Microsoft 365 configureren met beveiligde e-mail

Inhoud

Inleiding

In dit document worden de configuratiestappen beschreven om Microsoft 365 te integreren met Cisco Secure Email voor levering van inkomende en uitgaande e-mail.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Email Gateway of Cloud Gateway
- CLI-toegang (Command Line Interface) tot uw Cisco Secure Email Cloud Gateway-

omgeving:
Cisco Secure Email Cloud Gateway > CLI-toegang (Command Line Interface)
- Microsoft 365
- Simple Mail Transfer Protocol (SMTP)
- Domain Name Server of Domain Name System (DNS)

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document kan worden gebruikt voor gateways op locatie of voor Cisco Cloud-gateways.

Als u een Cisco Secure Email Administrator bent, bevat uw welkomstbrief uw Cloud Gateway IP-adressen en andere relevante informatie. Naast de brief die u hier ziet, wordt er een versleutelde e-mail naar u gestuurd die u aanvullende informatie geeft over het aantal Cloud Gateway (ook bekend als ESA) en Cloud Email and Web Manager (ook bekend als SMA) dat is meegeleverd voor uw toewijzing. Als u geen exemplaar van de brief hebt ontvangen of niet in het bezit hebt, neem dan contact op ces-activations@cisco.com met uw contactgegevens en domeinnaam onder de 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

Elke client heeft speciale IP's. U kunt de toegewezen IP-adressen of hostnamen gebruiken in de Microsoft 365-configuratie.

Opmerking: het is ten zeerste aan te raden om te testen vóór een geplande conversie van de productie-mail, omdat configuraties tijd nodig hebben om te repliceren in de Microsoft 365 Exchange-console. Laat minimaal een uur staan om alle wijzigingen van kracht te laten worden.

Opmerking: de IP-adressen in de schermopname zijn evenredig met het aantal cloudgateways dat is geleverd aan uw toewijzing. Bijvoorbeeld, xxx.yy.140.105 is het Gegevens 1 interfaceIP adres voor Gateway 1, en xxx.yy.150.1143 is het Gegevens 1 interfaceIP adres voor Gateway 2. Gegevens 2 interface IP-adres voor gateway 1 is xxx.yy.143.186 , en gegevens 2 interface IP-adres voor gateway 2 is xxx.yy.32.98. Als uw welkome brief geen informatie voor Gegevens 2 (Uitgaande interface IPs) omvat, neem contact op met Cisco TAC om de Data 2-interface aan uw toewijzing toe te voegen.

Microsoft 365 configureren met beveiligde e-mail

Inkomende e-mail vanuit Cisco Secure Email configureren in Microsoft 365

Spamfilterregel omzeilen

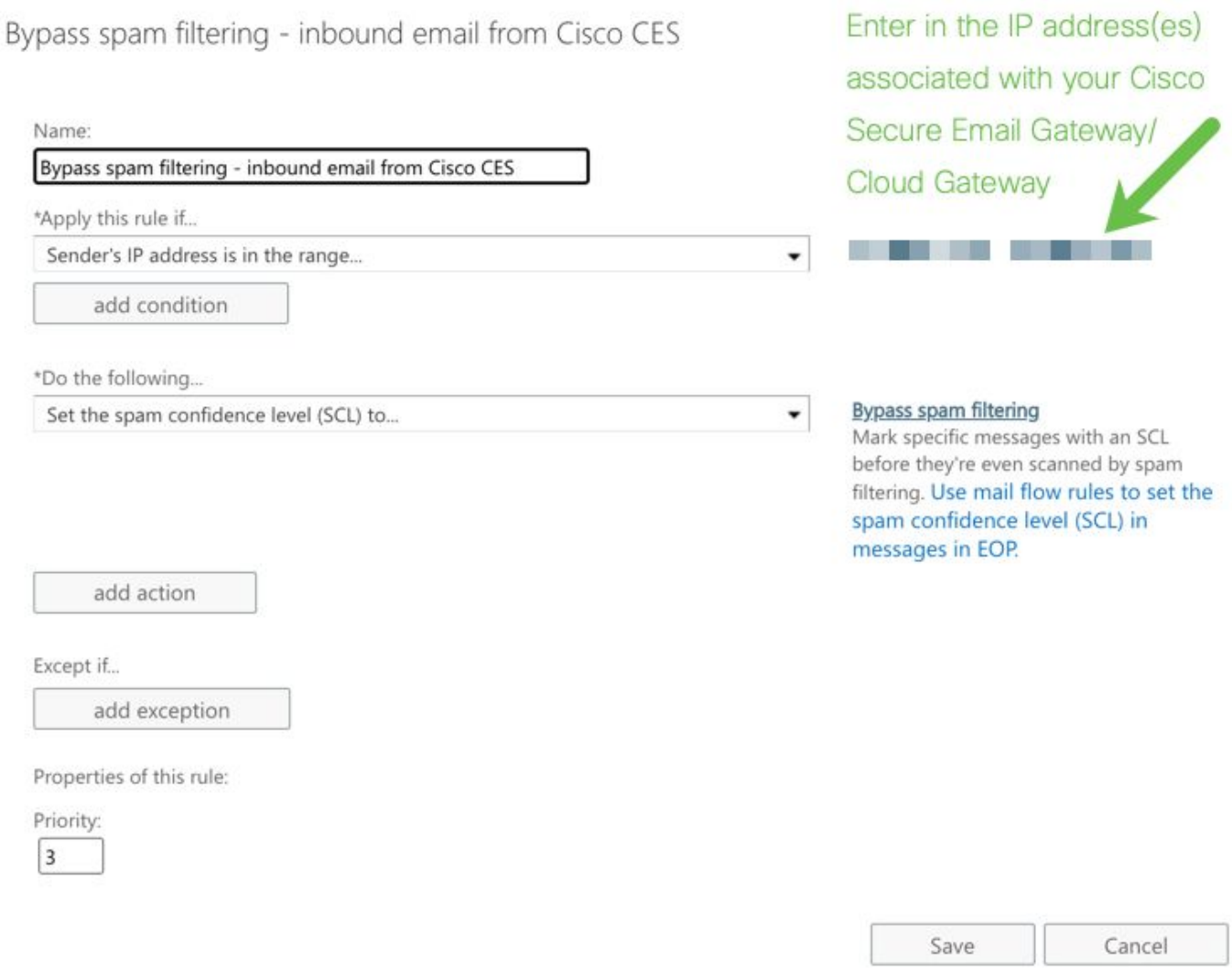
- Log in op het Microsoft 365 Admin Center (https://portal.microsoft.com).
- In het linker menu vouwt u het programma uit **Admin Centers**.
- Klik op de knop **Exchange**.
- Navigeer vanuit het linkermenu naar **Mail flow > Rules**.
- Klik om een nieuwe regel **[+]** aan te maken.
- Kies **Bypass spam filtering...** uit de vervolgkeuzelijst.
- Voer een naam in voor uw nieuwe regel: **Bypass spam filtering - inbound email from Cisco CES**.
- Voor *Deze regel toepassen als..., kies **The sender - IP address is in any of these ranges or exactly matches**.

1. Voeg voor de pop-up gespecificeerde IP-adresbereiken de IP-adressen toe die in uw welkomstbrief voor Cisco Secure Email worden verstrekt.
2. Klik op de knop **OK**.

