Configurar o Microsoft 365 com Secure Email

Contents

Introdução

Este documento descreve as etapas de configuração para integrar o Microsoft 365 com o Cisco Secure Email para entrega de e-mail de entrada e saída.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Email Gateway ou Cloud Gateway
- Acesso à interface de linha de comando (CLI) para seu ambiente Cisco Secure Email Cloud

Gateway:
Cisco Secure Email Cloud Gateway > Acesso à Interface de Linha de Comando (CLI)
- Microsoft 365
- SMTP (Simple Mail Transfer Protocol)
- Servidor de Nomes de Domínio ou Sistema de Nomes de Domínio (DNS)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento pode ser usado para gateways locais ou gateways de nuvem da Cisco.

Se você for um administrador do Cisco Secure Email, sua carta de boas-vindas incluirá seus endereços IP do gateway de nuvem e outras informações pertinentes. Além da carta que você vê aqui, um e-mail criptografado é enviado para você, fornecendo detalhes adicionais sobre o número de Gateway de nuvem (também conhecido como ESA) e Gerenciador de e-mail e Web de nuvem (também conhecido como SMA) provisionados para sua alocação. Se você não recebeu ou não tem uma cópia da carta, entre em contato ces-activations@cisco.com com suas informações de contato e o nome de domínio em serviço.

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

Cada cliente tem IPs dedicados. Você pode usar os IPs ou nomes de host atribuídos na configuração do Microsoft 365.

Observação: é altamente recomendável testar antes de qualquer transição de e-mail de produção planejada, pois as configurações levam tempo para serem replicadas no console do Microsoft 365 Exchange. No mínimo, aguarde uma hora para que todas as alterações entrem em vigor.

Observação: os endereços IP na captura de tela são proporcionais ao número de gateways de nuvem provisionados para sua alocação. Por exemplo, xxx.yy.140.105 é o endereço IP da interface Data 1 para o Gateway 1 e xxx.yy.150.1143 é o endereço IP da interface Data 1 para o Gateway 2. O endereço IP da interface dos Dados 2 para o Gateway 1 é xxx.yy.143.186 1 e o endereço IP da interface dos Dados 2 para o Gateway 2 é xxx.yy.32.98. Se sua carta de boas-vindas não incluir informações para Dados 2 (IPs de interface de saída), entre em contato com o TAC da Cisco para adicionar a interface de Dados 2 à sua alocação.

Configurar o Microsoft 365 com Secure Email

Configurar e-mail de entrada do Microsoft 365 no Cisco Secure Email

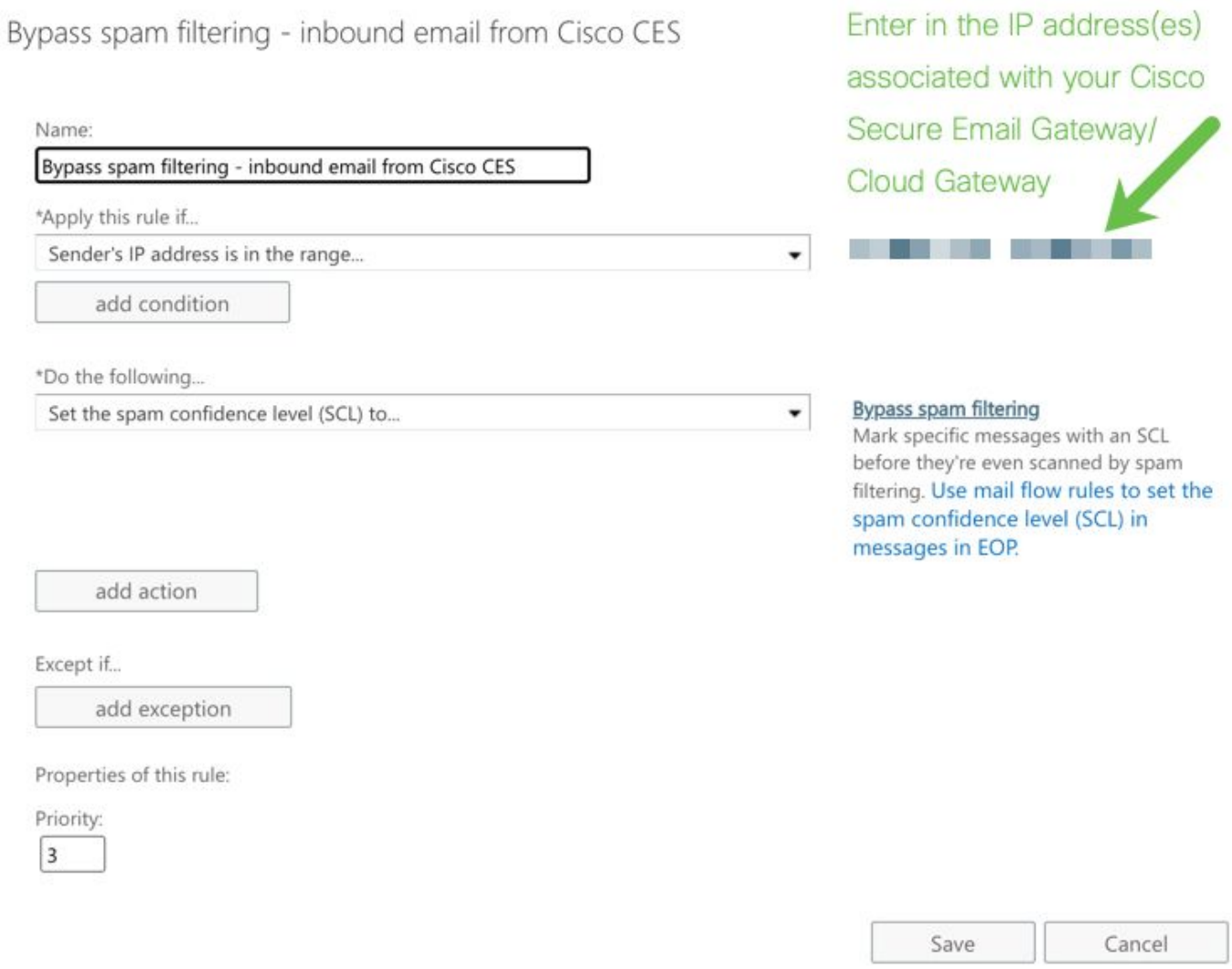
Ignorar regra de filtragem de spam

- Faça login no Microsoft 365 Admin Center (https://portal.microsoft.com).
- No menu à esquerda, expanda **Admin Centers**.
- Clique em **Exchange**.
- No menu à esquerda, navegue até **Mail flow > Rules**.
- Clique **[+]** para criar uma nova regra.
- Escolha **Bypass spam filtering...** na lista suspensa.
- Digite um nome para a nova regra: **Bypass spam filtering - inbound email from Cisco CES**.
- Para *Aplicar esta regra se..., escolha **The sender - IP address is in any of these ranges or exactly matches**.

1. Para a janela pop-up especificar intervalos de endereços IP, adicione os endereços IP fornecidos na carta de boas-vindas do Cisco Secure Email.
2. Clique em **OK**.

- Para *Fazer o seguinte..., a nova regra foi pré-selecionada: **Set the spam confidence level (SCL) to... - Bypass spam filtering**.
- Clique em **Save**.

