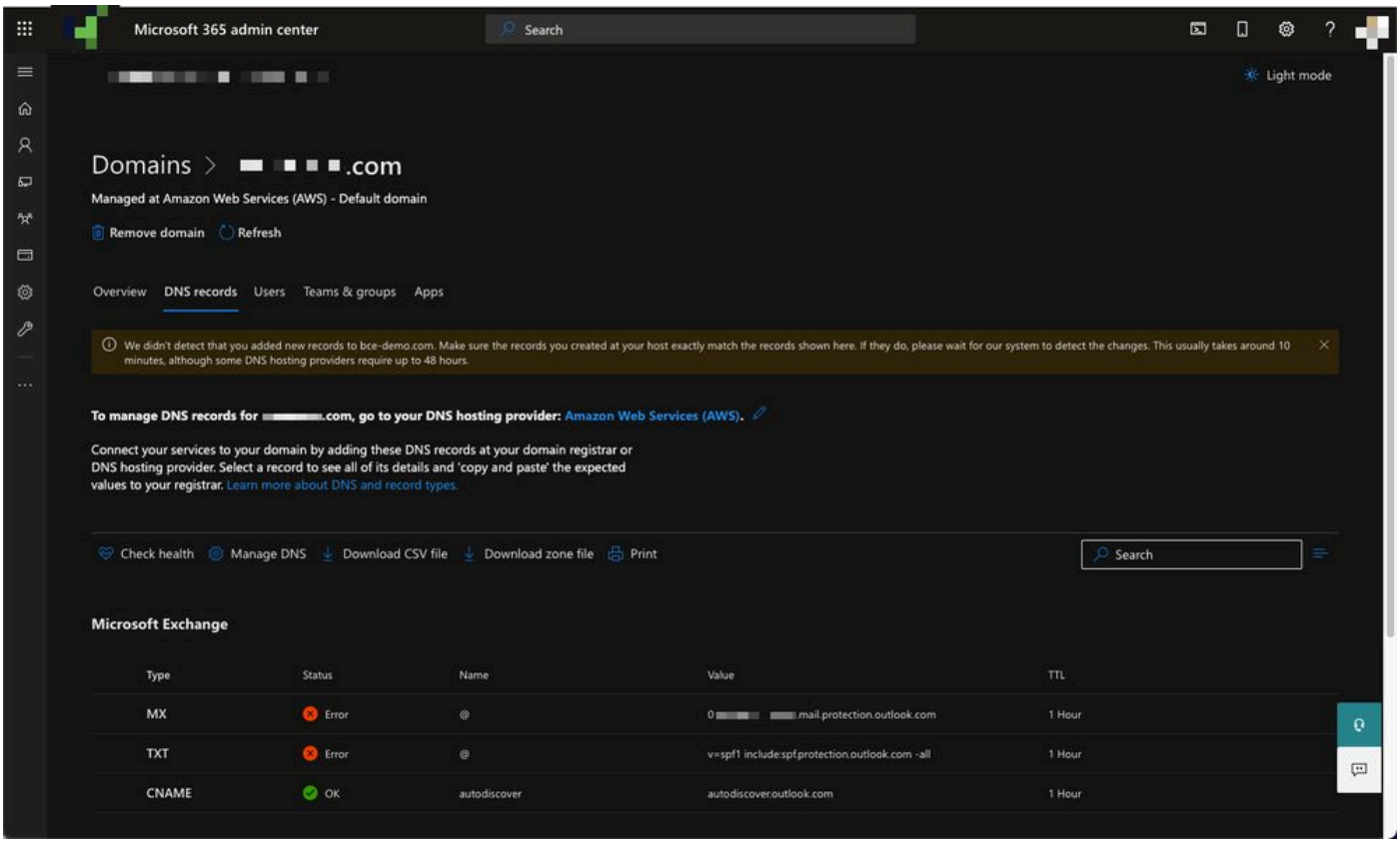

Configuration DNS (enregistrement MX)

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 :

1. Connectez-vous à la console d'administration de Microsoft Office 365.
2. Naviguez jusqu'à **Home** > **Settings** > **Domains**.
3. Choisissez votre nom de domaine par défaut.
4. Cliquer**Check 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

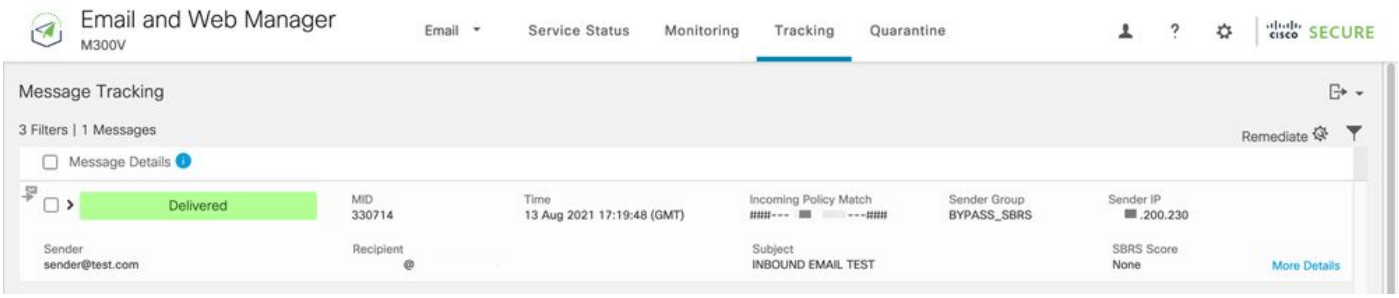
Testez le courrier entrant vers votre adresse de messagerie Microsoft 365. Vérifiez ensuite qu'il arrive dans votre boîte de réception de messagerie Microsoft 365.