- Voor *Doe het volgende..., de nieuwe regel is vooraf geselecteerd: **Set the spam confidence level (SCL) to... - Bypass spam filtering**.

- Klik op de knop **Save**.

Een voorbeeld van hoe uw regel eruit ziet:



Ontvangende connector

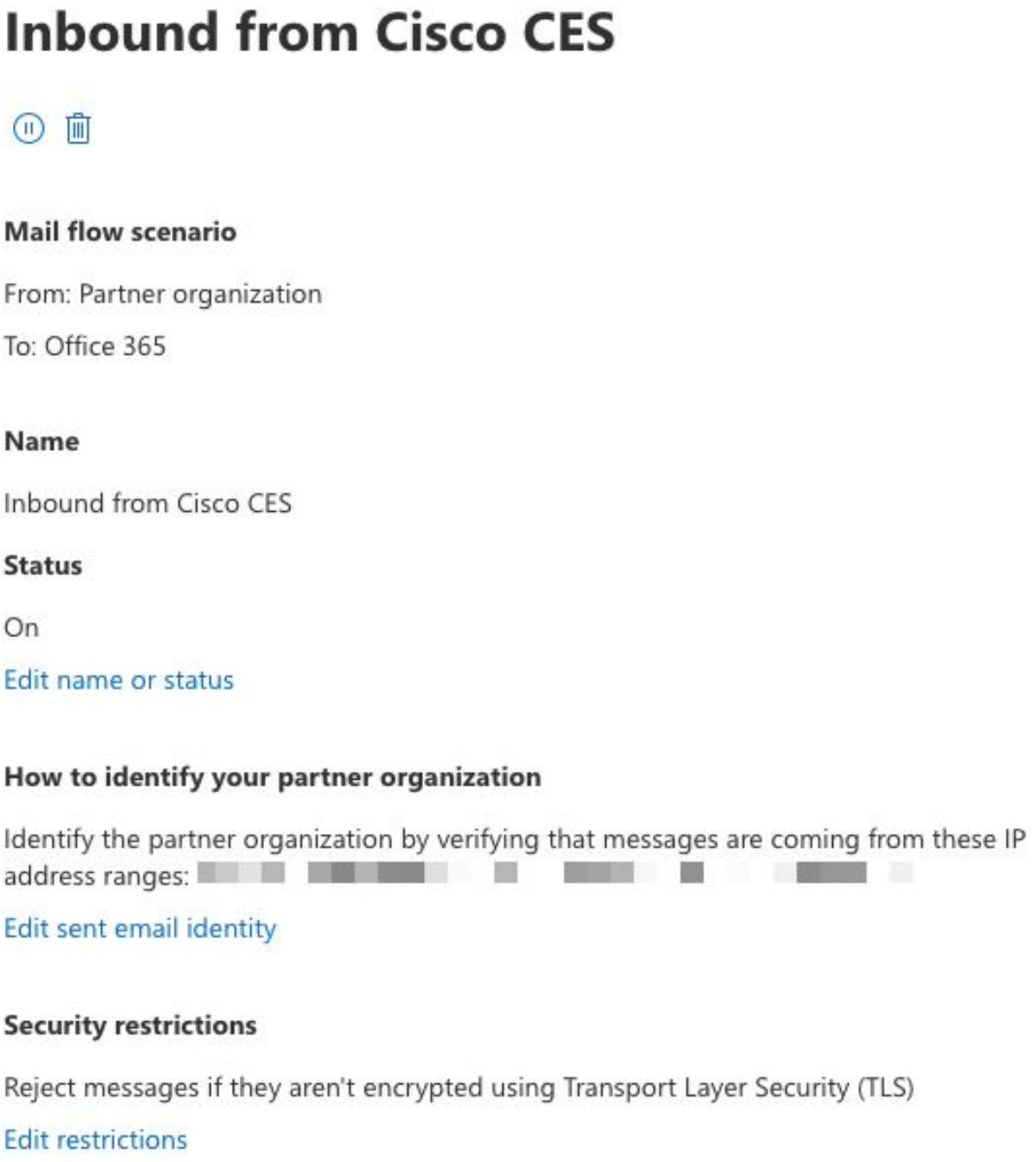
- Blijf in het Exchange-beheercentrum.
- Navigeer vanuit het linkermenu naar **Mail flow > Connectors**.
- Klik om een nieuwe connector **[+]** te maken.
- Kies in het pop-upvenster Selecteer het scenario voor de e-mailstroom:

1. Van: Partner organization

    - in: **Office365**

- Klik op de knop **Next**.
- Voer een naam in voor uw nieuwe connector: **Inbound from Cisco CES**.
- Voer desgewenst een beschrijving in.
- Klik op de knop **Next**.
- Klik op de knop **Use the sender's IP address**.
- Klik op de knop **Next**.
- Klik op **[+]** en voer de IP-adressen in die worden aangegeven in uw welkomstbrief voor beveiligde e-mail van Cisco.
- Klik op de knop **Next**.
- Kiezen **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- Klik op de knop **Next**.
- Klik op de knop **Save**.

Een voorbeeld van hoe uw verbindingsconfiguratie eruit ziet:



E-mail van Cisco Secure Email naar Microsoft 365 configureren

Besturingselementen voor bestemming

Stel een self-throttle op aan een bezorgingsdomein in uw Bestemmingscontroles. Natuurlijk kunt u de gaspedaal later verwijderen, maar dit zijn nieuwe IPs naar Microsoft 365, en u wilt geen gaspedaal door Microsoft vanwege zijn onbekende reputatie.

- Meld u aan bij uw gateway.
- Naar navigeren **Mail Policies > Destination Controls**.
- Klik op de knop **Add Destination**.

- Gebruik:

1. Bestemming: Voer uw domeinnaam in

2. Gelijktijdige verbindingen: **10**

   - Maximum aantal berichten per verbinding: **20**
   - TLS-ondersteuning: **Preferred**

- Klik op de knop **Submit**.
- Klik rechtsboven **Commit Changes** in de gebruikersinterface om de wijzigingen in de configuratie op te slaan.

Een voorbeeld van hoe uw Bestemmingscontroletabel eruit ziet:

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.

Toegangstabel voor ontvangers

Stel vervolgens de Recipient Access Table (RAT ofwel Toegangstabel voor ontvangers) in om e-mail voor uw domeinen te accepteren:

- Naar navigeren **Mail Policies > Recipient Access Table (RAT)**.