Um exemplo de como sua regra se parece:



Conector de recebimento

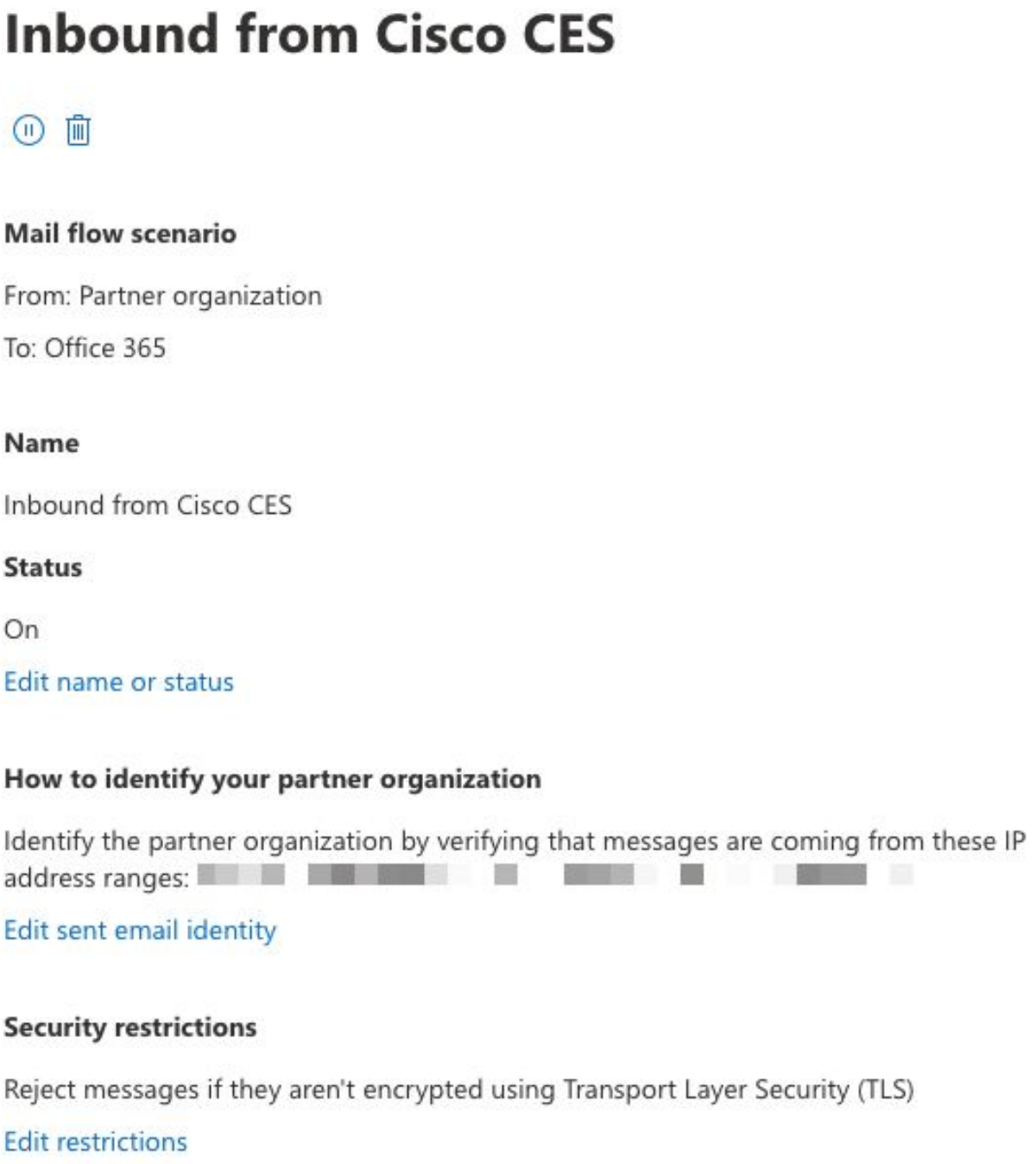
- Permanecer no Exchange Admin Center.
- No menu à esquerda, navegue até **Mail flow > Connectors**.
- Clique **[+]** para criar um novo conector.
- Na janela pop-up Selecionar cenário do fluxo de e-mail, escolha:

1. De: Partner organization

    - Para: **Office365**

- Clique em **Next**.
- Digite um nome para o novo conector: **Inbound from Cisco CES**.
- Insira uma descrição, se desejar.
- Clique em **Next**.
- Clique em **Use the sender's IP address**.
- Clique em **Next**.
- Clique **[+]** e insira os endereços IP indicados na carta de boas-vindas do Cisco Secure Email.
- Clique em **Next**.
- Escolher **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- Clique em **Next**.
- Clique em **Save**.

Um exemplo de como é a configuração do conector:



Configurar e-mail no Cisco Secure Email para o Microsoft 365

Controles de destino

Imponha um acelerador automático para um domínio de entrega nos Controles de destino. É claro que você pode remover o acelerador mais tarde, mas esses são novos IPs para o Microsoft 365, e você não quer nenhum acelerador pela Microsoft devido à sua reputação desconhecida.

- Faça login no Gateway.
- Navegue até **Mail Policies > Destination Controls**.
- Clique em **Add Destination**.

- Uso:

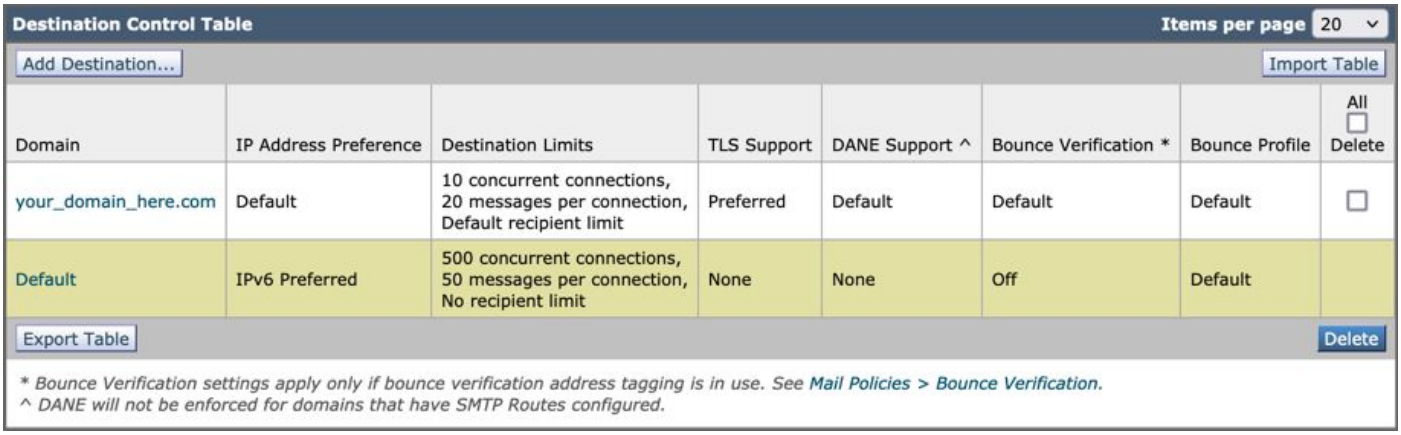
1. Destino: insira seu nome de domínio

2. Conexões simultâneas: **10**

   - Máximo de mensagens por conexão: **20**
   - Suporte TLS: **Preferred**

- Clique em **Submit**.
- Clique **Commit Changes** no canto superior direito da Interface do usuário (UI) para salvar suas alterações de configuração.