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 :

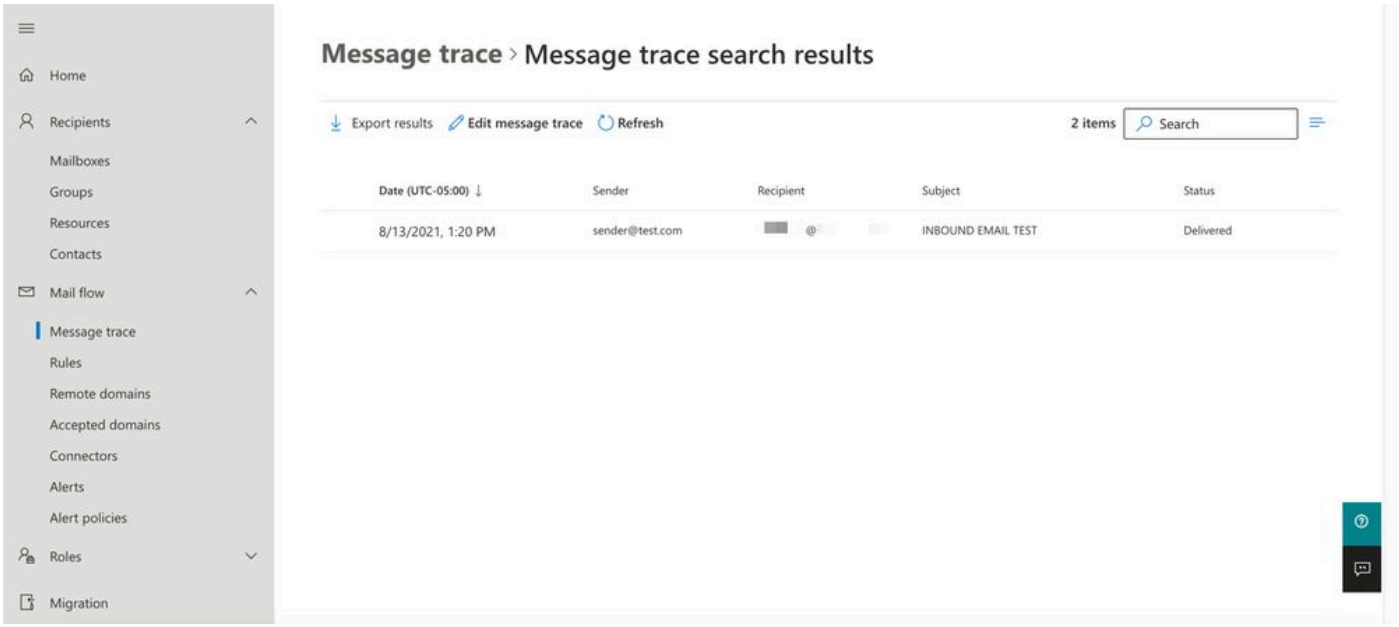
1. Connectez-vous à votre SMA.

2. Cliquer **Tracking**.
3. Saisissez les critères de recherche requis, puis cliquez sur **Search**;et attendez-vous à voir les résultats suivants :




Pour afficher les journaux de messagerie dans Microsoft 365 :

1. Connectez-vous au Centre d'administration Microsoft Exchange.
2. Naviguez jusqu'à **Mail flow** > **Message Trace**.
3. 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.
4. 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

### Configuration de RELAYLIST sur la passerelle de messagerie sécurisée Cisco

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.