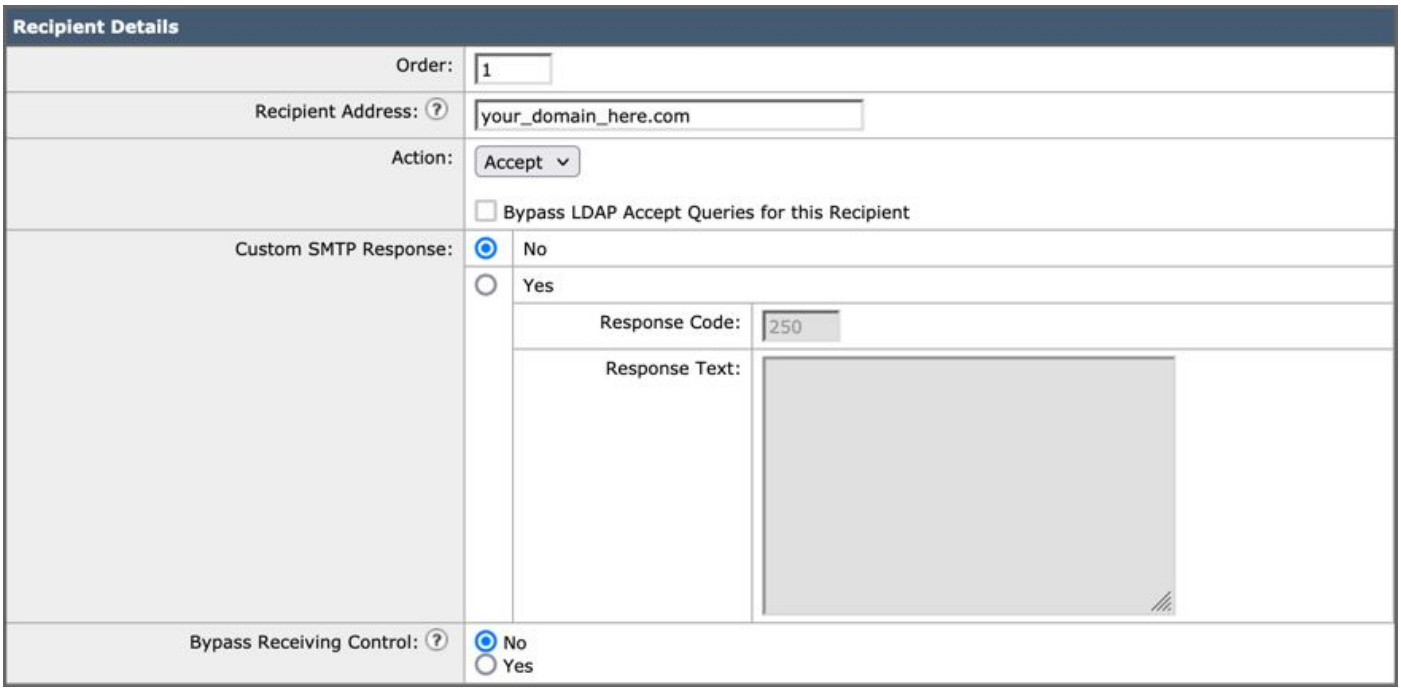
Opmerking: Zorg ervoor dat de Luisteraar voor Inkomende Luisteraar, IncomingMail of MailFlow is, gebaseerd op de feitelijke naam van uw Luisteraar voor uw primaire mailstroom.

- Klik op de knop **Add Recipient**.
- Voeg uw domeinen toe in het veld Ontvankelijk adres.
- Kies de standaardactie van **Accept**.

- Klik op de knop **Submit**.

- Klik **Commit Changes** in de rechterbovenhoek van de UI om uw configuratieveranderingen op te slaan.

Een voorbeeld van hoe uw RAT-vermelding eruit ziet:



SMTP-routes

Stel de SMTP-route in om e-mail te leveren vanuit Cisco Secure Email naar uw Microsoft 365-domein:

- Naar navigeren **Network > SMTP Routes**.

- Klik op de knop **Add Route...**

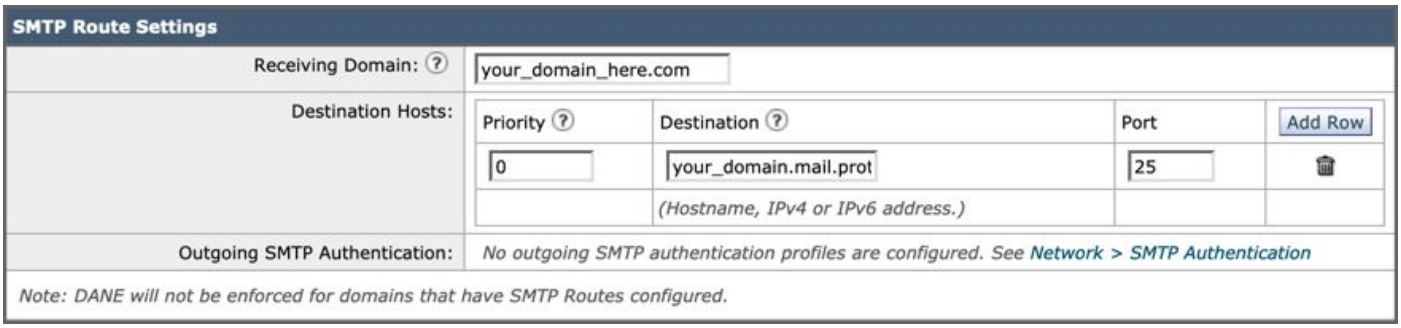
- Domein ontvangen: voer uw domeinnaam in.

- Bestemmingshosts: voeg uw originele Microsoft 365 MX-record toe.

- Klik op de knop **Submit**.

- Klik **Commit Changes** in de rechterbovenhoek van de UI om uw configuratieveranderingen op te slaan.

Een voorbeeld van hoe uw SMTP-routeinstellingen eruit zien:



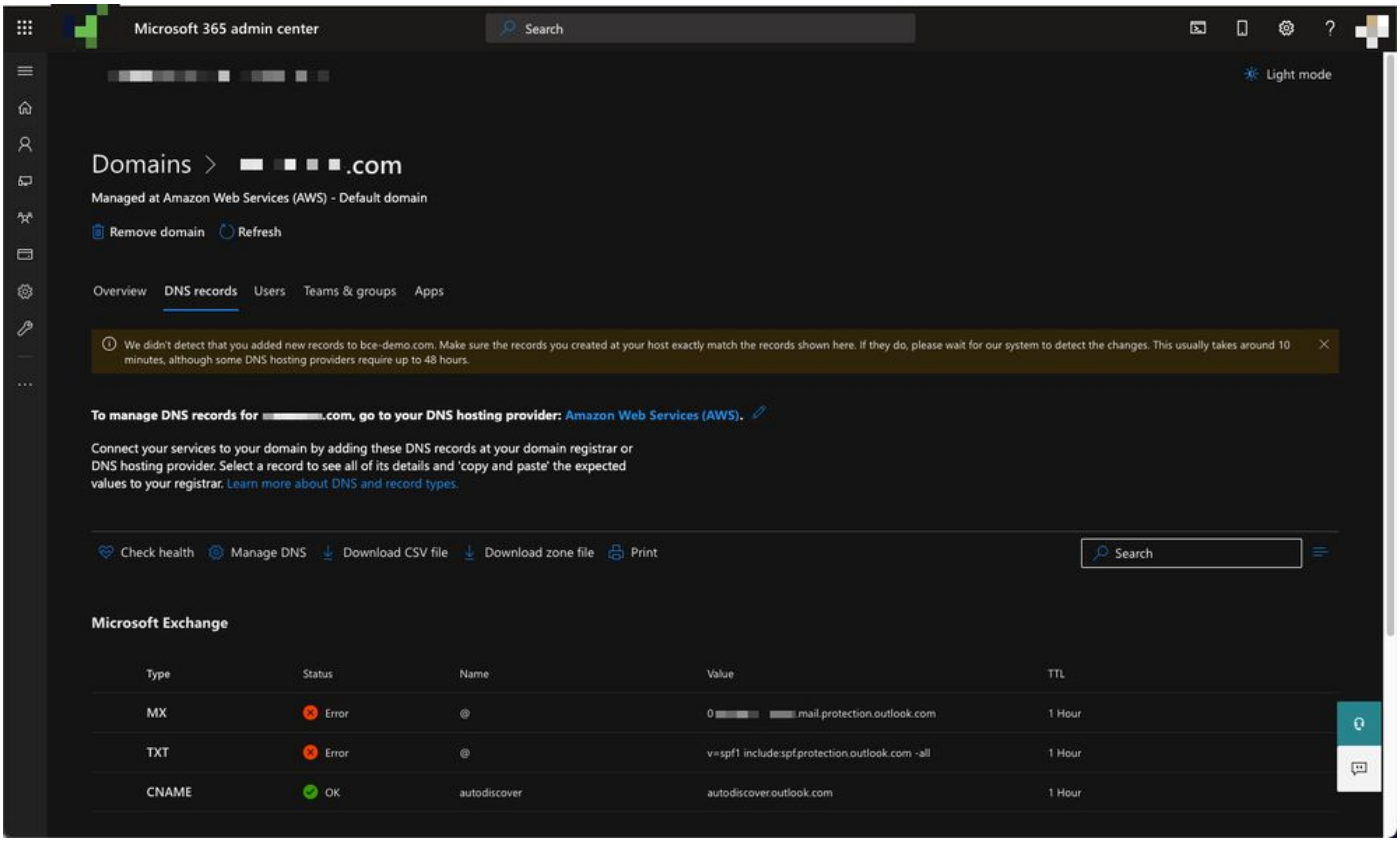
Configuratie van DNS (MX-record)