Um exemplo de como é a sua Tabela de Controle de Destino:



Destination Control Table — Items per page 20

Add Destination... | Import Table

Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
your_domain_here.com	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Preferred	Default	Default	Default	☐
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	None	Off	Default	

Export Table | Delete

** Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*
^ DANE will not be enforced for domains that have SMTP Routes configured.

Tabela de acesso do destinatário

Em seguida, defina a tabela de acesso do destinatário (RAT) para aceitar e-mails dos domínios:

- Navegue até **Mail Policies > Recipient Access Table (RAT)**.

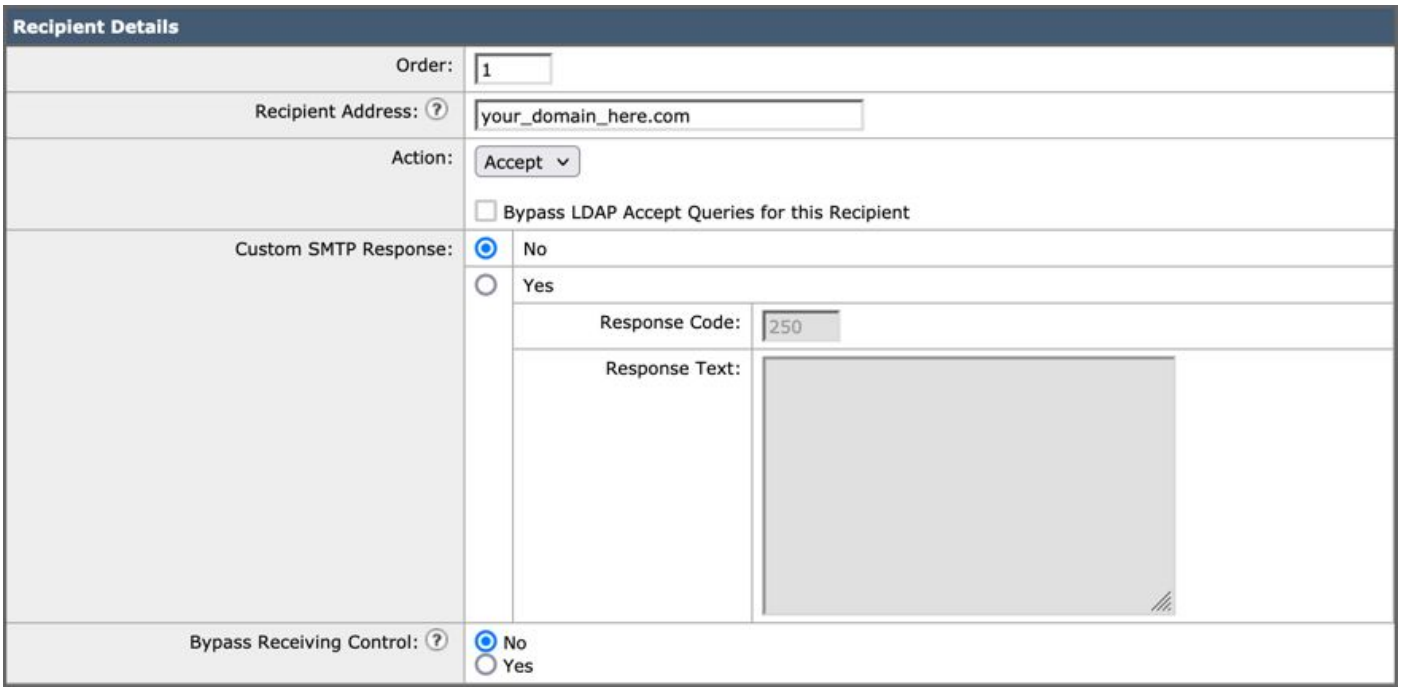
> **Observação**: Certifique-se de que o Listener seja para Listener de Entrada, Correio de Entrada ou Fluxo de Correio, com base no nome real do Listener do seu fluxo de correio principal.

- Clique em **Add Recipient**.
- Adicione os domínios no campo Endereço do destinatário.
- Escolha a ação padrão de **Accept**.

- Clique em **Submit**.

- Clique **Commit Changes** no canto superior direito da interface do usuário para salvar suas alterações de configuração.

Um exemplo de como é a sua entrada RAT:



Rotas SMTP

Defina a rota SMTP para entregar e-mails do Cisco Secure Email ao seu domínio do Microsoft 365:

- Navegue até **Network > SMTP Routes**.

- Clique em **Add Route...**

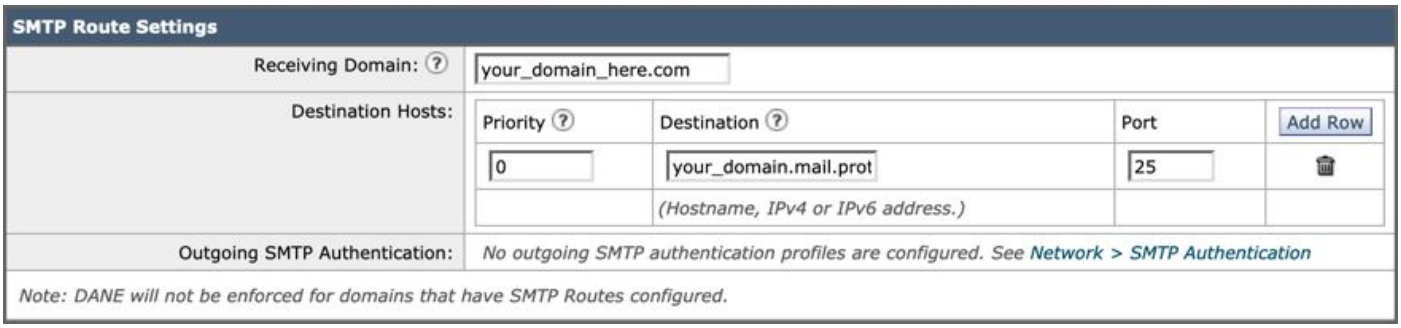
- Domínio de recebimento: insira seu nome de domínio.

- Hosts de destino: adicione seu registro original do Microsoft 365 MX.

- Clique em **Submit**.

- Clique **Commit Changes** no canto superior direito da interface do usuário para salvar suas alterações de configuração.