1. Connectez-vous à votre modem routeur.
2. Naviguez jusqu'à **Mail Policies** > **HAT Overview**.

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

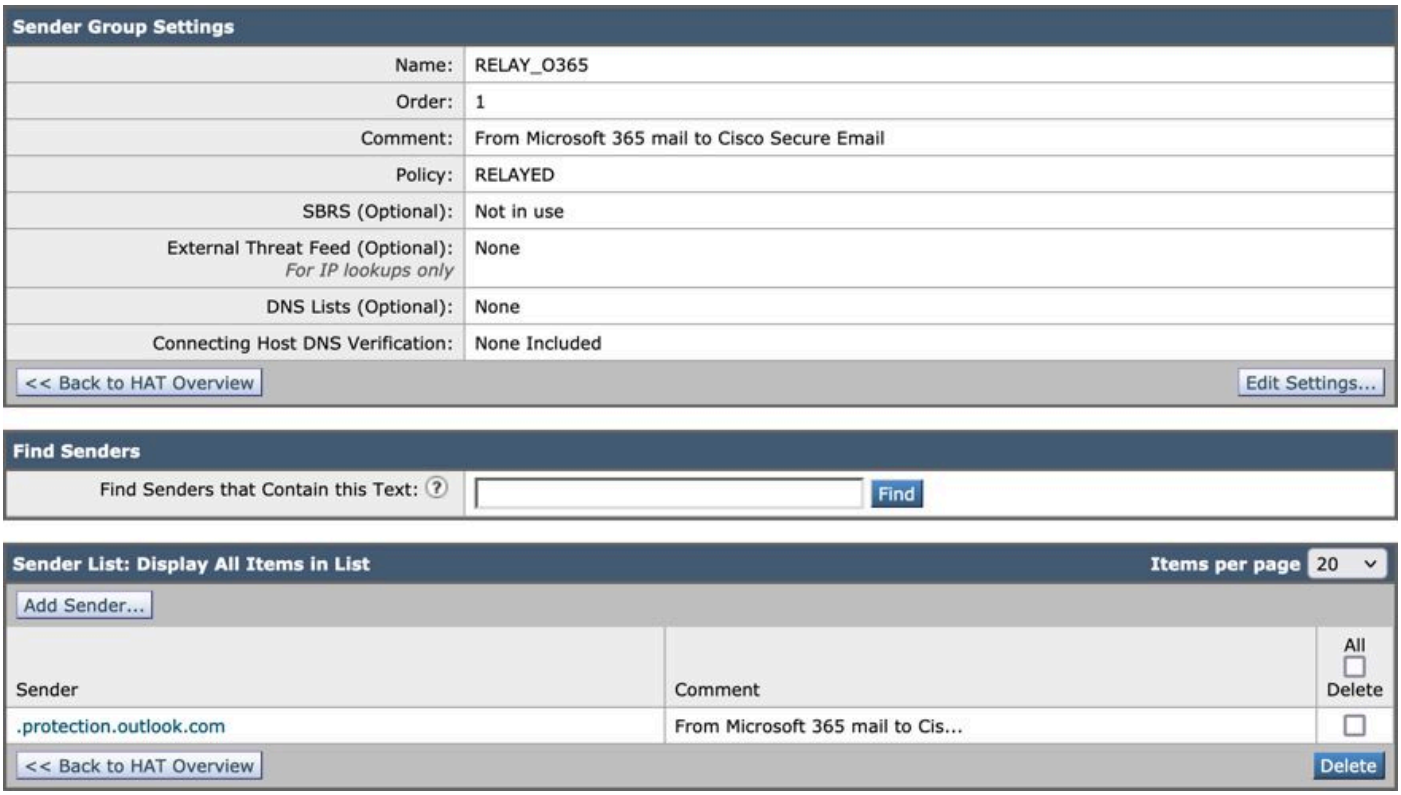
3. Cliquer **Add Sender Group...**
4. Configurez le groupe d'expéditeurs comme suit :
   1. Name : RELAY_O365
   2. Commentaire : **<<**saisissez un commentaire si vous souhaitez noter votre groupe d'expéditeurs**>>**
   3. Policy (politique) : RELAYED (relayée)
   4. Cliquer **Submit and Add Senders**.
   5. Expéditeur : **.protection.outlook.com**.

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

   6. Cliquer **Submit**.
   7. Cliquez **Commit Changes** dans le coin supérieur droit 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

1. Cliquer <

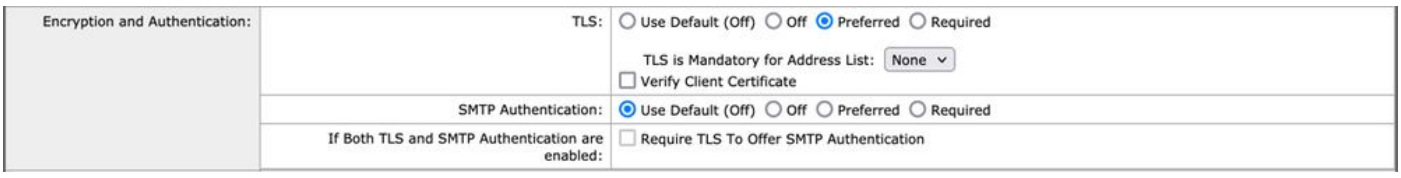
   < **trong**="">

   .

   <>

   - Cliquez sur la politique de flux de messagerie nommée : **RELAYED**.
   - Faites défiler la page vers le bas et recherchez dans la **Security Features** section **Encryption and Authentication**.
   - Pour TLS, sélectionnez : **Preferred**.
   - Cliquer **Submit**.
   - Cliquez **Commit Changes** dans le coin supérieur droit 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

