Secure Email로 Microsoft 365 구성

목차

소개

이 문서에서는 인바운드 및 아웃바운드 이메일 전달을 위해 Microsoft 365를 Cisco Secure Email과 통합하는 컨피그레이션 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Email Gateway 또는 Cloud Gateway
- Cisco Secure Email Cloud Gateway 환경에 대한 CLI(Command Line Interface) 액세스

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

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서는 온프레미스 게이트웨이 또는 Cisco 클라우드 게이트웨이에 사용할 수 있습니다.

Cisco Secure Email 관리자라면 환영 편지에 클라우드 게이트웨이 IP 주소 및 기타 관련 정보가 포함됩니다. 여기에 표시되는 편지 외에도, 할당에 대해 프로비저닝된 클라우드 게이트웨이(ESA라고도 함) 및 클라우드 이메일 및 웹 관리자(SMA라고도 함) 수에 대한 추가 세부 정보를 제공하는 암호화된 이메일이 전송됩니다. 편지를 받지 못했거나 사본을 가지고 있지 않은 경우, 서비스 중인 연락처 정보 및 도메인 이름으로 문의하십시오ces-activations@cisco.com.

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

각 클라이언트에는 전용 IP가 있습니다. Microsoft 365 설정에서 할당된 IP 또는 호스트 이름을 사용할 수 있습니다.

참고: 컨피그레이션은 Microsoft 365 Exchange 콘솔에서 복제하는 데 시간이 걸리기 때문에 계획된 프로덕션 메일 컷오버 전에 테스트하는 것이 좋습니다. 적어도 모든 변경 사항이 적용되려면 1시간은 허용됩니다.

참고: 화면 캡처의 IP 주소는 할당에 프로비저닝된 클라우드 게이트웨이의 수에 비례합니다. 예를 들어 xxx.yy.140.105 xxx.yy.150.1143 는 게이트웨이 1의 데이터 1 인터페이스 IP 주소이고, 게이트웨이 2의 데이터 1 인터페이스 IP 주소입니다. 게이트웨이 1의 데이터 2 인터페이스 IP 주소는 xxx.yy.143.186 이고, 게이트웨이 2의 데이터 2 인터페이스 IP 주소는 입니다 xxx.yy.32.98. 환영 서신에 데이터 2(발신 인터페이스 IP)에 대한 정보가 포함되어 있지 않은 경우 Cisco TAC에 문의하여 할당에 추가된 데이터 2 인터페이스를 받으십시오.

Secure Email로 Microsoft 365 구성

Cisco Secure Email에서 Microsoft 365로 수신되는 이메일 설정

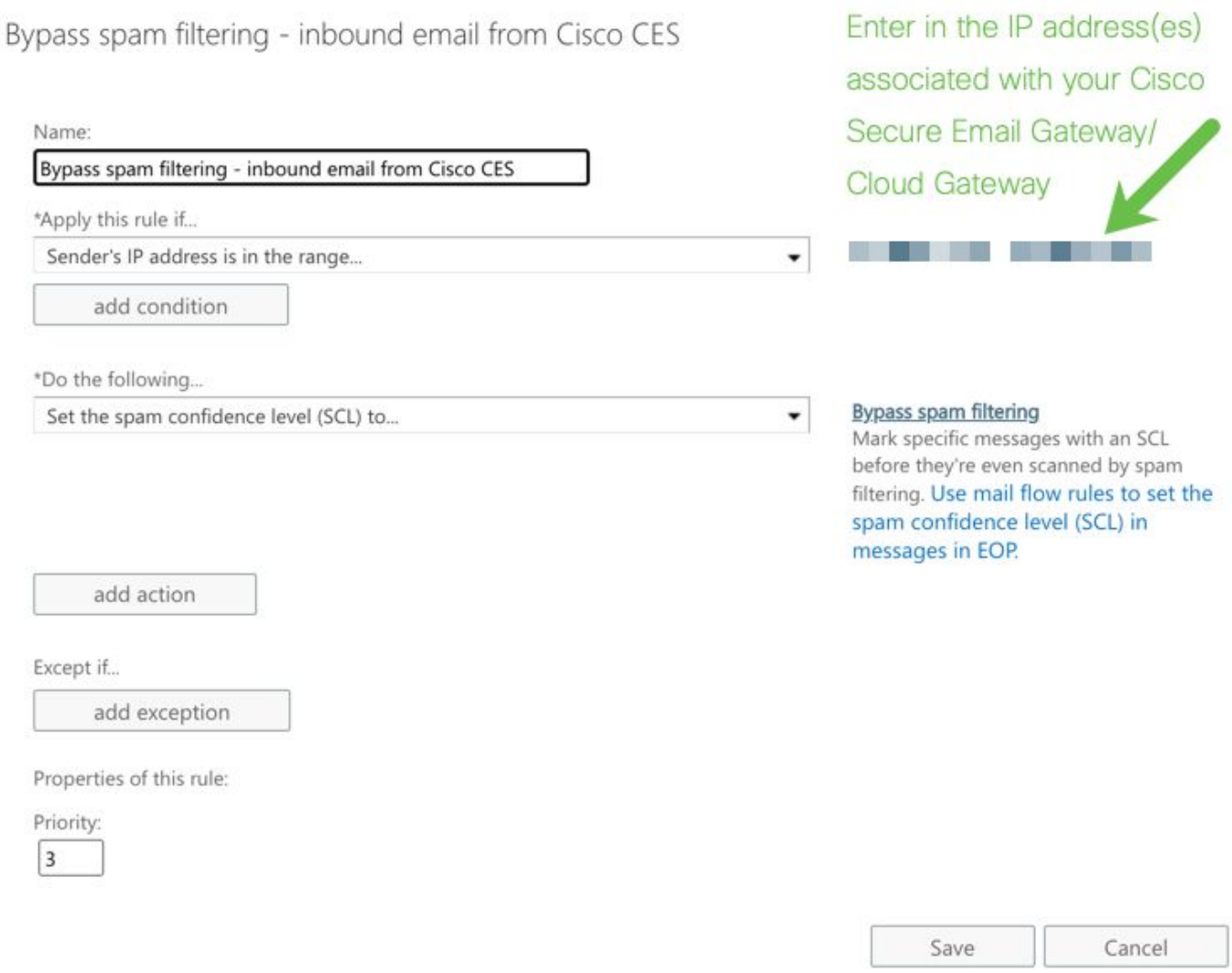
스팸 필터링 규칙 우회

- Microsoft 365 Admin Center(https://portal.microsoft.com)에 로그인합니다.
- 왼쪽 메뉴에서 **Admin Centers**.
- 클릭 **Exchange**.
- 왼쪽 메뉴에서 **Mail flow** > **Rules**.
- 새 규칙 **[+]** 을 생성하려면 클릭합니다.
- 드롭다운 목록**Bypass spam filtering...** 에서 선택합니다.
- 새 규칙의 이름 입력: **Bypass spam filtering - inbound email from Cisco CES**.
- *이 규칙 적용...에서 다음을 선택합니다. **The sender - IP address is in any of these ranges or exactly matches**.