Um exemplo de como as configurações de rota SMTP são:



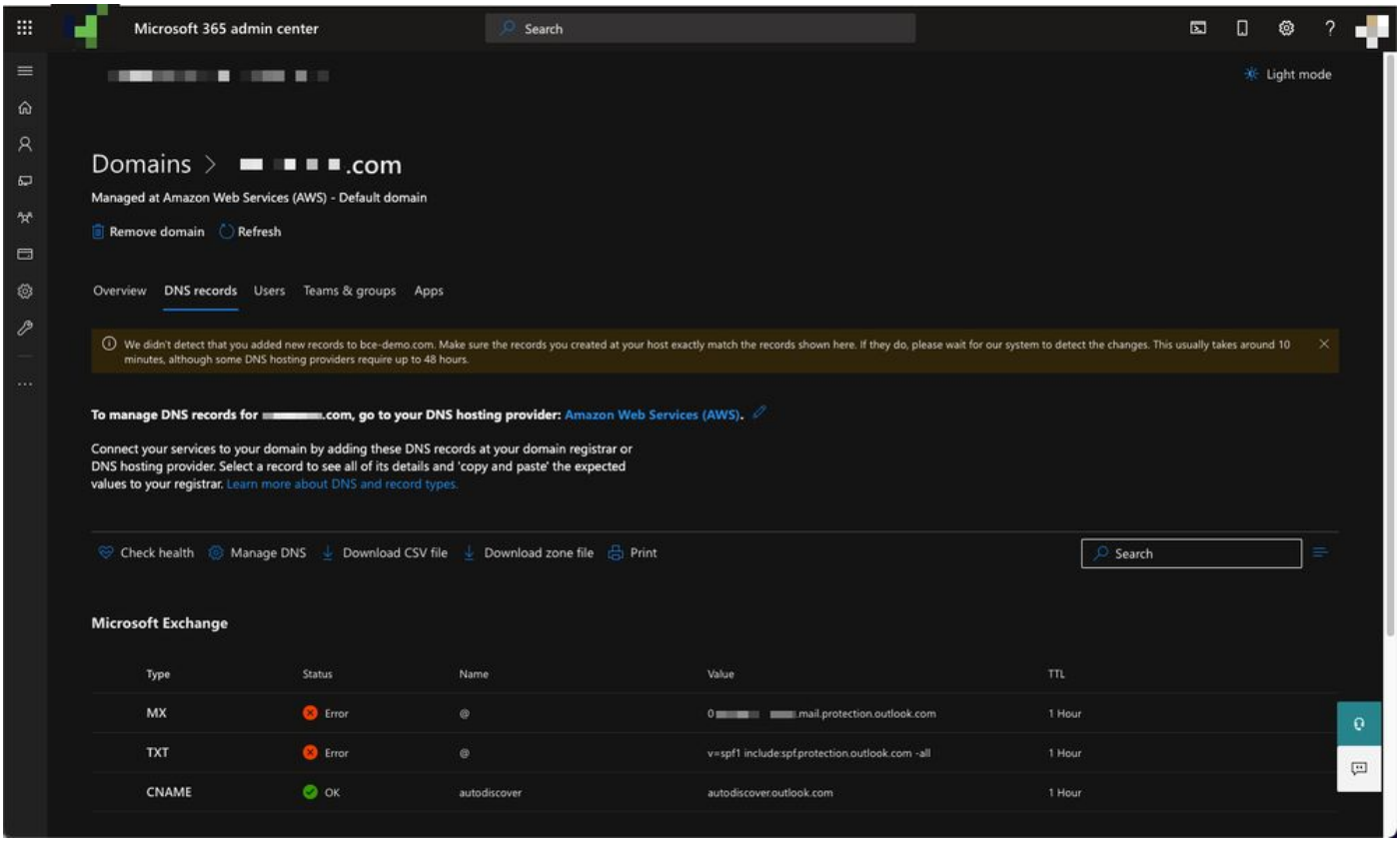
Configuração do DNS (registro do MX)

Você está pronto para interromper o domínio por meio de uma alteração de registro MX (Mail Exchange). Trabalhe com seu administrador DNS para resolver seus registros MX para os endereços IP de sua instância do Cisco Secure Email Cloud, conforme fornecido na carta de boas-vindas do Cisco Secure Email.

Verifique também a alteração no registro MX do console do Microsoft 365:

- Faça login no console Microsoft 365 Admin (https://admin.microsoft.com).
- Navegue até **Home > Settings > Domains**.
- Escolha o nome de domínio padrão.
- Clique emCheck Health.

Isso fornece os Registros MX atuais de como o Microsoft 365 pesquisa seus registros DNS e MX associados ao seu domínio:



Observação: neste exemplo, o DNS é hospedado e gerenciado pelo Amazon Web Services (AWS). Como administrador, espere ver um aviso se o seu DNS estiver hospedado em qualquer lugar fora da conta do Microsoft 365. Você pode ignorar avisos como: "Não detectamos que você adicionou novos registros a your_domain_here.com. Certifique-se de que os registros criados no host correspondam aos mostrados aqui..." As instruções passo a passo redefinem os registros MX para o que foi inicialmente configurado para redirecionar para sua conta do Microsoft 365. Isso remove o Cisco Secure Email Gateway do fluxo de tráfego de entrada.

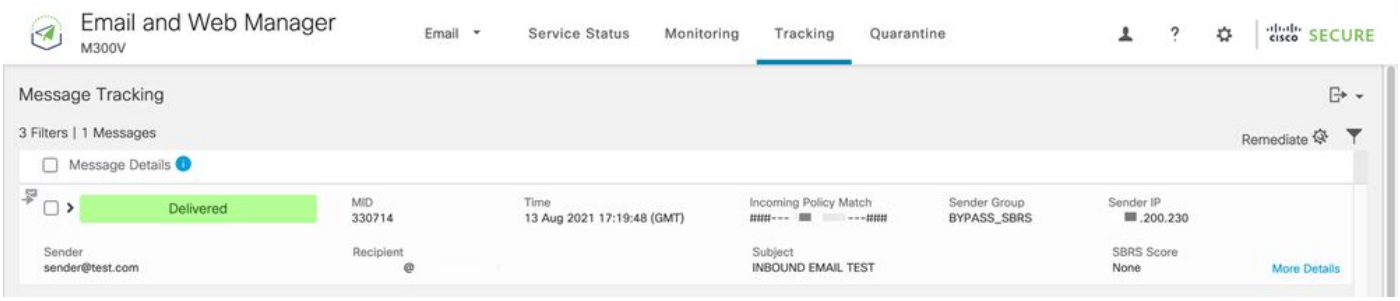
Testar email de entrada

Teste os emails de entrada para o seu endereço de email do Microsoft 365. Em seguida, verifique se ele chega à sua caixa de entrada de e-mail do Microsoft 365.

Valide os logs de e-mail em Rastreamento de mensagens no Cisco Secure Email e Web Manager (também conhecido como SMA) fornecido com sua instância.