1. Connectez-vous au Centre d'administration Microsoft Exchange.
2. Accédez à **Mail flow** > **Connectors.**
3. Cliquez sur[+ Add a connetor]pour créer un nouveau connecteur.
4. Dans la fenêtre contextuelle Sélectionner votre scénario de flux de messagerie, sélectionnez :
    1. From (de) : Office365
    2. Par :Partner organization
5. Cliquer **Next**.
6. Entrez un nom pour votre nouveau connecteur : **Outbound to Cisco CES**.
7. Saisissez une description (facultatif).
8. Cliquer **Next**.
9. Pour « Quand voulez-vous utiliser ce connecteur ? » :
    1. Choisissez : **Only when I have a transport rule set up that redirects messages to this connector**.
    2. Cliquer **Next**.
10. Cliquer **Route email through these smart hosts**.
11. Cliquez sur **[+]** et entrez les adresses IP sortantes ou les noms d'hôte fournis dans votre lettre de bienvenue CES.
12. Cliquer **Save**.
13. Cliquer **Next**.
14. Pour « Comment Office 365 se connecte-t-il au serveur de messagerie de votre organisation partenaire ? » :
    1. Choisissez : **Always use TLS to secure the connection (recommended)**.
    2. ChoisirAny digital certificate, including self-signed certificates.
    3. Cliquer **Next**.
15. L'écran de confirmation s'affiche.
16. Cliquer **Next**.
17. Utilisez **[+]** pour saisir une adresse e-mail valide et cliquez sur **OK**.
18. Cliquez sur **Validate** et autorisez l'exécution de la validation.
19. Une fois terminé, cliquez sur
20. 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. Connectez-vous à votre Centre d'administration Exchange.
2. Cliquez sur **Mail Flow**;l'onglet Règles et assurez-vous qu'il est actif.
3. Cliquez sur **[+]** pour ajouter une nouvelle règle.
4. Choisir **Create a new rule**.
5. Entrez un nom pour votre nouvelle règle : **Outbound to Cisco CES**.
6. Pour *Appliquer cette règle si..., choisissez : **The sender is located...**
    1. Pour la fenêtre contextuelle Sélectionner l'emplacement de l'expéditeur, sélectionnez : **Inside the organization**.
    2. Cliquer **OK**.
7. Cliquer **More options...**
8. Cliquez sur le **add condition** bouton et insérez une deuxième condition :
    1. Choisir **The recipient...**
    2. Choisissez : **Is external/internal**.
    3. Pour la fenêtre contextuelle Sélectionner l'emplacement de l'expéditeur, sélectionnez : **Outside the organization**.
    4. Cliquer **OK**.
9. 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.
10. Revenir à "*Effectuez les opérations suivantes..." et insérez une deuxième action :
    1. Choisissez : **Modify the message properties...**
    2. Choisissez : **set the message header**.
    3. Définissez l'en-tête du message : **X-OUTBOUND-AUTH**.
    4. Cliquer **OK**.
    5. Définissez la valeur : **mysecretkey**.
        1. **mysecretkey** is simply a placeholder. Please customize this so it is specific to your environment.
    6. Cliquer **OK**.
11. 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 sa livraison 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

Empêcher le relais ouvert

---



Avertissement : Il s'agit d'une étape cruciale. La sécurisation de l'écouteur sortant est essentielle pour empêcher les utilisateurs non autorisés de relayer des e-mails via le périphérique.

---

Deux options sont répertoriées ci-dessous. Il est recommandé d'utiliser le filtre de message (CLI) ou le filtre de contenu (GUI) pour les personnes moins familières avec CLI (Command Line Interface).

Option 1: Interdire Open Relay via l'interface utilisateur graphique

Créez deux filtres de contenu dans l'interface utilisateur graphique :

- Le premier filtre agit sur tous les e-mails qui n'ont pas l'en-tête X-OUTBOUND-AUTH ou qui ne contiennent pas la valeur précédemment configurée dans Microsoft Office 365.
- Le deuxième filtre s'applique aux e-mails légitimes envoyés à partir du service partagé Microsoft Office 365. Ce filtre supprime l'en-tête X-OUTBOUND-AUTH afin qu'il ne puisse pas être utilisé à mauvais escient à l'avenir.

1. Dans l'interface graphique utilisateur, accédez à Politiques de messagerie >> Filtres de contenu sortant >> sélectionnez Stop_O365_OpenRelay (sélectionnez Ajouter un filtre... si ce n'est pas disponible).
2. Assurez-vous que le premier filtre de contenu est configuré :
    - Name : <cela peut être n'importe quoi>
    - Description: <cela peut être n'importe quoi>
    - Appliquer la règle : Uniquement si toutes les conditions correspondent
    - Conditions
        - Autre en-tête :
            - Nom d'en-tête : <Entrez le nom d'en-tête précédemment indiqué lors de la création de la règle de flux de messagerie sur Microsoft Office 365) (par exemple, **X-OUTBOUND-AUTH)**.
                - Certains clients peuvent avoir cette configuration prédéfinie en utilisant une valeur d'en-tête de X-IronPort-Tenant. Bien que cela puisse également être utilisé, la partie cruciale consiste simplement à s'assurer que la valeur d'en-tête entrée dans la condition de filtre de contenu correspond à la valeur d'en-tête qui a été configurée dans la règle de flux de messagerie sur Microsoft Office 365.
            - Valeur d'en-tête (différente) : <Entrez la valeur de l'en-tête précédemment répertorié lors de la création de la règle de flux de messagerie sur Microsoft

Office 365 (telle que mysecretkey).
    - Écouteur De Réception (Is) : Sortant
- Actions
    - Ajouter une entrée de journal : $Header["X-OUTBOUND-AUTH"]
        - Certains clients peuvent avoir cette configuration prédéfinie en utilisant une valeur d'en-tête de X-IronPort-Tenant. Bien que cette option puisse également être utilisée, la partie essentielle consiste à s'assurer que la valeur d'en-tête entrée dans la condition Filtre de contenu correspond à la valeur d'en-tête configurée dans la règle de flux de courrier sur Microsoft Office 365.
    - Quarantaine : <sélectionner la quarantaine correspondante>
- Évitez d'utiliser des caractères spéciaux autres que ceux répertoriés précédemment (tels que *, (, |, etc.), car ils peuvent provoquer des correspondances faussement positives et entraîner la mise en quarantaine des e-mails légitimes.
- Cliquez sur Submit.