  1. Specify IP address ranges(IP 주소 범위 지정) 팝업창에서 Cisco Secure Email 환영 편지에 제공된 IP 주소를 추가합니다.
  2. 클릭 **OK**.

- *다음을 수행..., 새 규칙이 미리 선택되었습니다. **Set the spam confidence level (SCL) to... - Bypass spam filtering**.
- 클릭 **Save**.

규칙의 예:



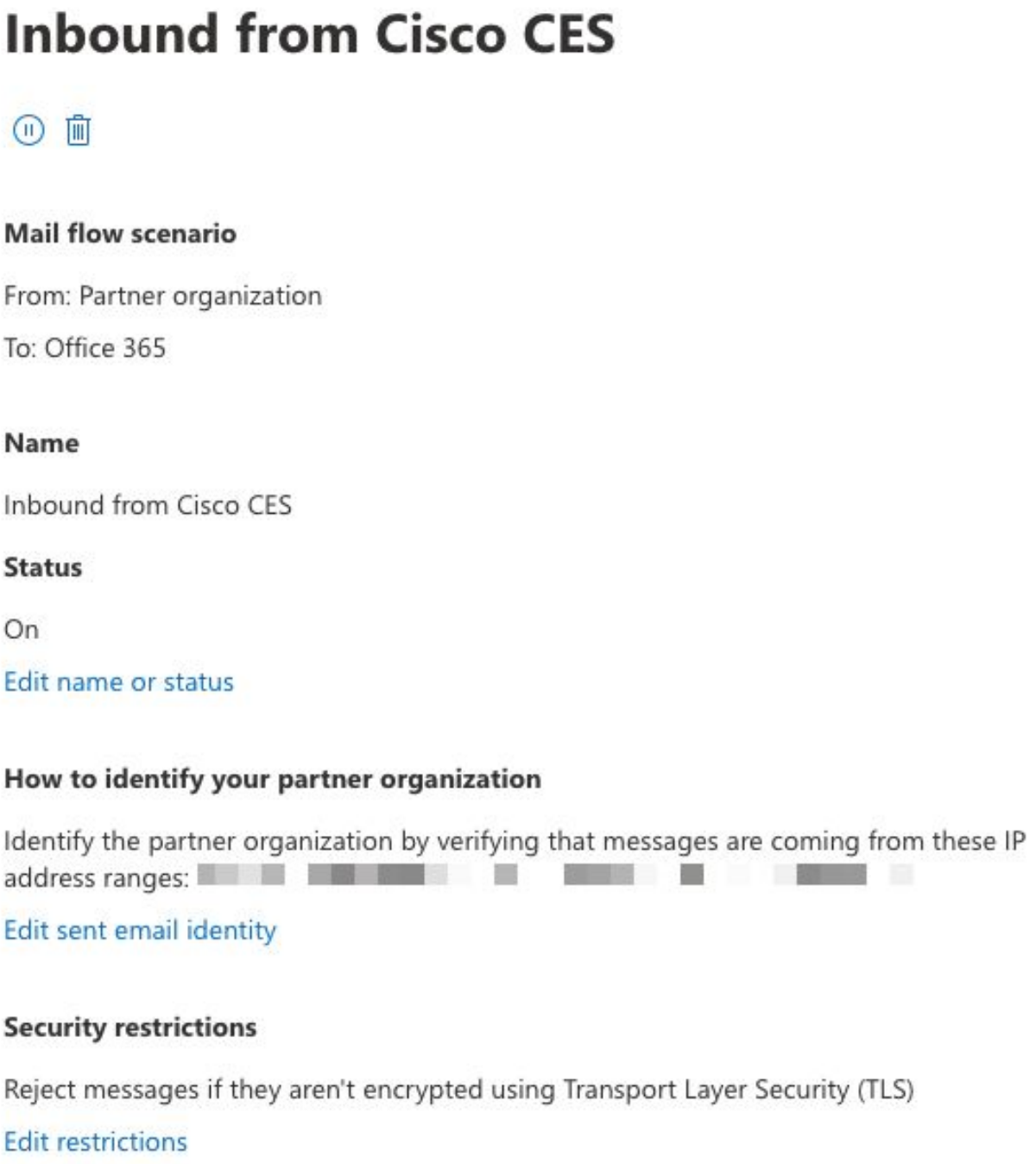
수신 커넥터

- Exchange Admin Center에 남아 있습니다.
- 왼쪽 메뉴에서 **Mail flow** > **Connectors**.
- 새 커넥터 **[+]** 를 생성하려면 를 클릭합니다.
- Select your mail flow scenario 팝업 창에서 다음을 선택합니다.

1. 발신: Partner organization
    - 수신: **Office365**

- 클릭 **Next**.
- 새 커넥터의 이름을 입력합니다. **Inbound from Cisco CES**.
- 원하는 경우 설명을 입력합니다.
- 클릭 **Next**.
- 클릭 **Use the sender's IP address**.
- 클릭 **Next**.
- Cisco Secure **[+]** Email 환영 서신에 표시된 IP 주소를 클릭하여 입력합니다.
- 클릭 **Next**.
- 선택 **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- 클릭 **Next**.
- 클릭 **Save**.

커넥터 컨피그레이션의 예:



Cisco Secure Email에서 Microsoft 365로 이메일 설정

대상 제어

Destination Controls(대상 제어)의 전달 도메인에 자체 스로틀을 적용합니다. 물론 나중에 스로틀을 제거할 수도 있지만 이는 Microsoft 365에 대한 새로운 IP이며 Microsoft의 알려지지 않은 평판 때문에 스로틀링을 원하지 않습니다.

- 게이트웨이에 로그인합니다.
- 탐색 **Mail Policies** > **Destination Controls**.
- 클릭 **Add Destination**.

- Use:

1. Destination(대상): 도메인 이름 입력

2. 동시 연결: **10**

   - 연결당 최대 메시지 수: **20**
   - TLS 지원: **Preferred**

- 클릭 **Submit**.
- 컨피그레이션 변경 사항**Commit Changes** 을 저장하려면 UI(사용자 인터페이스)의 오른쪽 상단을 클릭합니다.

Destination Control Table(대상 제어 테이블) 모양을 보여 주는 예:

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.

수신자 액세스 테이블

다음으로 도메인에 대해 메일을 수락하도록 RAT(Recipient Access Table)를 설정합니다.