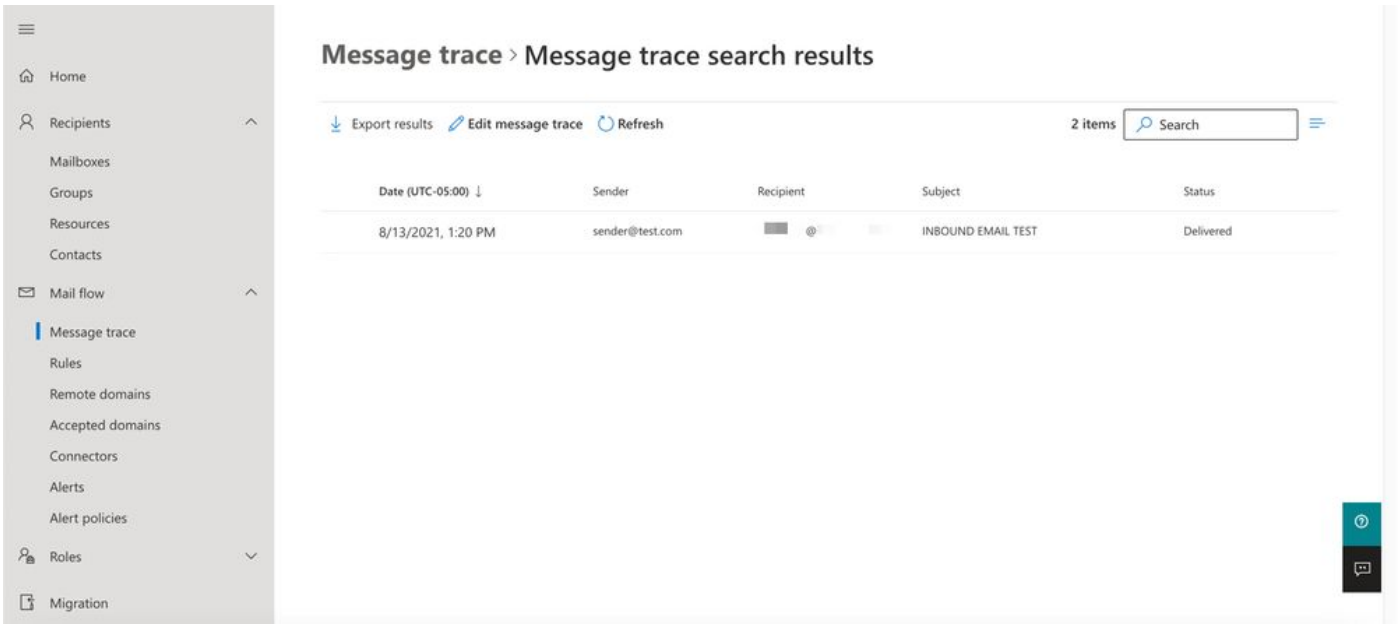
Para ver os registros de e-mail no SMA:

- Faça login no SMA (https://sma.iphmx.com/ng-login).
- Clique em **Tracking**.
- Insira os critérios de pesquisa necessários e clique em **Search**; e espere ver esses resultados:



Para ver os registros de e-mail no Microsoft 365:

- Faça login no Microsoft 365 Admin Center (https://admin.microsoft.com).
- Expandir **Admin Centers**.
- Clique em **Exchange**.
- Navegue até **Mail flow > Message trace**.
- A Microsoft fornece critérios padrão para a pesquisa. Por exemplo, escolha **Messages received by my primary domain in the last day** para iniciar sua consulta de pesquisa.
- Insira os critérios de pesquisa necessários para os destinatários e clique **Search** e espere ver resultados semelhantes a:



Configurar e-mail de saída no Microsoft 365 para o Cisco Secure Email

Configurar LISTA DE RETRANSMISSÃO no Cisco Secure Email Gateway

Consulte sua carta de boas-vindas do Cisco Secure Email. Além disso, uma interface secundária é especificada para mensagens de saída pelo Gateway.

- Faça login no Gateway.
- Navegue até **Mail Policies > HAT Overview**.

Observação: Certifique-se de que o Listener se refere a Ouvinte de Saída, E-mail de Saída ou Fluxo de E-mail Externo, com base no nome real do Listener para seu fluxo de e-mail externo/de saída.

- Clique em **Add Sender Group...**
- Configure o grupo de remetentes como:

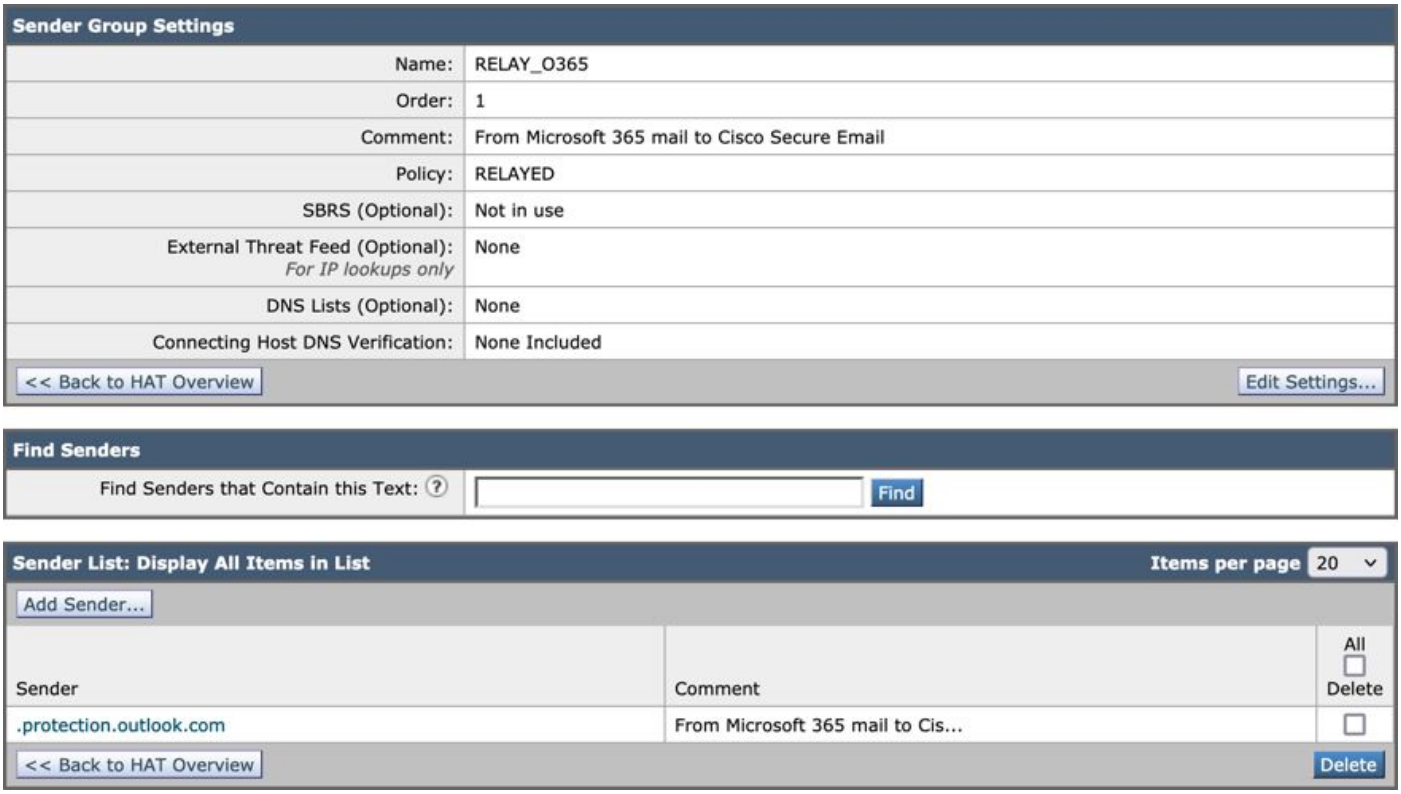
1. Nome: RELAY_O365
2. Comentário: <<enter a comment if you wish to notate your sender group>>
3. Política: RETRANSMITIDA
4. Clique em **Submit and Add Senders**.

- Remetente: **.protection.outlook.com**

Observação: o **.** (ponto) no início do nome de domínio do remetente é obrigatório.

- Clique em **Submit**.
- Clique **Commit Changes** no canto superior direito da interface do usuário para salvar suas alterações de configuração.