U bent klaar om het domein te doorsnijden via een Mail Exchange (MX) record wijziging. Werk samen met uw DNS-beheerder om uw MX-records op te lossen naar de IP-adressen voor uw Cisco Secure Email Cloud-exemplaar, zoals voorzien in uw welkomstbrief voor Cisco Secure Email.

Controleer ook de wijziging van het MX-record van uw Microsoft 365-console:

- Meld u aan bij de Microsoft 365 Admin-console (https://admin.microsoft.com).
- Naar navigeren **Home > Settings > Domains**.
- Kies uw standaard domeinnaam.
- Klik op de knop Check Health.

Dit biedt de huidige MX Records van hoe Microsoft 365 uw DNS- en MX-records opzoekt die aan uw domein zijn gekoppeld:



Opmerking: in dit voorbeeld wordt het DNS gehost en beheerd door Amazon Web Services (AWS). Als beheerder, verwacht een waarschuwing te zien als uw DNS ergens buiten de Microsoft 365-account wordt gehost. Je kunt waarschuwingen als: "We hebben niet gedetecteerd dat je nieuwe records hebt toegevoegd aan your_domain_here.com. Zorg ervoor dat de records die u bij uw host hebt gemaakt overeenkomen met de hier weergegeven records..." Met de stapsgewijze instructies worden de MX-records opnieuw ingesteld op wat aanvankelijk was geconfigureerd om naar uw Microsoft 365-account te worden doorgestuurd. Dit verwijdert de Cisco Secure Email Gateway uit de inkomende verkeersstroom.

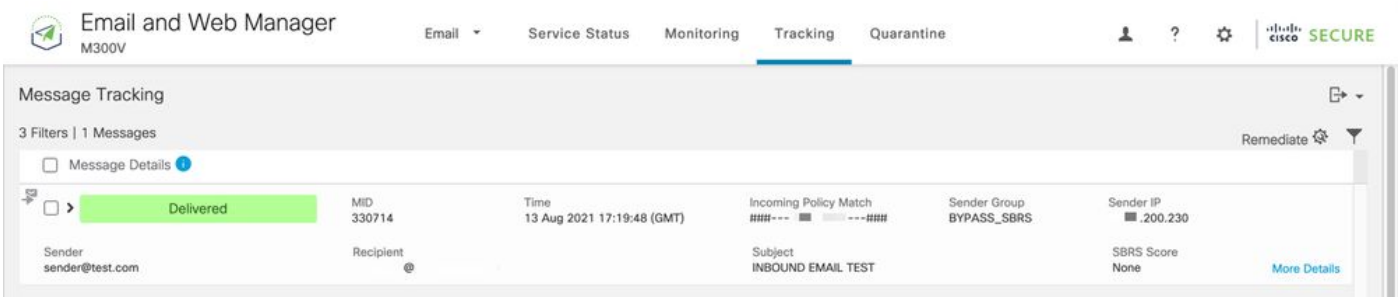
Inkomende e-mail testen

Test inkomende mail naar uw Microsoft 365 e-mailadres. Controleer vervolgens of het in je Microsoft 365 email inbox aankomt.

Valideren van de e-maillogbestanden in het berichtentraceren op uw Cisco Secure Email and Web Manager (ook bekend als SMA) die bij uw exemplaar wordt geleverd.

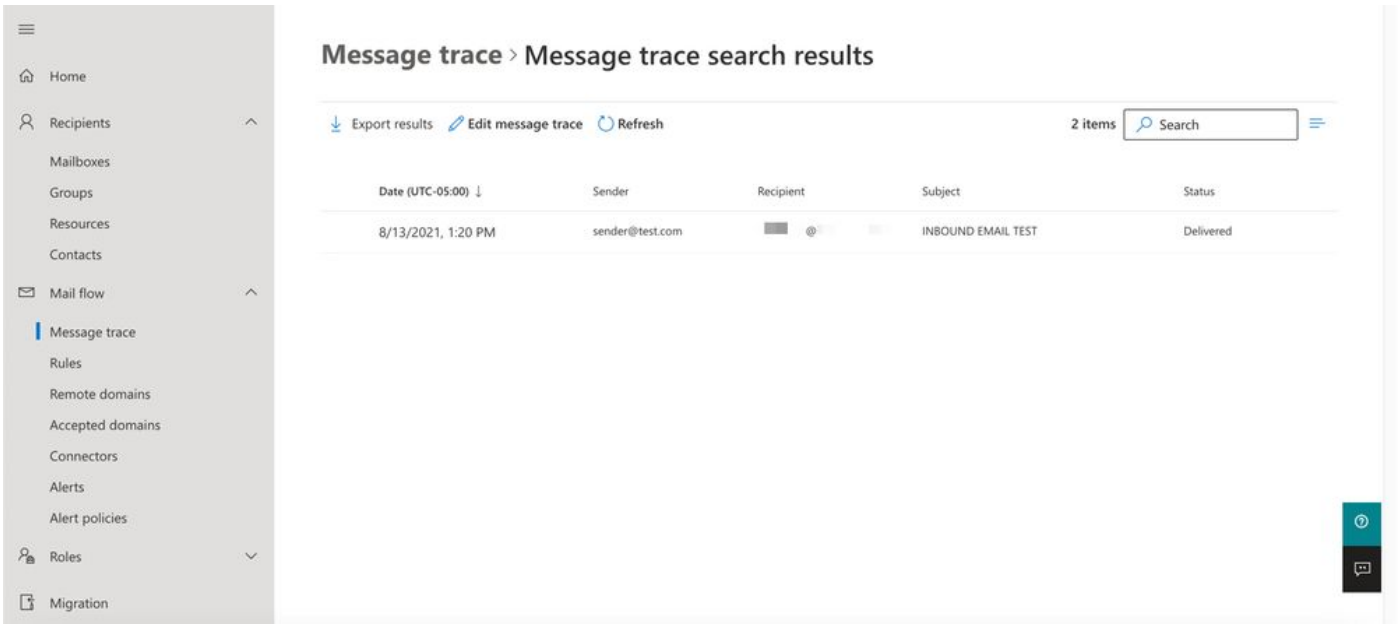
U kunt e-maillogboeken als volgt bekijken in uw SMA:

- Meld u aan bij uw SMA (https://sma.iphmx.com/ng-login).
- Klik op de knop **Tracking**.
- Voer de gewenste zoekcriteria in en klik op **Search**; en verwacht dergelijke resultaten te zien:



U kunt e-maillogboeken als volgt bekijken in Microsoft 365:

- Log in op het Microsoft 365 Admin Center (https://admin.microsoft.com).
- Uitbreiden **Admin Centers**.
- Klik op de knop **Exchange**.
- Naar navigeren **Mail flow > Message trace**.
- Microsoft geeft standaardcriteria om mee te zoeken. Kies bijvoorbeeld **Messages received by my primary domain in the last day** om uw zoekopdracht te starten.
- Voer de gewenste zoekcriteria voor ontvangers in en klik op **Search** en verwacht resultaten te zien die vergelijkbaar zijn met:



Uitgaande e-mail van Microsoft 365 configureren in Cisco Secure Email

RELAYLIST configureren op Cisco Secure Email Gateway

Raadpleeg uw welkomstbrief voor Cisco Secure Email. Bovendien wordt een secundaire interface gespecificeerd voor uitgaande berichten via uw gateway.

- Meld u aan bij uw gateway.
- Naar navigeren **Mail Policies > HAT Overview**.

Opmerking: Zorg ervoor dat de Luisteraar is voor Uitgaande Luisteraar, UitgaandeMail, of MailFlow-Ext, gebaseerd op de feitelijke naam van uw Luisteraar voor uw externe/uitgaande e-mailstroom.

- Klik op de knop **Add Sender Group...**
- Configureer de afzendersgroep als volgt:

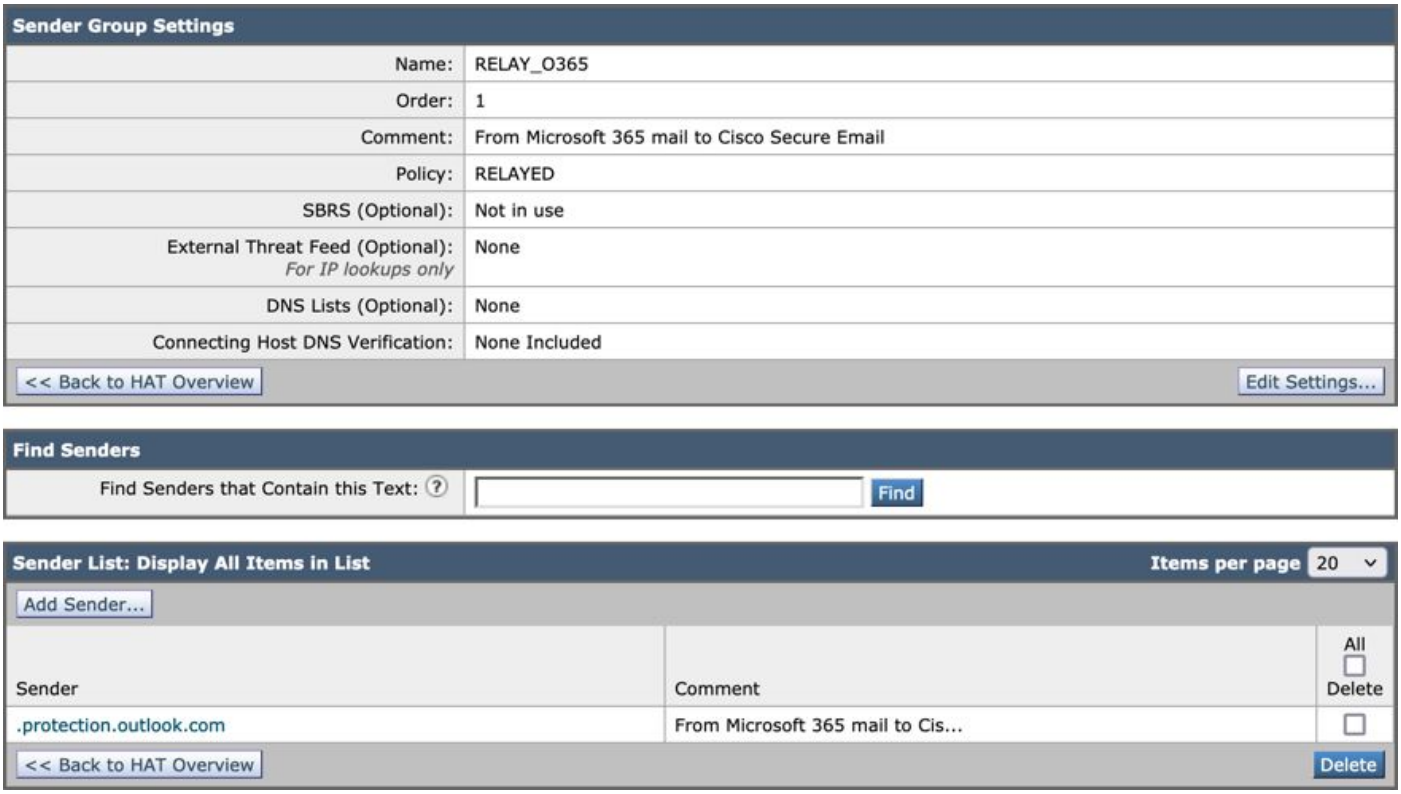
1. Naam: RELAY_O365
2. Opmerking: <<voer een opmerking in als u de groep van afzenders wilt noteren>
3. Beleid: RELAYED
4. Klik op de knop **Submit and Add Senders**.

- Afzender: **.protection.outlook.com**

Opmerking: De **.** (punt) aan het begin van de naam van het afzenderdomein is vereist.

- Klik op de knop **Submit**.
- Klik **Commit Changes** in de rechterbovenhoek van de UI om uw configuratieveranderingen op te slaan.

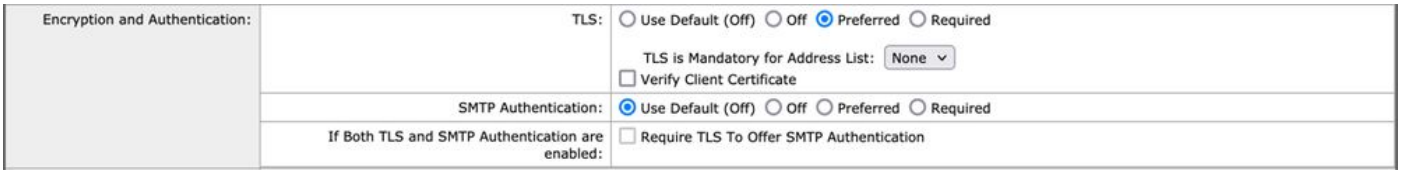
Een voorbeeld van hoe uw Sender Group Settings eruit ziet:



TLS inschakelen

- Klik op de knop **<<Back to HAT Overview**.
- Klik op het E-mailstroombeleid met de naam: **RELAYED**.
- Blader naar beneden en kijk in het **Security Features** gedeelte naar **Encryption and Authentication**.
- Kies het volgende voor TLS: **Preferred**.
- Klik op de knop **Submit**.
- Klik **Commit Changes** in de rechterbovenhoek van de UI om uw configuratieveranderingen op te slaan.