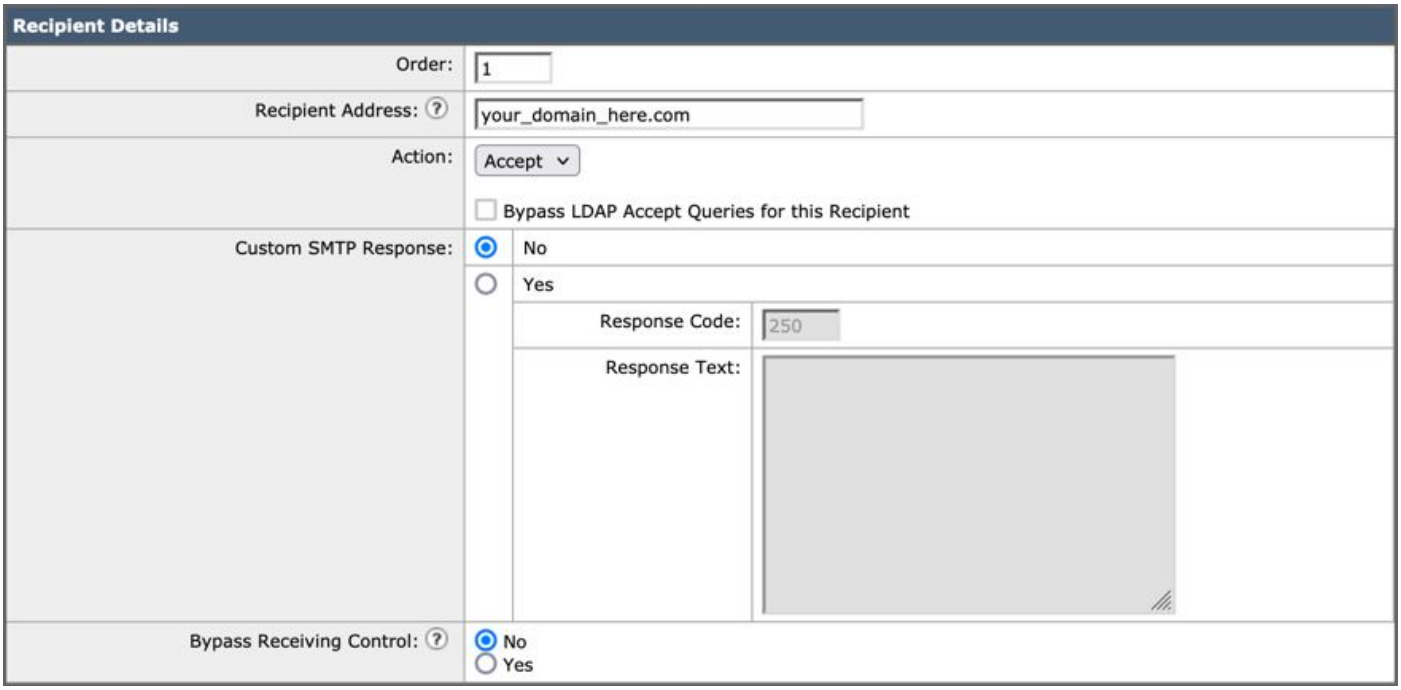
- 탐색 **Mail Policies** > **Recipient Access Table (RAT)**.

> **참고**: 기본 메일 흐름에 대한 리스너의 실제 이름을 기반으로 리스너가 수신 리스너, IncomingMail 또는 MailFlow에 대한 리스너인지 확인합니다.

- 클릭 **Add Recipient**.
- Recipient Address 필드에 도메인을 추가합니다.
- 기본 작업 선택 **Accept**.

- 클릭 **Submit**.
- UI**Commit Changes** 의 오른쪽 상단을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

RAT 항목의 예:

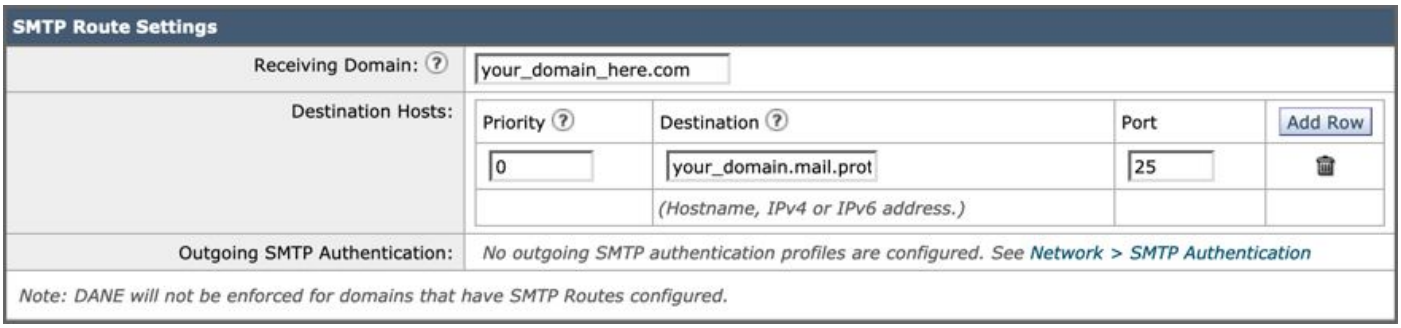


SMTP 경로

Cisco Secure Email에서 Microsoft 365 도메인으로 메일을 전달하도록 SMTP 경로를 설정합니다.

- 탐색 **Network > SMTP Routes**.
- 클릭 **Add Route...**
- Receiving Domain(수신 도메인): 도메인 이름을 입력합니다.
- 대상 호스트: 원래 Microsoft 365 MX 레코드를 추가합니다.
- 클릭 **Submit**.
- UI**Commit Changes** 의 오른쪽 상단을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

SMTP 경로 설정의 예:



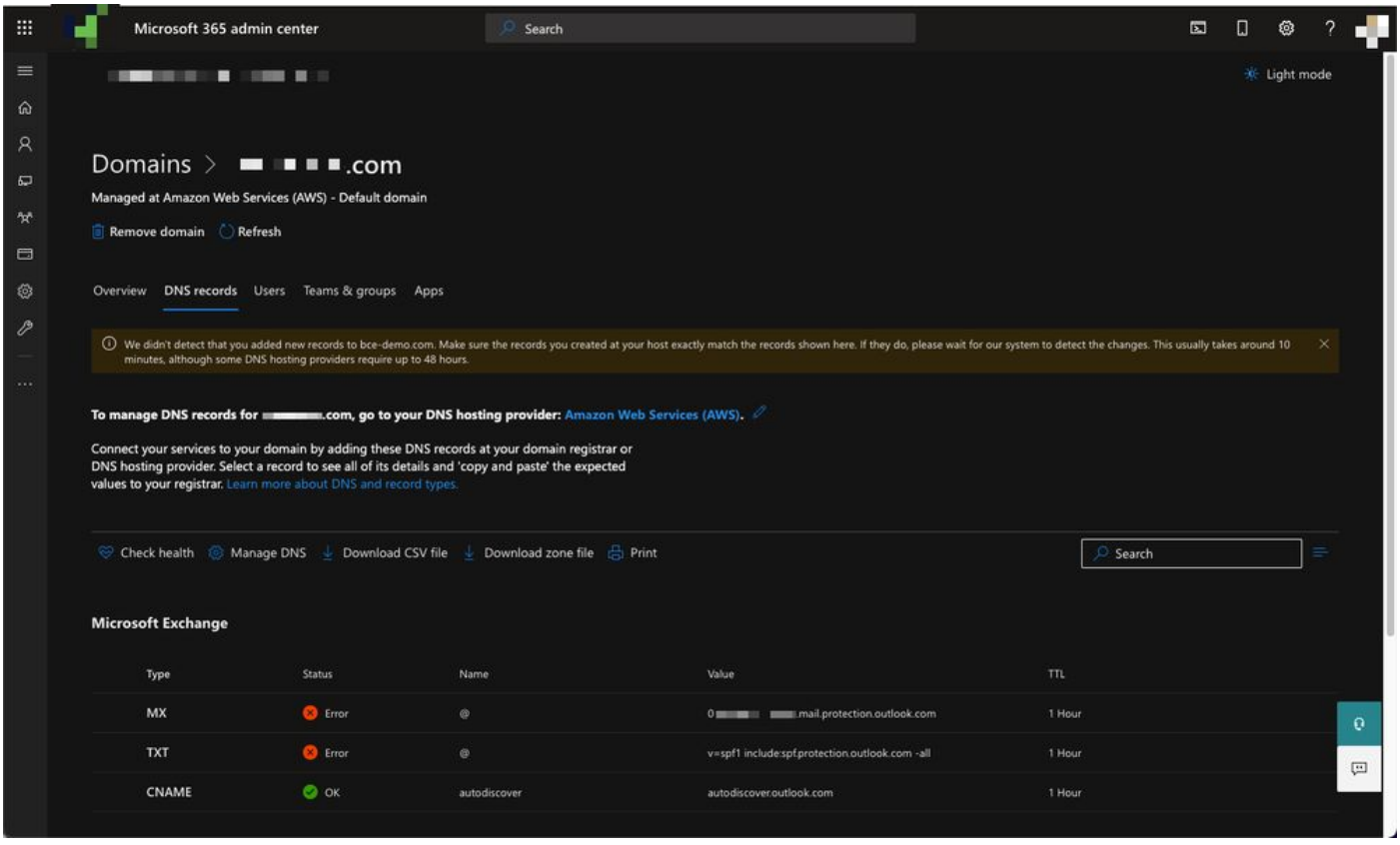
DNS(MX 레코드) 설정

MX(Mail Exchange) 레코드 변경을 통해 도메인을 제거할 준비가 되었습니다. DNS 관리자와 함께 Cisco Secure Email Cloud 인스턴스의 IP 주소에 대한 MX 레코드를 Cisco Secure Email Welcome Letter에 제공된 대로 확인합니다.

또한 Microsoft 365 콘솔에서 MX 레코드의 변경 사항을 확인합니다.

- Microsoft 365 관리 콘솔(https://admin.microsoft.com)에 로그인합니다.
- 탐색 **Home** > **Settings** > **Domains**.
- 기본 도메인 이름을 선택합니다.
- 클릭Check Health.

Microsoft 365가 도메인과 연결된 DNS 및 MX 레코드를 조회하는 방법에 대한 현재 MX 레코드를 제공합니다.



참고: 이 예에서는 DNS가 AWS(Amazon Web Services)에 의해 호스팅되고 관리됩니다. 관리자는 DNS가 Microsoft 365 계정 외부에서 호스팅되는 경우 경고를 표시합니다. 다음과 같은 경고를 무시할 수 있습니다. "your_domain_here.com에 새 레코드를 추가했음을 감지하지 못했습니다. 호스트에서 생성한 레코드가 여기에 표시된 레코드와 일치하는지 확인합니다." 단계별 지침은 MX 레코드를 Microsoft 365 계정으로 리디렉션하도록 처음에 구성된 레코드로 재설정합니다. 이렇게 하면 수신 트래픽 흐름에서 Cisco Secure Email Gateway가 제거됩니다.

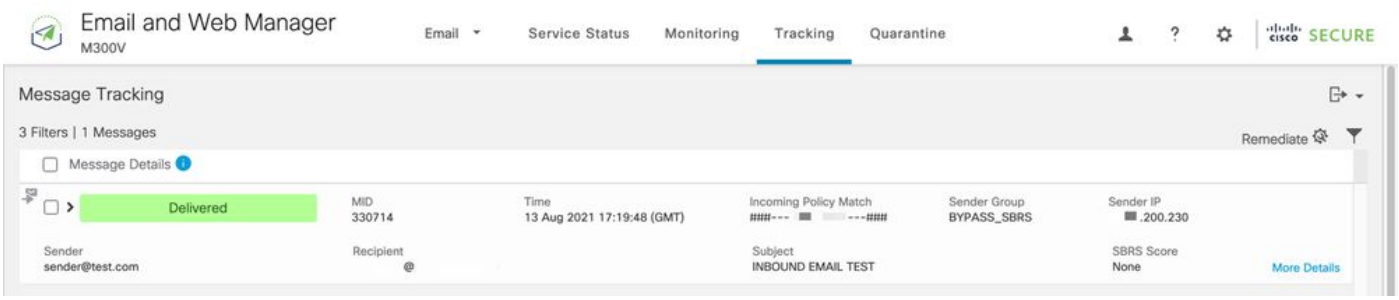
인바운드 이메일 테스트

Microsoft 365 전자 메일 주소로 보내는 인바운드 메일을 테스트합니다. 그런 다음 Microsoft 365 전자 메일 받은 편지함에 도착하는지 확인합니다.

인스턴스와 함께 제공된 Cisco Secure Email and Web Manager(SMA라고도 함)에서 메시지 추적의 메일 로그를 확인합니다.

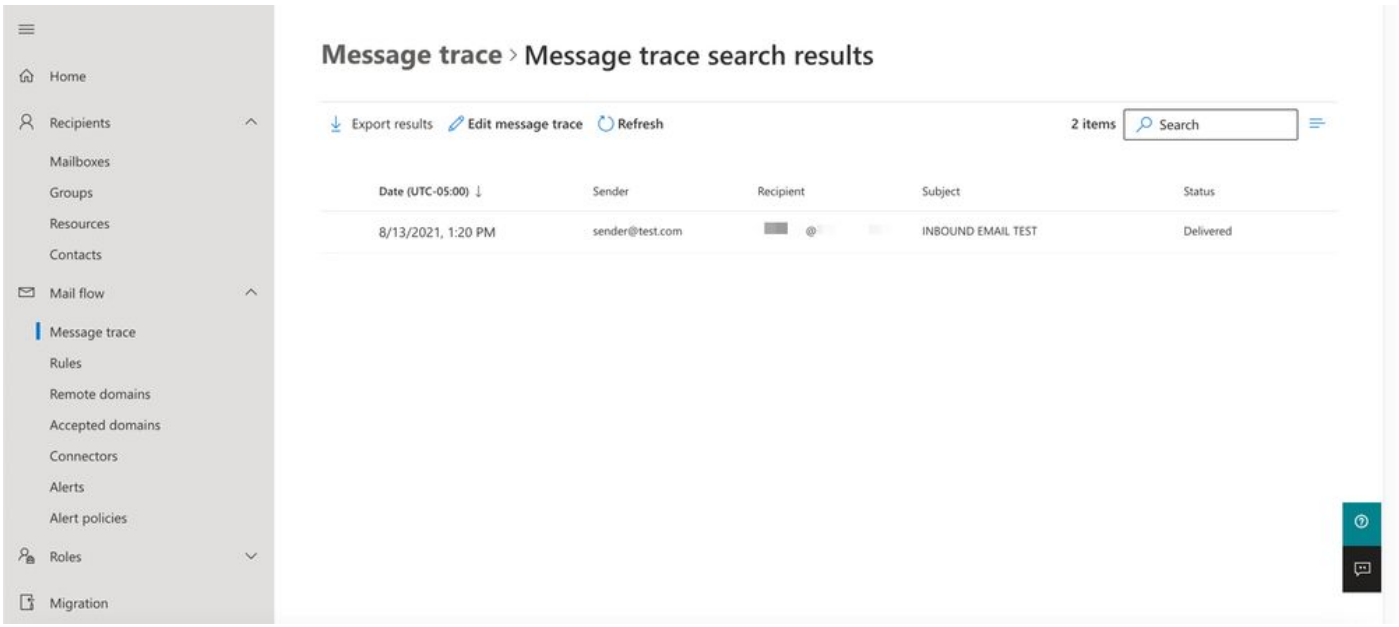
SMA에서 메일 로그 보기:

- SMA에 로그인합니다(https://sma.iphmx.com/ng-login).
- 클릭 **Tracking**.
- 필요한 검색 기준을 입력하고 를 **Search**클릭하면 다음과 같은 결과가 표시됩니다.