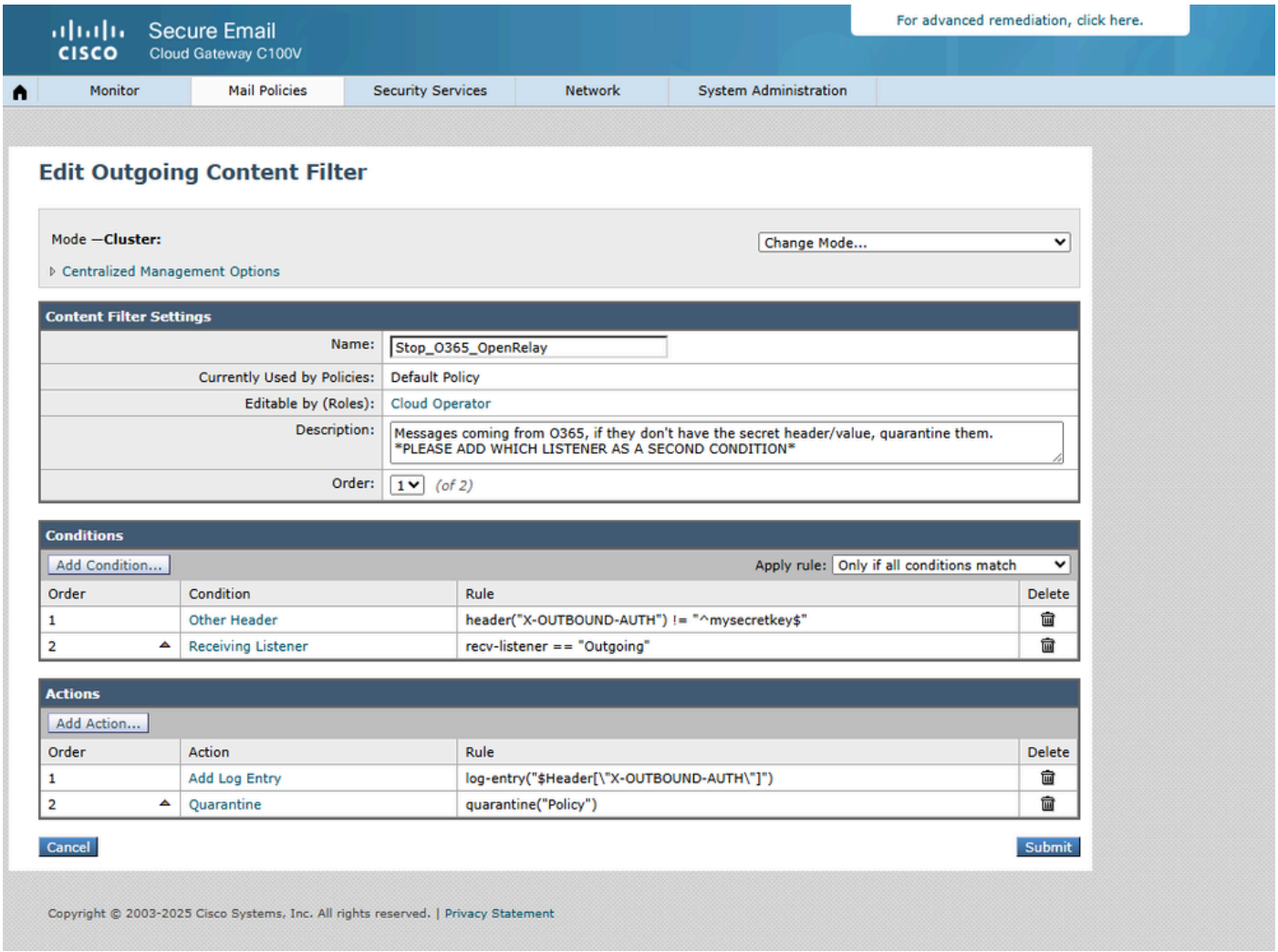
3. Ensuite, sélectionnez le filtre de contenu Strip_Secret_Header et configurez : (sélectionnez Ajouter un filtre... si non disponible) :
    - Name : <cela peut être n'importe quoi>
    - Description: <cela peut être n'importe quoi>
    - Conditions
        - Autre en-tête :
            - Nom d'en-tête : <Entrez le nom d'en-tête précédemment indiqué lors de la création de la règle de flux de messagerie sur Microsoft Office 365) (par exemple, **X-OUTBOUND-AUTH)**.
                - Certains clients peuvent avoir cette configuration prédéfinie en utilisant une valeur d'en-tête de X-IronPort-Tenant. Bien que cette option puisse également être utilisée, la partie essentielle consiste à s'assurer que la valeur d'en-tête entrée dans la condition Filtre de contenu correspond à la valeur d'en-tête configurée dans la règle de flux de courrier sur Microsoft Office 365.
            - Valeur d'en-tête (Égal à) : <Entrez la valeur de l'en-tête précédemment répertorié lors de la création de la règle de flux de messagerie sur Microsoft Office 365 (telle que mysecretkey).
    - Actions
        - En-Tête De Bande
            - Nom d'en-tête : <Entrez le nom d'en-tête précédemment indiqué lors de la création de la règle de flux de messagerie sur Microsoft Office 365) (par exemple, **X-OUTBOUND-AUTH**).
                - Certains clients peuvent avoir cette configuration prédéfinie en utilisant une valeur d'en-tête de X-IronPort-Tenant. Bien que cela puisse également être utilisé, la partie cruciale est simplement de s'assurer que la valeur d'en-tête entrée dans la condition de filtre de contenu correspond à la valeur d'en-tête qui a été configurée dans la règle de flux de courrier sur Microsoft Office 365.
                - Cliquez sur Submit, puis accédez à Politiques de messagerie >> Politiques de messagerie sortante.