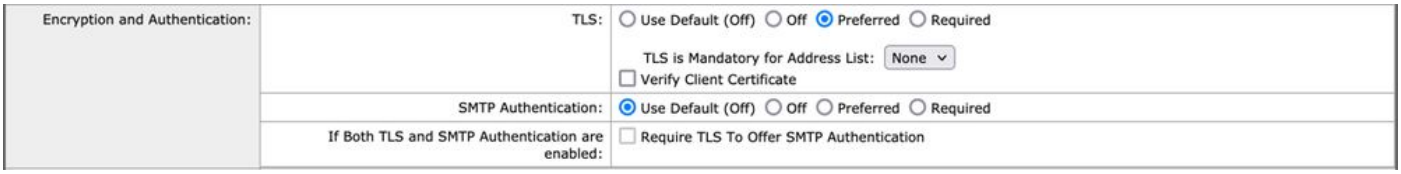
Um exemplo de como são as configurações do grupo de remetente:



Ativar TLS

- Clique em **<<Back to HAT Overview**.
- Clique na política de fluxo de e-mails denominada: **RELAYED**.
- Desça e procure na **Security Features** seção **Encryption and Authentication**.
- Em TLS, escolha: **Preferred**.
- Clique em **Submit**.
- Clique **Commit Changes** no canto superior direito da interface do usuário para salvar suas alterações de configuração.

Um exemplo de como é a configuração da Política de fluxo de e-mail:



Configurar e-mail do Microsoft 365 para o CES

- Faça login no Microsoft 365 Admin Center (https://admin.microsoft.com).
- Expandir **Admin Centers**.
- Clique em **Exchange**.
- Navegue até **Mail flow > Connectors**.
- Clique [+] para criar um novo conector.
- Na janela pop-up Selecionar cenário do fluxo de e-mail, escolha:

1. De: Office365
    - Para:Partner organization

- Clique em **Next**.
- Digite um nome para o novo conector: **Outbound to Cisco CES**.
- Insira uma descrição, se desejar.
- Clique em **Next**.
- Para Quando você deseja usar este conector?:

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

- Clique em **Route email through these smart hosts**.

- Clique **[+]** e insira os endereços IP de saída ou os nomes de host fornecidos em sua carta de boas-vindas do CES.

- Clique em **Save**.
- Clique em **Next**.
- Para saber Como o Office 365 deve se conectar ao servidor de email da sua organização parceira?

1. Escolha: **Always use TLS to secure the connection (recommended)**.

    - EscolhaAny digital certificate, including self-signed certificates.
    - Clique em **Next**.

- Você verá a tela de confirmação.
- Clique em **Next**.
- Use **[+]** para inserir um endereço de e-mail válido e clique em **OK**.
- Clique em **Validate** e permita que a validação seja executada.
- Depois de concluir, clique em **Close**.
- Clique emSave.

Um exemplo de como é a aparência do Conector de Saída:

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

Criar uma regra de fluxo de e-mails

1. Para o pop-up selecionar local do remetente, escolha: **Inside the organization**.

    - Clique em **OK**.

- Clique em **More options...**
- Clique no **add condition** botão e insira uma segunda condição:

    1. Escolher **The recipient...**

        - Escolha: **Is external/internal**.
        - Para o pop-up selecionar local do remetente, escolha: **Outside the organization** .
        - Clique em **OK**.

- Para *Fazer o seguinte..., escolha: **Redirect the message to...**

    1. Selecione: **o seguinte conector**.
    2. E selecione seu conector **Outbound to Cisco CES**.
    3. Click **OK**.

- Volte para "*Faça o seguinte..." e insira uma segunda ação:

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

        - Escolha: **set the message header**
        - Defina o cabeçalho da mensagem: **X-OUTBOUND-AUTH**.
        - Clique em **OK**.
        - Defina o valor: **mysecretkey**.

- Clique em **OK**.

- Clique em **Save**.

Observação: para evitar mensagens não autorizadas da Microsoft, um cabeçalho x secreto pode ser carimbado quando as mensagens saem do domínio Microsoft 365; esse cabeçalho é avaliado e removido antes da entrega para a Internet.

Um exemplo de como é a sua configuração do Microsoft 365 Routing:

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

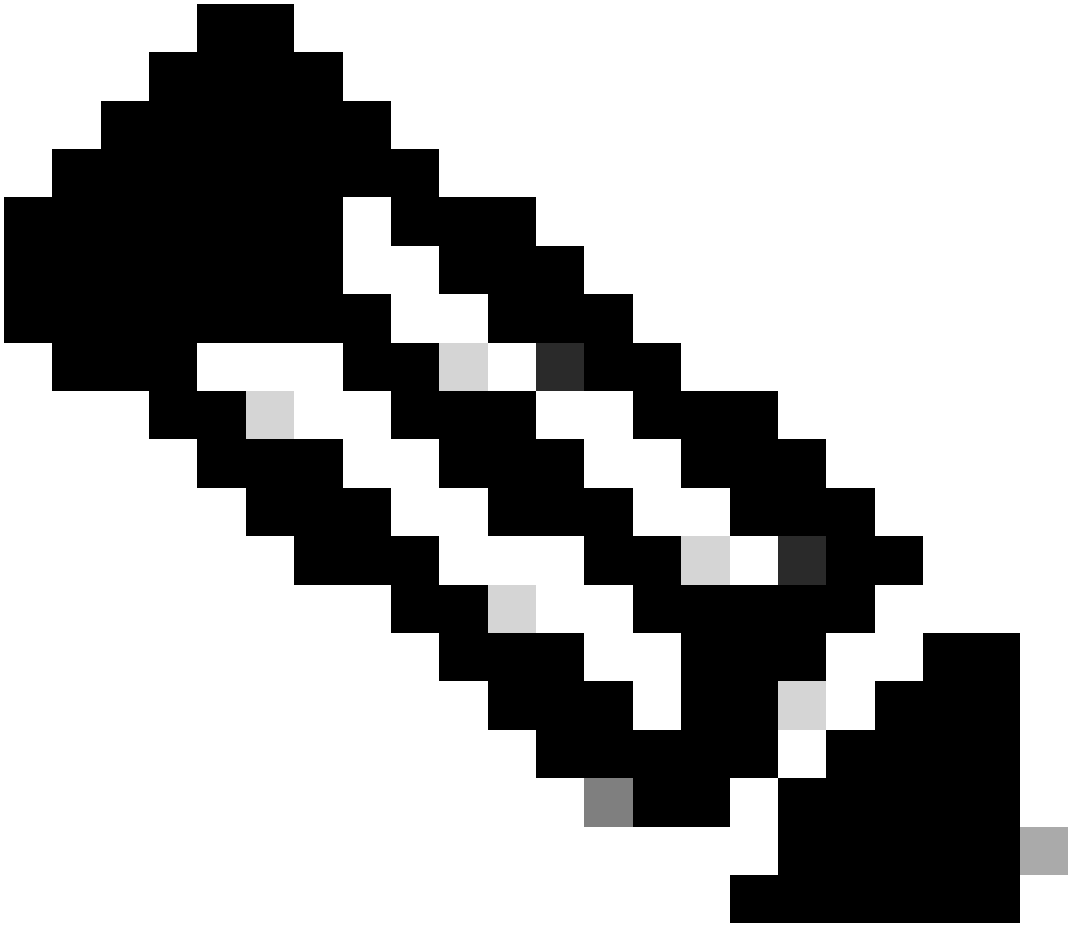
PCI

Comments:

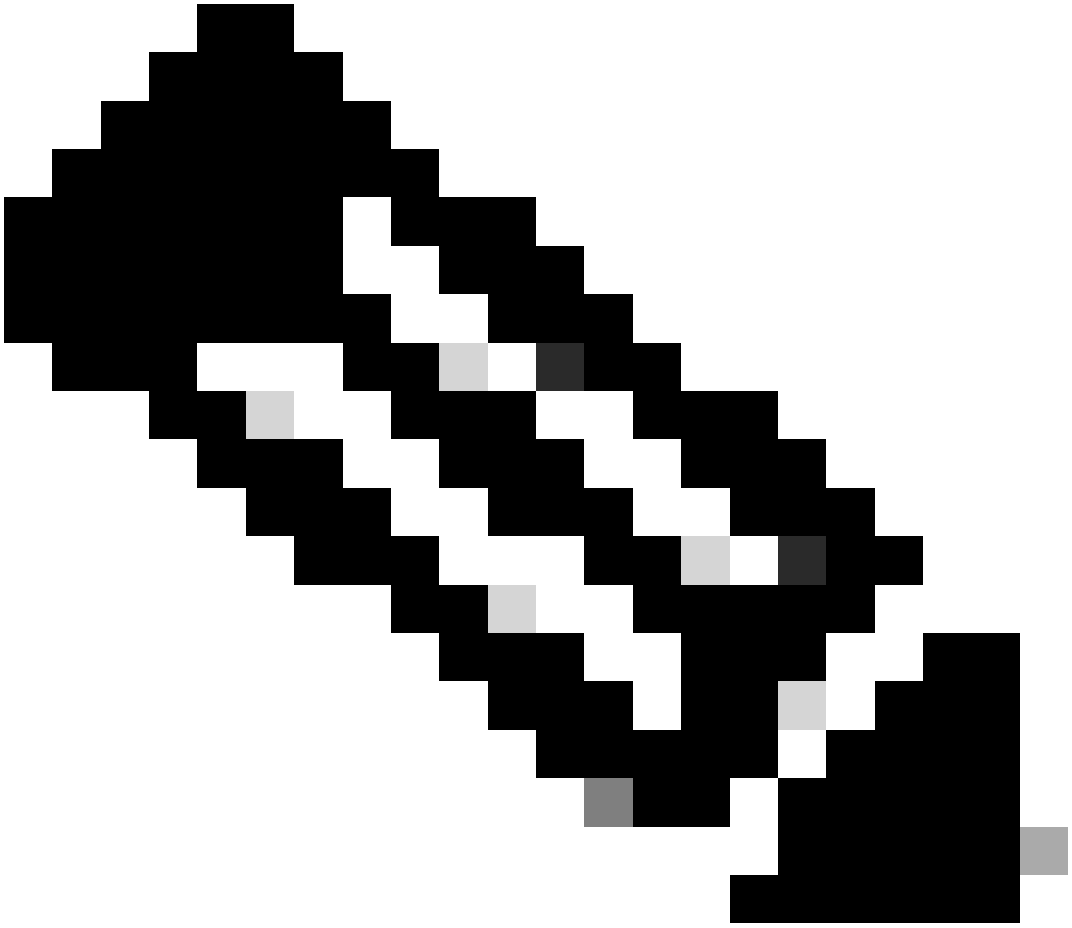
ℹ Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

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

- Pressione Retornar uma vez para criar uma nova linha em branco.
- Digite **[.]** na nova linha para finalizar o novo filtro de mensagens.
- Clique em **return** uma vez para sair do menu Filtros.
- Execute o **Commit** comando para salvar as alterações na sua configuração.



Observação: evite caracteres especiais para a chave secreta. Os ^ e $ mostrados no filtro da mensagem são caracteres regex e usam como fornecido no exemplo.



Observação: revise o nome de como sua RELAYLIST está configurada. Ele pode ser configurado com um nome alternativo ou você pode ter um nome específico com base na sua política de retransmissão ou no seu provedor de e-mail.

Testar email de saída

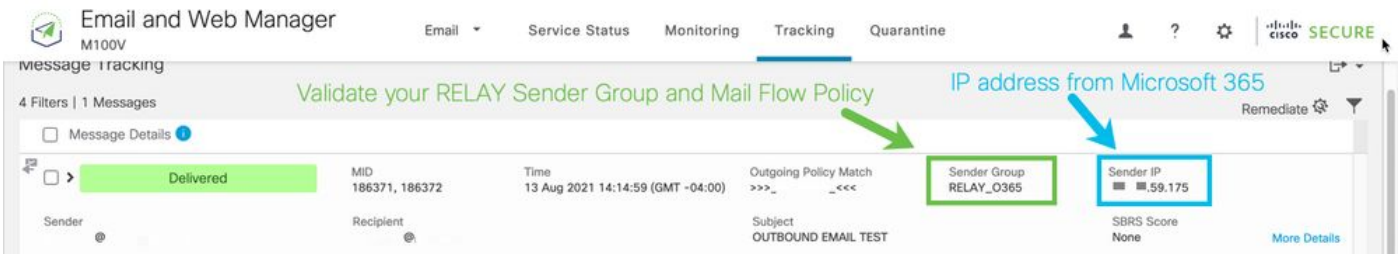
Teste os emails de saída do seu endereço de email do Microsoft 365 para um destinatário de domínio externo. Você pode rever o Rastreamento de mensagens do Cisco Secure Email e do Web Manager para garantir que ele seja encaminhado corretamente para a saída.

Observação: revise sua configuração TLS (**Administração do sistema > configuração SSL**) no Gateway e as cifras usadas para SMTP