Microsoft 365에서 메일 로그 보기:

- Microsoft 365 Admin Center(https://admin.microsoft.com)에 로그인합니다.
- Expand **Admin Centers**.
- 클릭 **Exchange**.
- 탐색 **Mail flow** > **Message trace**.
- Microsoft는 검색할 기본 조건을 제공합니다. 예를 들어, 검색 쿼리를 시작하도록 선택합니다 **Messages received by my primary domain in the last day**.
- 수신자에 필요한 검색 조건을 입력하고 을 클릭하면 다음 **Search** 과 유사한 결과가 표시됩니다.



Microsoft 365에서 Cisco Secure Email로 발신되는 이메일 설정

Cisco Secure Email Gateway에서 RELAYLIST 설정

Cisco Secure Email 환영 서신을 참조하십시오. 또한 게이트웨이를 통한 아웃바운드 메시지에 대해 보조 인터페이스가 지정됩니다.

- 게이트웨이에 로그인합니다.
- 탐색 **Mail Policies** > **HAT Overview**.

> **참고**: 외부/아웃바운드 메일 흐름에 대한 리스너의 실제 이름을 기반으로 리스너가 Outgoing Listener, OutgoingMail 또는 MailFlow-Ext에 대한 리스너인지 확인합니다.

- 클릭 **Add Sender Group...**
- 발신자 그룹을 다음과 같이 설정합니다.

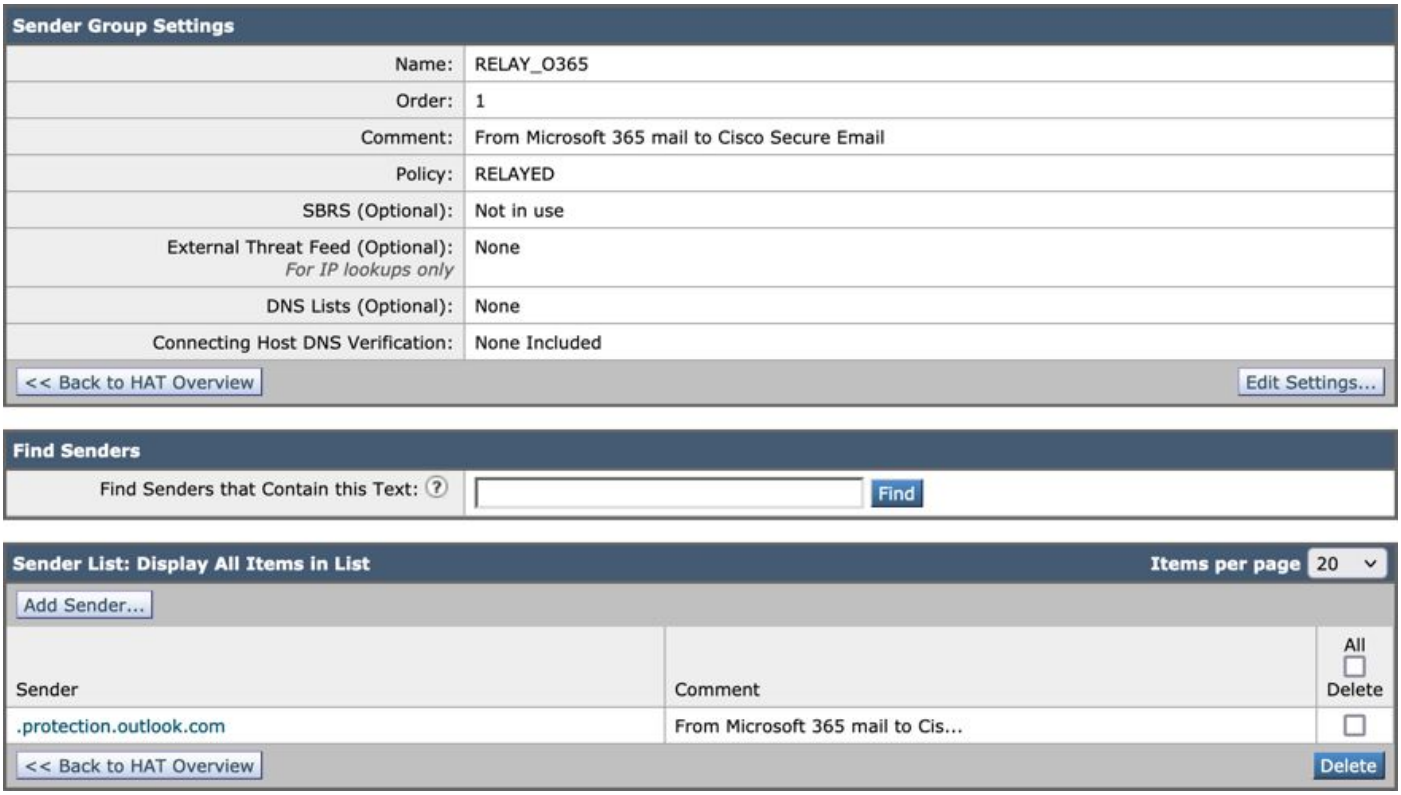
1. 이름: RELAY_O365
2. 설명: <<발신자 그룹에 메모를 남기려면 설명을 입력하십시오.>>
3. 정책: RELAYED
4. 클릭 **Submit and Add Senders**.

- 보낸 사람: **.protection.outlook.com**

> **참고**: **.** 발신자 도메인 이름의 시작 부분에 (점)이 필요합니다.

- 클릭 **Submit**.
- UI**Commit Changes** 의 오른쪽 상단을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

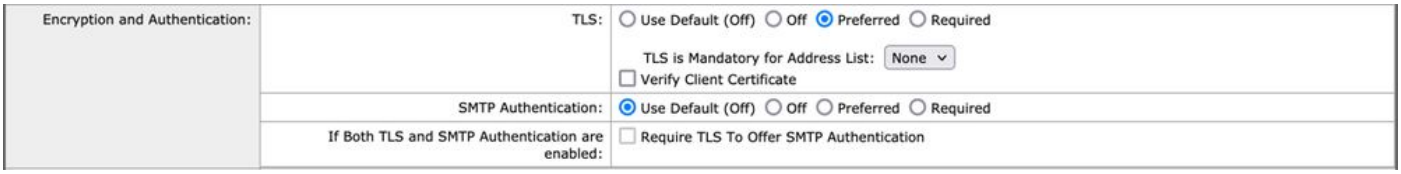
Sender Group 설정의 예:



TLS 활성화

- 클릭 <<**Back to HAT Overview**.
- 다음과 같은 이름의 메일 흐름 정책을 클릭합니다. **RELAYED**.
- 아래로 스크롤하여 섹션을 **Security Features** 살펴봅니다. **Encryption and Authentication**.
- TLS의 경우 다음을 선택합니다. **Preferred**.
- 클릭 **Submit**.
- UI**Commit Changes** 의 오른쪽 상단을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

메일 플로우 정책 컨피그레이션의 예:



Microsoft 365에서 CES로 메일 설정

- Microsoft 365 Admin Center(https://admin.microsoft.com)에 로그인합니다.
- Expand **Admin Centers**.
- 클릭 **Exchange**.
- 탐색 **Mail flow** > **Connectors**.
- 새 커넥터를 생성하려면 를 클릭합니다[+].
- Select your mail flow scenario 팝업 창에서 다음을 선택합니다.