4. Assurez-vous que les filtres de contenu nouvellement créés sont maintenant activés sous la stratégie par défaut, et toute autre stratégie requise.
    - Assurez-vous que le filtre de contenu Strip_Secret_Header est dans le bon ordre sur la ou les stratégies de messagerie. Il doit être placé après le filtre de contenu Stop_O365_OpenRelay, sinon vous risquez d'avoir un impact sur le flux de messagerie et/ou les filtres de contenu risquent de ne pas fonctionner comme prévu.
5. Envoyer >> Valider vos modifications.
6. Testez le trafic de vos e-mails sortants.

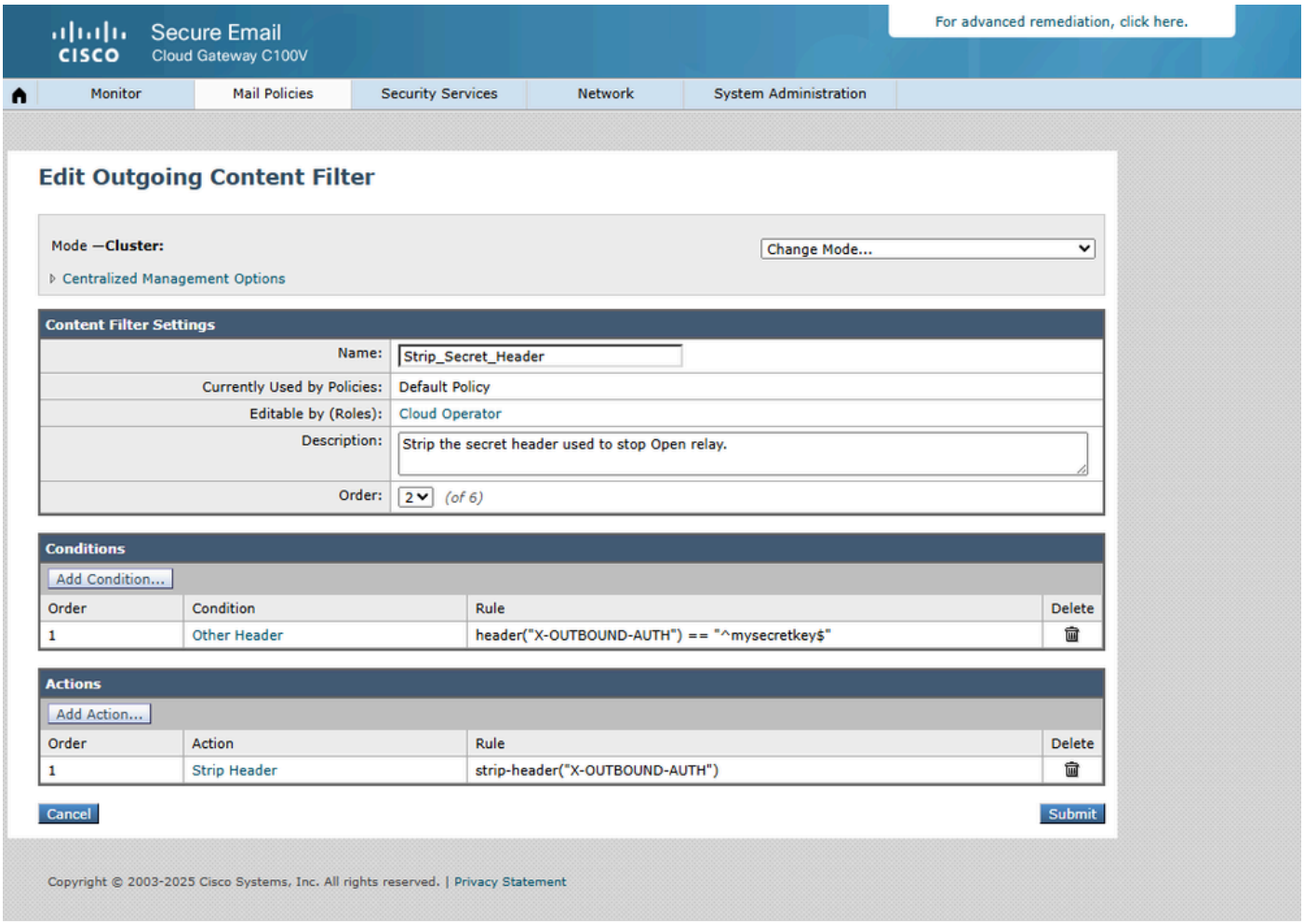
---

Conseil : Une fois que vos tests se sont terminés avec succès et que la remise du courrier fonctionne comme prévu, il est recommandé de remplacer l'action « quarantaine » du filtre de contenu par « abandonner ».