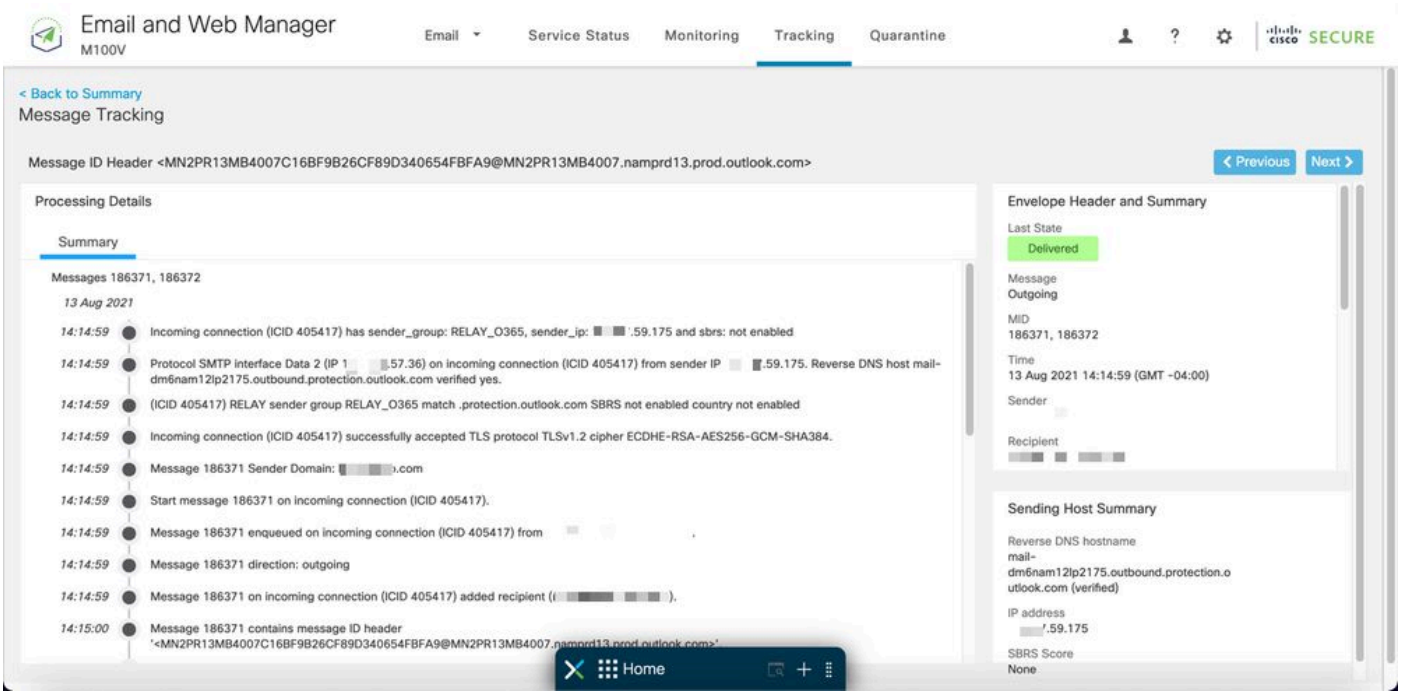
de saída. As Melhores práticas da Cisco recomendam:

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

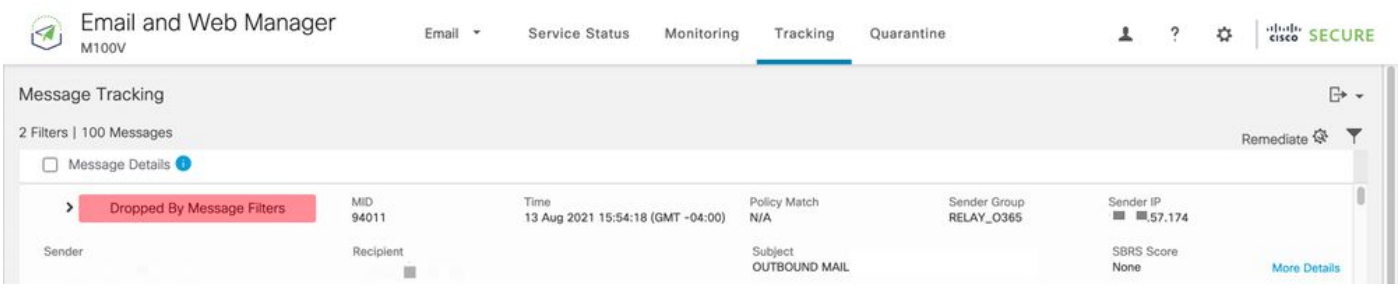
Um exemplo de rastreamento com entrega bem-sucedida:

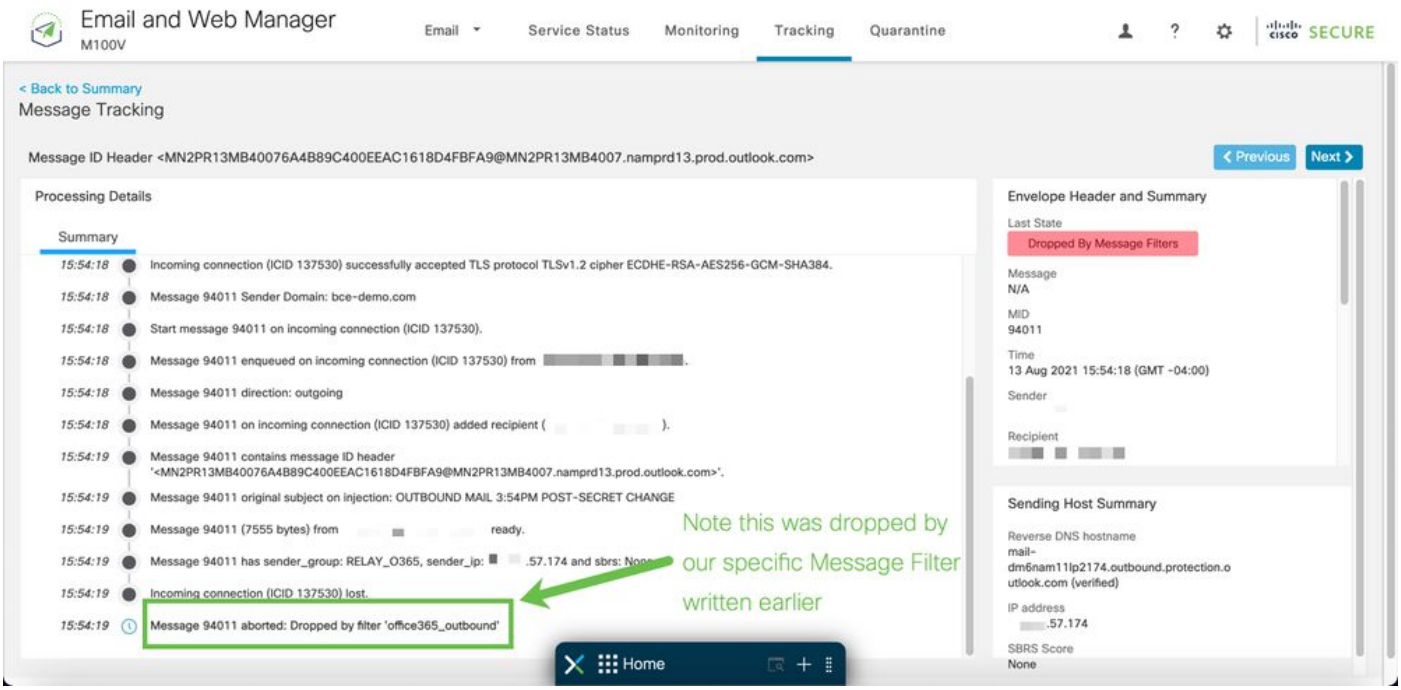


Clique **More Details** para ver os detalhes completos da mensagem:



Um exemplo de rastreamento de mensagem em que o cabeçalho x não corresponde:





Informações Relacionadas

Documentação do Cisco Secure Email Gateway

- Notas de versão
- Guia do usuário
- Guia de referência CLI
- Guias de programação de API para Cisco Secure Email Gateway
- Fonte aberta usada no Cisco Secure Email Gateway
- Guia de instalação do Cisco Content Security Virtual Appliance (inclui vESA)

Documentação do Secure Email Cloud Gateway

- Notas de versão
- Guia do usuário

Documentação do Cisco Secure Email and Web Manager

- Notas de versão e matriz de compatibilidade

    - Guia do usuário
- Guias de programação de API para Cisco Secure Email e Web Manager
- Guia de instalação do Cisco Content Security Virtual Appliance (inclui vSMA)

Documentação do produto Cisco Secure

- Arquitetura de nomenclatura do portfólio Cisco Secure

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.