1. 발신: Office365
    - 수신:Partner organization

- 클릭 **Next**.
- 새 커넥터의 이름을 입력합니다. **Outbound to Cisco CES**.
- 원하는 경우 설명을 입력합니다.
- 클릭 **Next**.
- 이 커넥터를 언제 사용하시겠습니까?:

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

- 클릭 **Route email through these smart hosts**.
- CES **[+]** 환영 서신에 제공된 아웃바운드 IP 주소 또는 호스트 이름을 클릭하여 입력합니다.
- 클릭 **Save**.
- 클릭 **Next**.
- Office 365를 파트너 조직의 전자 메일 서버에 연결하려면 어떻게 해야 합니까?

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

    - 선택합니다Any digital certificate, including self-signed certificates.
    - 클릭 **Next**.

- 확인 화면이 나타납니다.
- 클릭 **Next**.
- 올바른 이메일 주소 **[+]** 를 입력하고 **OK**.
- 를 **Validate** 클릭하고 유효성 검사를 실행할 수 있도록 허용합니다.
- 완료되면 다음을 클릭합니다. **Close**.
- 클릭Save.

아웃바운드 커넥터의 예를 들면 다음과 같습니다.

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

메일 흐름 규칙 생성

1. Select sender location(발신자 위치 선택) 팝업에서 다음을 선택합니다. **Inside the organization**.

    - 클릭 **OK**.

- 클릭 **More options...**
- 단추 **add condition** 를 클릭하고 두 번째 조건을 삽입합니다.

    1. 선택 **The recipient...**

        - 선택: **Is external/internal**.
        - Select sender location(발신자 위치 선택) 팝업에서 다음을 선택합니다. **Outside the organization** .
        - 클릭 **OK**.

- *다음 작업 수행...에서 다음을 선택합니다. **Redirect the message to...**

    1. 선택: **다음 커넥터**.

    2. Outbound to **Cisco CES Connector(Cisco CES로 아웃바운드)**를 선택합니다.

    3. **OK(확인)**를 클릭합니다.

- "*다음 작업 수행..."으로 돌아가서 두 번째 작업을 삽입합니다.

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

        - 선택: **set the message header**
        - 메시지 헤더 설정: **X-OUTBOUND-AUTH**.
        - 클릭 **OK**.
        - 값 설정: **mysecretkey**.

- 클릭 **OK**.

- 클릭 **Save**.

참고: Microsoft에서 무단 메시지를 방지하기 위해 메시지가 Microsoft 365 도메인을 떠날 때 비밀 x-헤더에 스탬프를 적용할 수 있습니다. 이 헤더는 인터넷으로 전달되기 전에 평가 및 제거됩니다.

Microsoft 365 라우팅 구성의 예:

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

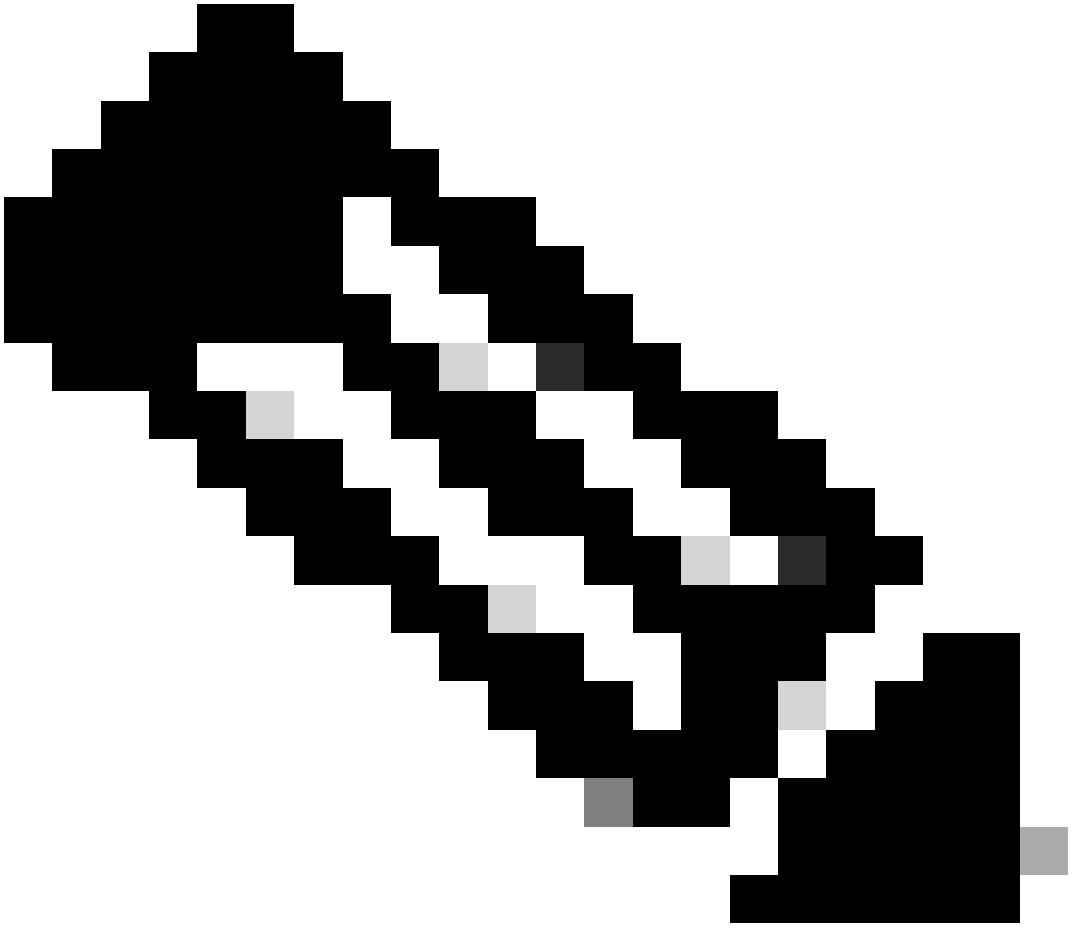
PCI

Comments:

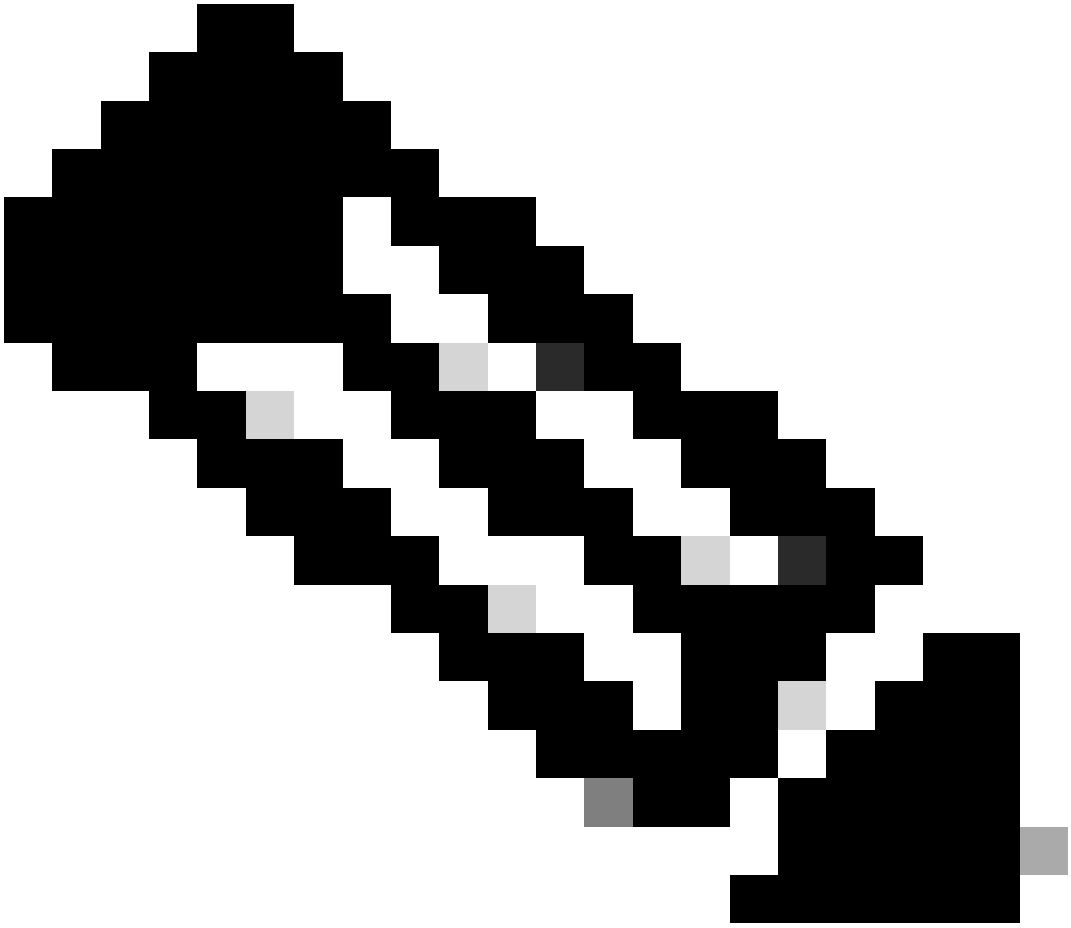
ℹ Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

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

- return 키를 한 번 눌러 빈 줄을 새로 만듭니다.
- 새 메시지 필터 **[.]** 를 종료하려면 새 줄에 을 입력합니다.
- Filters(필터) 메뉴를 종료하려면 **return** 한 번 클릭합니다.
- 명령을 **Commit** 실행하여 컨피그레이션에 변경 사항을 저장합니다.



참고: 비밀 키에 특수 문자를 사용하지 마십시오. 메시지 필터에 표시된 ^ 및 $는 regex 문자이며 예제에 제공된 대로 사용합니다.



참고: RELAYLIST가 구성된 방법의 이름을 검토하십시오. 대체 이름으로 구성할 수도 있고, 릴레이 정책 또는 메일 공급자에 따라 특정 이름을 가질 수도 있습니다.

아웃바운드 이메일 테스트

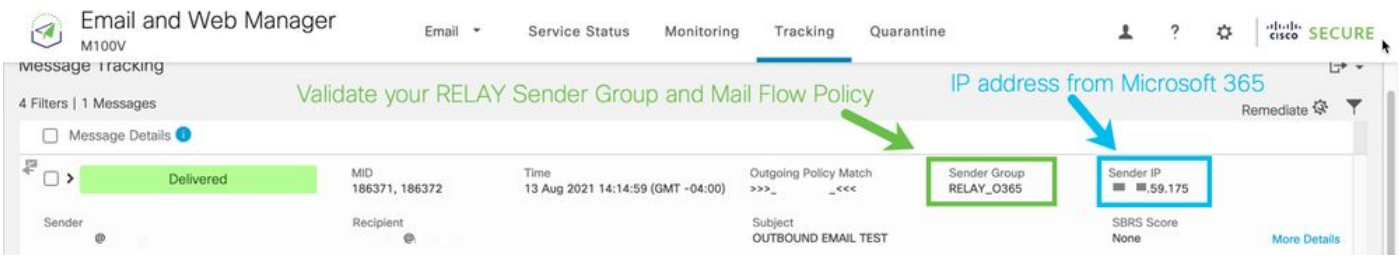
Microsoft 365 전자 메일 주소에서 외부 도메인 받는 사람에게 보내는 아웃바운드 메일을 테스트합니다. Cisco Secure Email and Web Manager에서 메시지 추적을 검토하여 적절하게 아웃바운드로 라우팅되었는지 확인할 수 있습니다.

참고: 게이트웨이의 TLS 구성(**System Administration(시스템 관리) > SSL 구성**)과 아웃바운드 SMTP에 사용되는 암호를 검

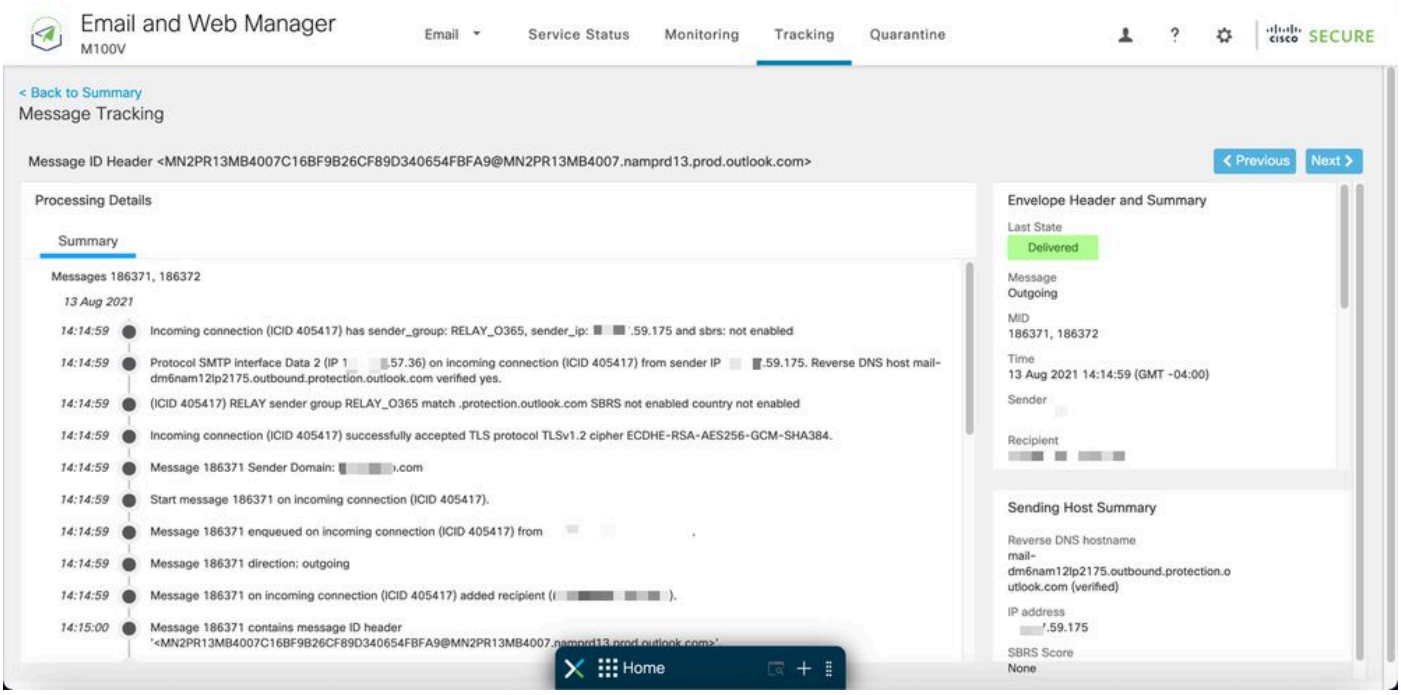
토합니다. Cisco Best Practice에서는 다음을 권장합니다.