---




Stop_O365_Filtre de contenu OpenRelay




Filtre de contenu Strip_Secret_Header

Option 2: Interdire le relais ouvert via CLI

Accédez à l'interface CLI de votre passerelle de messagerie sécurisée Cisco.

---

Remarque : Cisco Secure Email Cloud Gateway > Command Line Interface (CLI) Access.

---

Créez un filtre de message pour vérifier la présence et la valeur de l'en-tête x et supprimez l'en-tête s'il existe. En l'absence d'en-tête, supprimez le message.

1. Connectez-vous à votre modem routeur via l'interface de ligne de commande.
2. Exécutez la commande . **filters**
3. Si votre modem routeur est en cluster, appuyez sur return pour modifier les filtres en mode Cluster.
4. Utilisez la **New** commande suivante pour créer un filtre de message, le copier et le coller :

```
office365_outbound: if sendergroup == "RELAYLIST" {
```

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

5. Appuyez une fois sur return pour créer une nouvelle ligne vide.
6. Entrez [.] sur la nouvelle ligne pour terminer votre nouveau filtre de messages.
7. Cliquez **return** une fois pour quitter le menu Filtres.
8. 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 votre 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.

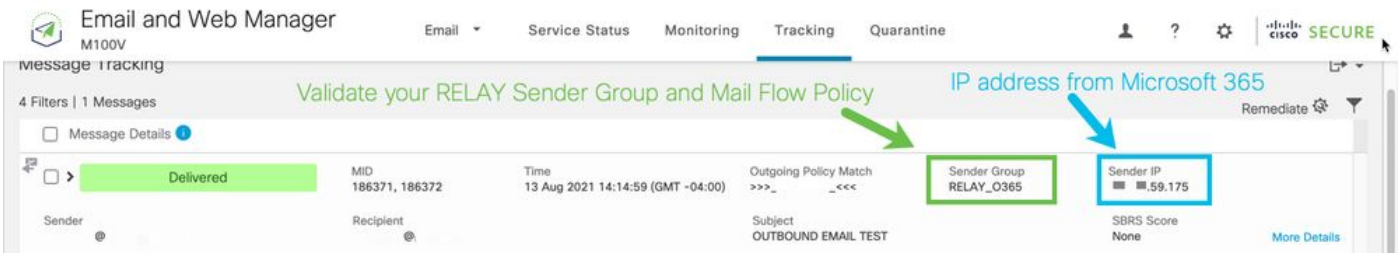
---

Remarque : Vérifiez votre configuration TLS (Administration système > Configuration SSL) sur le modem routeur et les chiffrements utilisés pour le protocole SMTP sortant. Les meilleures pratiques Cisco recommandent :