Een voorbeeld van hoe uw Mail Flow Policy-configuratie eruit ziet:



E-mail configureren van Microsoft 365 naar CES

- Log in op het Microsoft 365 Admin Center (https://admin.microsoft.com).
- Uitbreiden **Admin Centers**.
- Klik op de knop **Exchange**.
- Naar navigeren **Mail flow > Connectors**.
- Klik op [+] om een nieuwe connector te maken.
- Kies in het pop-upvenster Selecteer het scenario voor de e-mailstroom:

    1. Van: Office365

        - in:Partner organization

- Klik op de knop **Next**.
- Voer een naam in voor uw nieuwe connector: **Outbound to Cisco CES**.
- Voer desgewenst een beschrijving in.
- Klik op de knop **Next**.
- Wanneer wilt u deze connector gebruiken?:

    1. Kies: **Only when I have a transport rule set up that redirects messages to this connector**.

        - Klik op de knop **Next**.

- Klik op de knop **Route email through these smart hosts**.

- Klik **[+]** en voer de uitgaande IP-adressen of hostnamen in die u in uw CES welkomstbrief hebt opgegeven.

- Klik op de knop **Save**.
- Klik op de knop **Next**.
- Voor Hoe kan Office 365 verbinding maken met de e-mailserver van uw partnerorganisatie?

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

    - KiesAny digital certificate, including self-signed certificates.
    - Klik op de knop **Next**.

- Het bevestigingsscherm verschijnt.
- Klik op de knop **Next**.
- Gebruik dit **[+]** om een geldig e-mailadres in te voeren en klik op **OK**.
- Klik op **Validate** de validatie en laat deze uitvoeren.
- Klik nadat u het programma hebt voltooid op **Close**.
- Klik op de knop Save.

Een voorbeeld van hoe uw uitgaande connector eruit ziet:

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

1. Kies voor het pop-upvenster Scanderlocatie: **Inside the organization**.

    - Klik op de knop **OK**.

- Klik op de knop **More options...**
- Klik op **add condition** de knop en voer een tweede voorwaarde in:

    1. Kiezen **The recipient...**

        - Kies: **Is external/internal**.
        - Kies voor het pop-upvenster Scanderlocatie: **Outside the organization** .
        - Klik op de knop **OK**.

- Voor *Doe het volgende..., kies: **Redirect the message to...**

    1. Selecteer: **de volgende connector**.
    2. Selecteer uw **optie Uitgaand naar Cisco CES**-connector.
    3. Klik op **OK**.

- Ga terug naar "*Doe het volgende..." en voer een tweede handeling in:

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

        - Kies: **set the message header**
        - Stel de berichtkop in: **X-OUTBOUND-AUTH**.
        - Klik op de knop **OK**.
        - Stel de waarde in: **mysecretkey**.

- Klik op de knop **OK**.

- Klik op de knop **Save**.

Opmerking: Om te voorkomen dat onbevoegde berichten van Microsoft worden verzonden, kan een geheime x-header worden afgestempeld wanneer berichten uw Microsoft 365-domein verlaten; deze header wordt geëvalueerd en verwijderd voor levering op het internet.

Een voorbeeld van hoe uw Microsoft 365 Routing-configuratie eruit ziet:

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

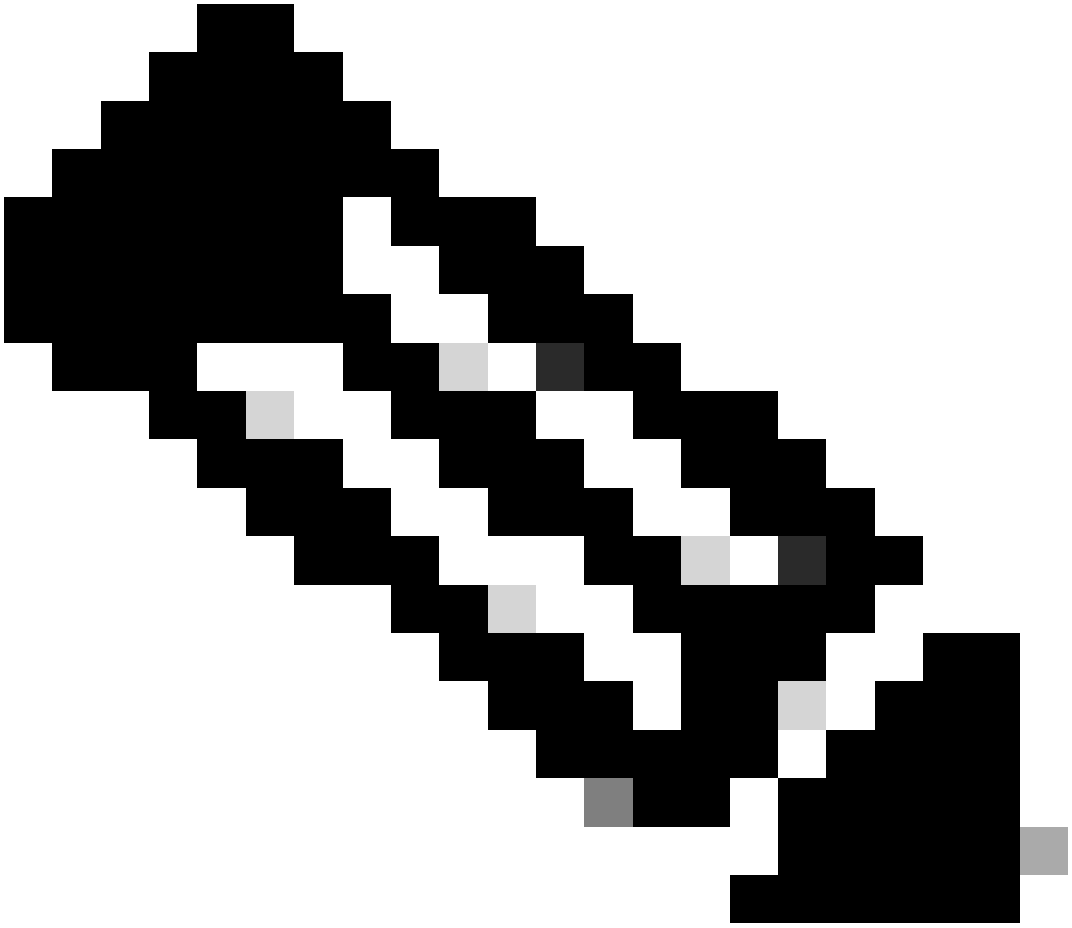
PCI

Comments:

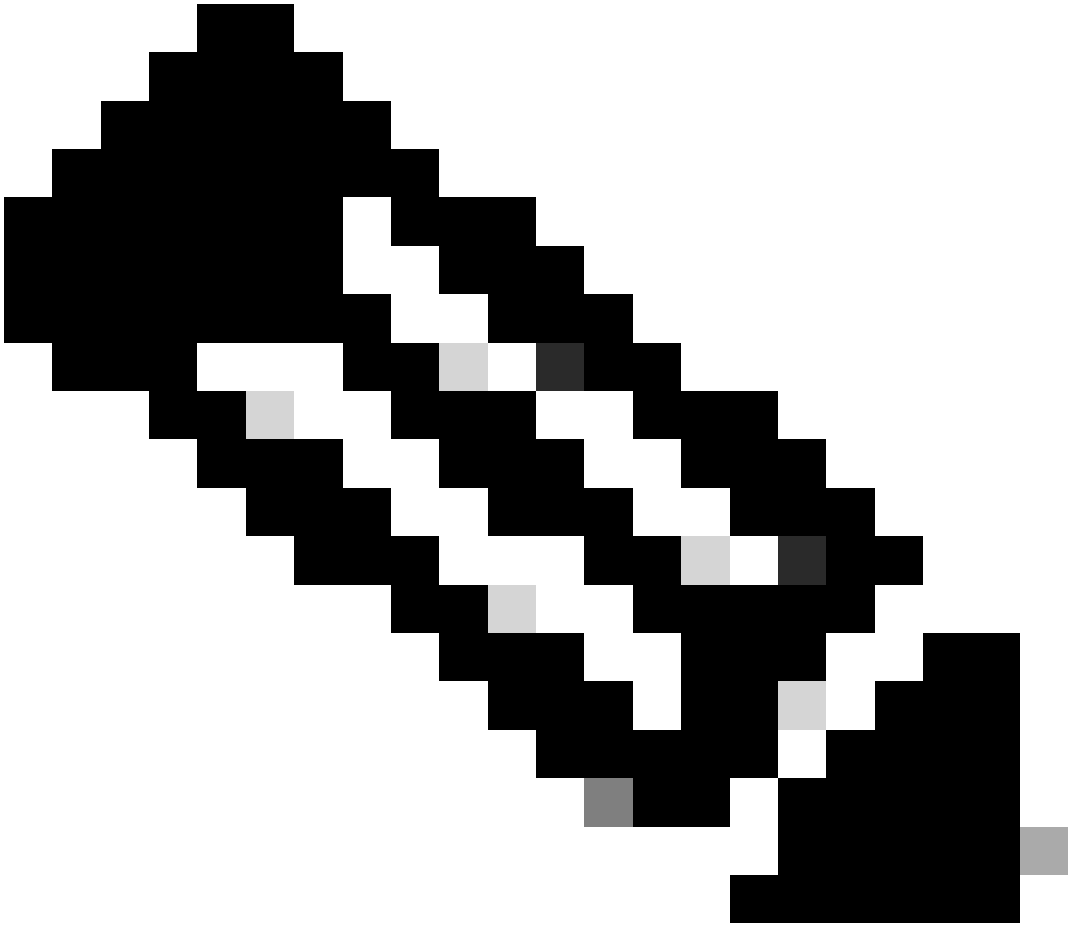
ℹ Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

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

- Druk één keer op Enter om een nieuwe lege regel te maken.
- Voer **[.]** op de nieuwe regel uw nieuwe berichtfilter in.
- Klik op **return** een keer om het menu Filters te verlaten.
- Voer de **Commit** opdracht uit om de wijzigingen in de configuratie op te slaan.



Opmerking: Vermijd speciale tekens voor de geheime sleutel. De ^ en $ in het berichtfilter zijn regex-tekens en gebruik zoals in het voorbeeld.



Opmerking: Controleer de naam van de configuratie van uw RELAYLIST. Het kan worden geconfigureerd met een alternatieve naam, of u kunt een specifieke naam hebben op basis van uw relay beleid of mail provider.

Uitgaande e-mail testen

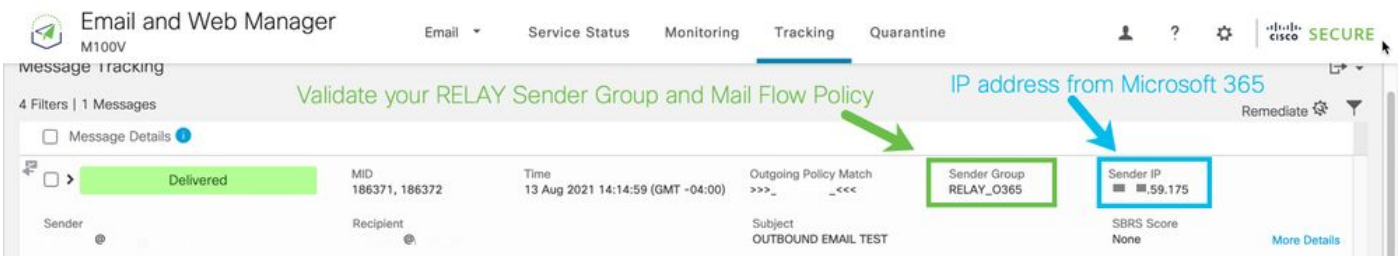
Test uitgaande post van uw Microsoft 365 e-mailadres naar een externe domeinontvanger. U kunt de Berichttracering vanuit uw Cisco Secure Email and Web Manager bekijken om er zeker van te zijn dat deze correct wordt verzonden.

Opmerking: controleer uw TLS-configuratie (**systeembeheer > SSL-configuratie**) op de gateway en de algoritmen die voor uitgaande

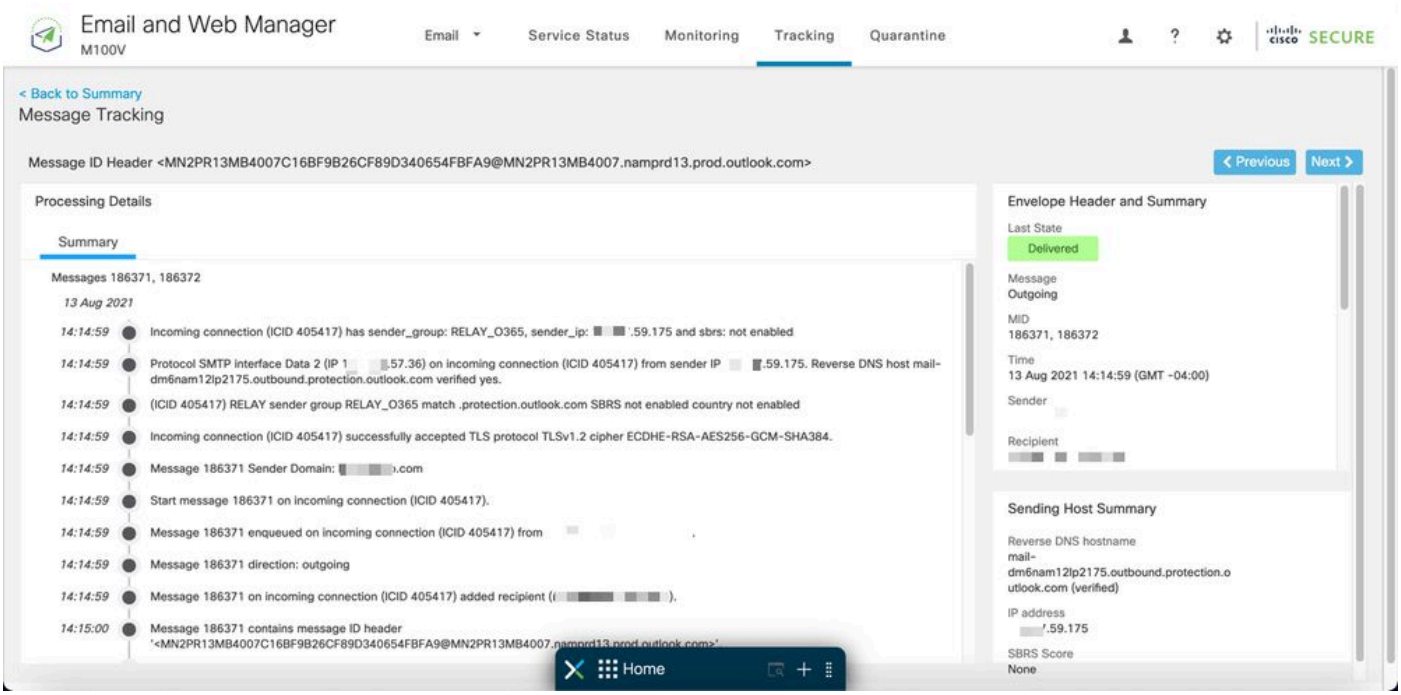
SMTP worden gebruikt. Aanbevolen door Cisco Best Practices:

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

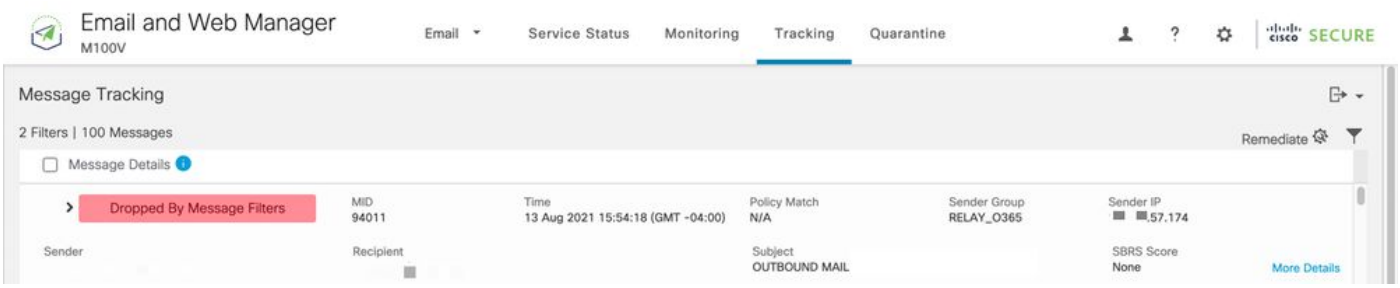
Een voorbeeld van Tracking (Tracering) met succesvolle levering:

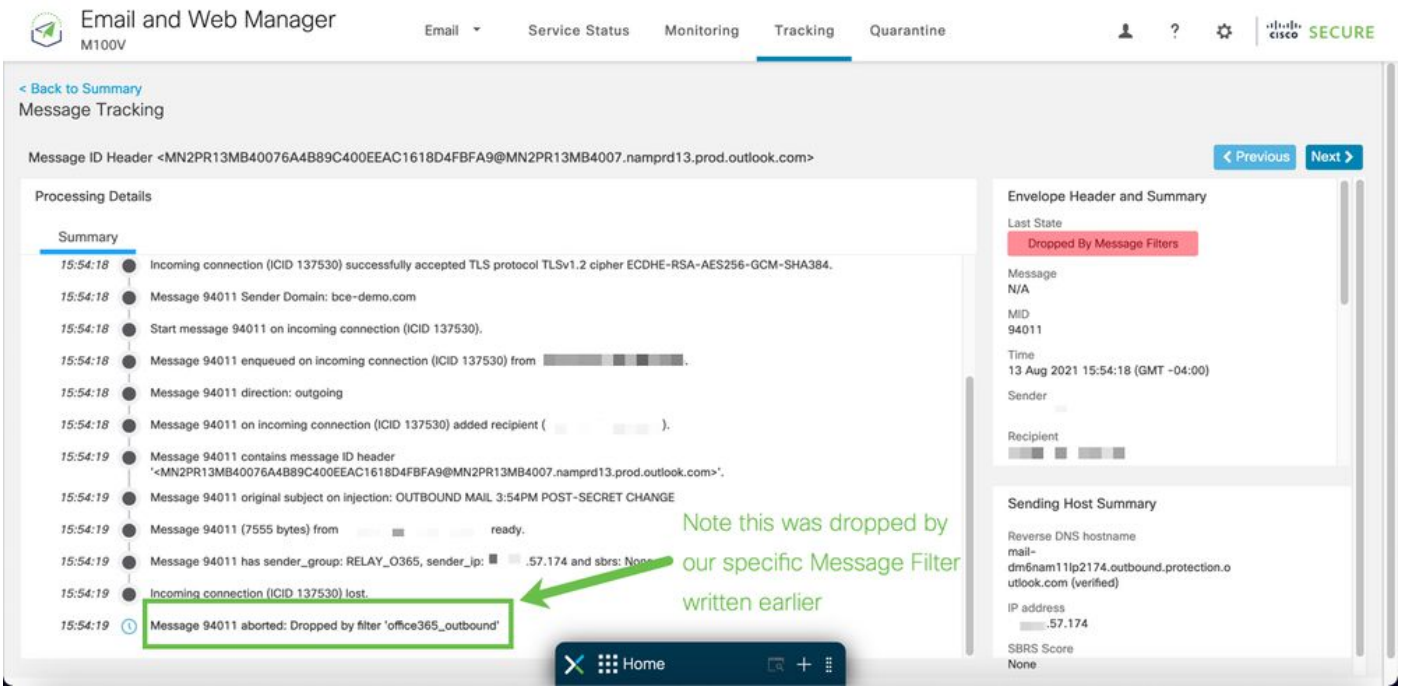


Klik **More Details** om de volledige berichtdetails te zien:



Een voorbeeld van berichttracering waarbij de x-header niet overeenkomt:





Gerelateerde informatie

Cisco Secure E-mail gateway-documentatie

- Release-opmerkingen
- Gebruikershandleiding
- CLI-referentiegids
- API-programmeerhandleidingen voor Cisco Secure Email Gateway
- Open bron die in Cisco Secure Email Gateway wordt gebruikt
- Installatiehandleiding voor Cisco Content Security virtuele applicatie (inclusief vESA)

Documentatie voor beveiligde e-mail met Cloud Gateway

- Release-opmerkingen
- Gebruikershandleiding

Cisco Secure Email en Web Manager-documentatie

- Releaseopmerkingen en compatibiliteitsmatrix

    - Gebruikershandleiding
- API-programmeerhandleidingen voor Cisco Secure Email and Web Manager
- Installatiehandleiding voor Cisco Content Security virtuele applicatie (inclusief vSMA)

Cisco beveiligde productdocumentatie

- Cisco Secure-portfolio-naamgevingsarchitectuur

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.