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

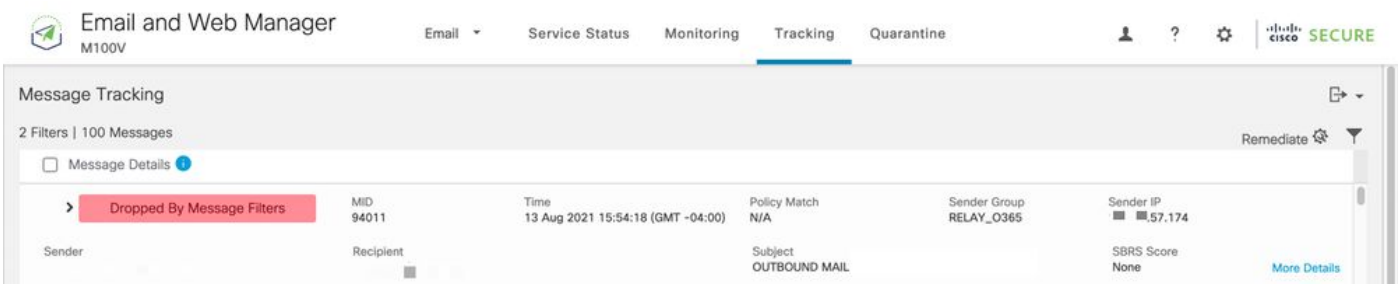
성공적인 전달 추적의 예시:

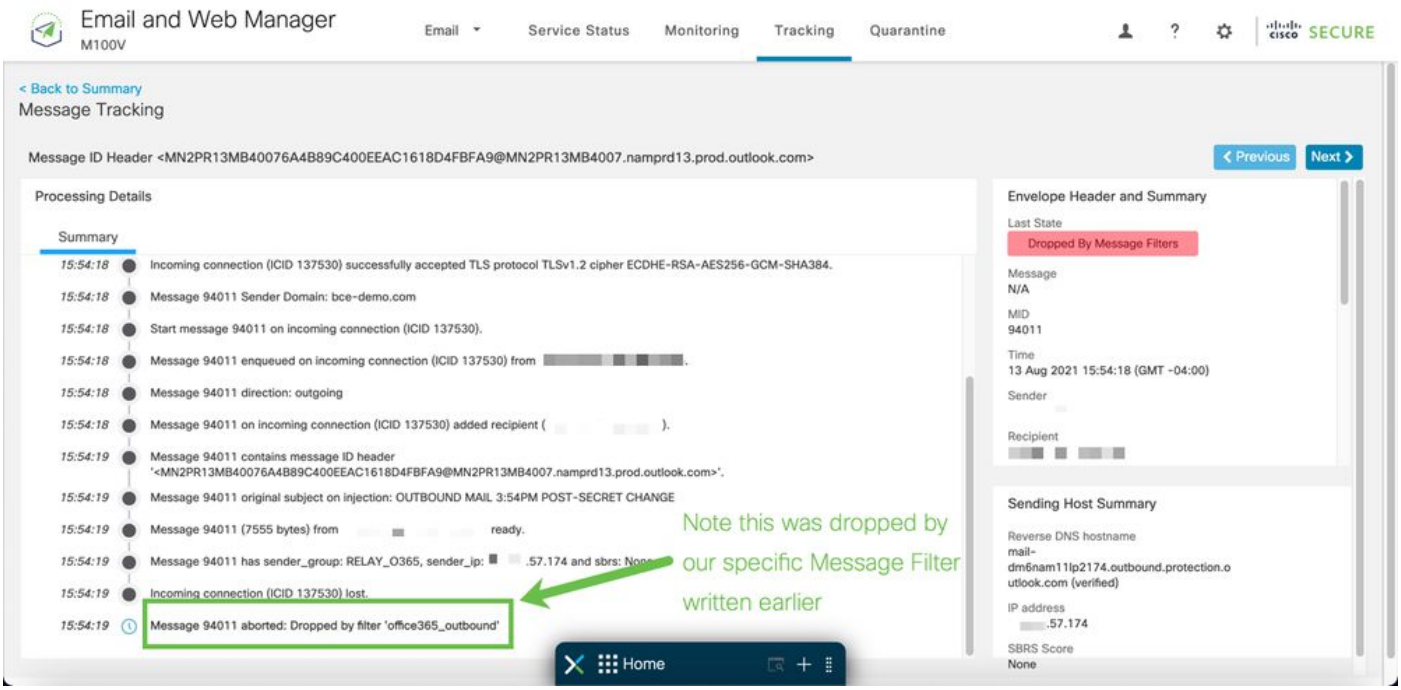


전체 메시지 세부사항**More Details** 을 보려면 클릭하십시오.



x-헤더가 일치하지 않는 메시지 추적의 예시:





관련 정보

Cisco Secure Email Gateway 설명서

- 릴리스 정보
- 사용 설명서
- CLI 참조 가이드
- Cisco Secure Email Gateway용 API 프로그래밍 가이드
- Cisco Secure Email Gateway에서 사용되는 오픈 소스
- Cisco Content Security Virtual Appliance 설치 설명서(vESA 포함)

Secure Email Cloud Gateway 설명서

- 릴리스 정보
- 사용 설명서

Cisco Secure Email and Web Manager 설명서

- 릴리스 정보 및 호환성 매트릭스

- 사용 설명서
- Cisco Secure Email and Web Manager용 API 프로그래밍 가이드
- Cisco Content Security Virtual Appliance 설치 설명서(vSMA 포함)

Cisco Secure Product 문서

- Cisco Secure 포트폴리오 명명 아키텍처

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.