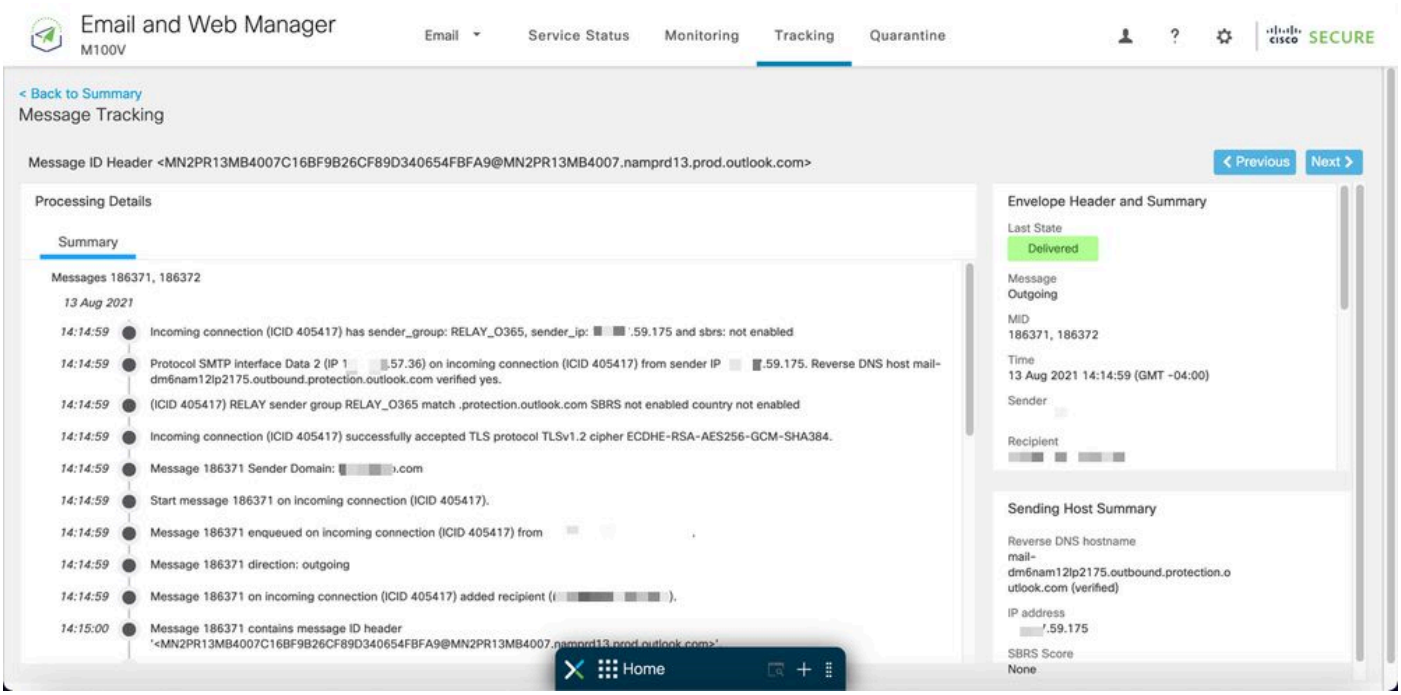
---

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

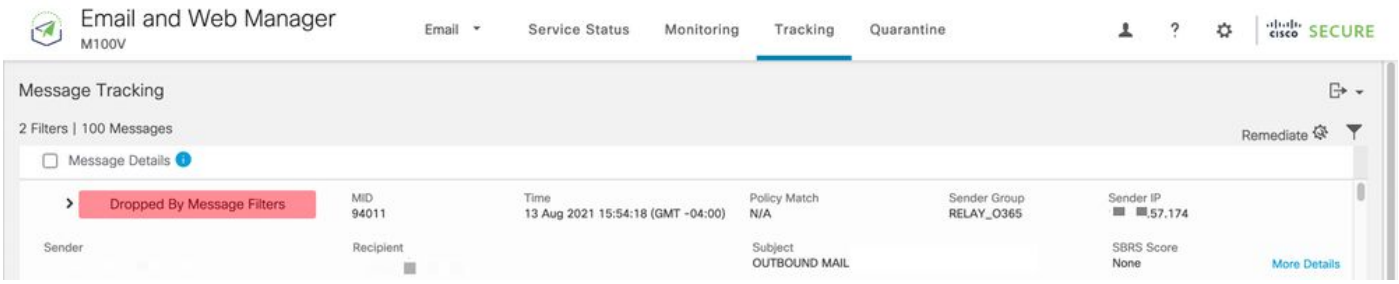
Exemple de suivi avec une livraison réussie :

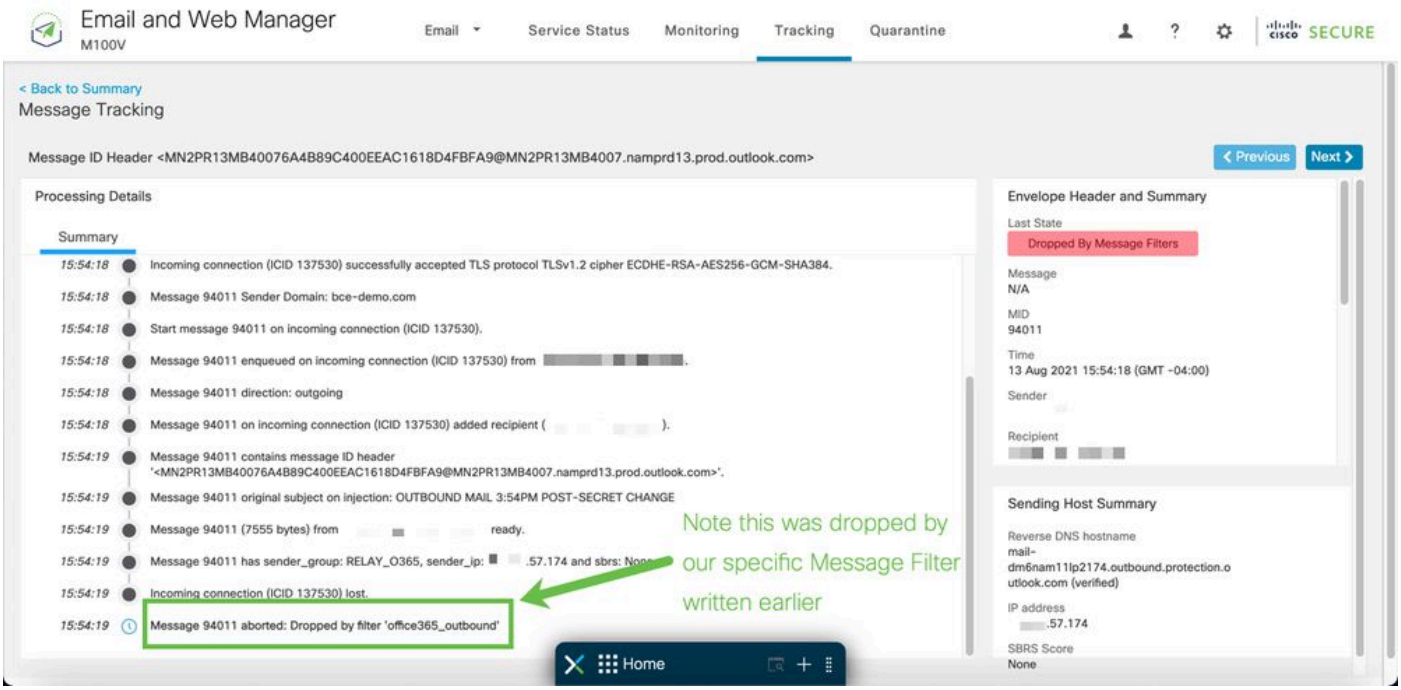



**More Details**Cliquez pour afficher les détails complets du message :




Exemple de suivi des messages où l'en-tête x ne correspond 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 Portfolio

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.