

ESA/CES로 Zoho Mail 구성

목차

[소개](#)

[Zoho 관리 포털에서 게이트웨이 구성](#)

[SMTP 경로](#)

[대상 제어](#)

[DNS\(MX 레코드\) 설정](#)

[Zoho Mail에서 Cisco Secure Email로 메일 구성\(아웃바운드\)](#)

[Cisco Secure Email Gateway에서 RELAYLIST 설정](#)

[TLS 활성화](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 Zoho 메일을 구성하고 Cisco ESA/CES와 통합하는 절차에 대해 설명합니다.

사전 요구 사항

Zoho 대시보드에 대한 실무 지식 및 관리자 액세스.

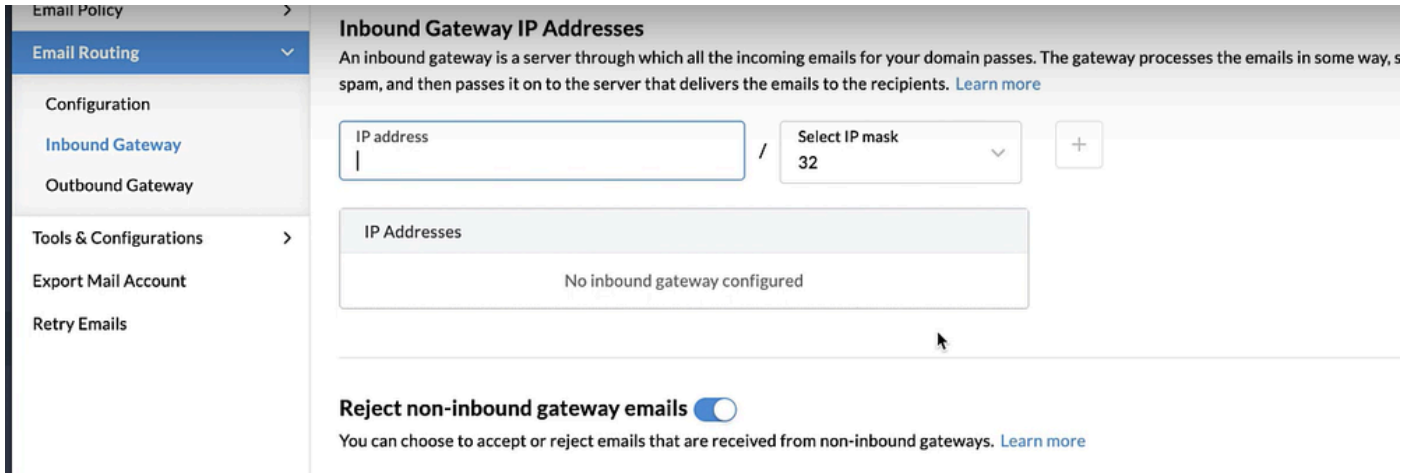
Email Security Appliance에 대한 지식 및 액세스

Zoho 관리 포털에서 게이트웨이 구성

1. Portal(포털) > Mail Settings(메일 설정)로 이동합니다.
2. 인바운드 및 아웃바운드 게이트웨이를 구성합니다.

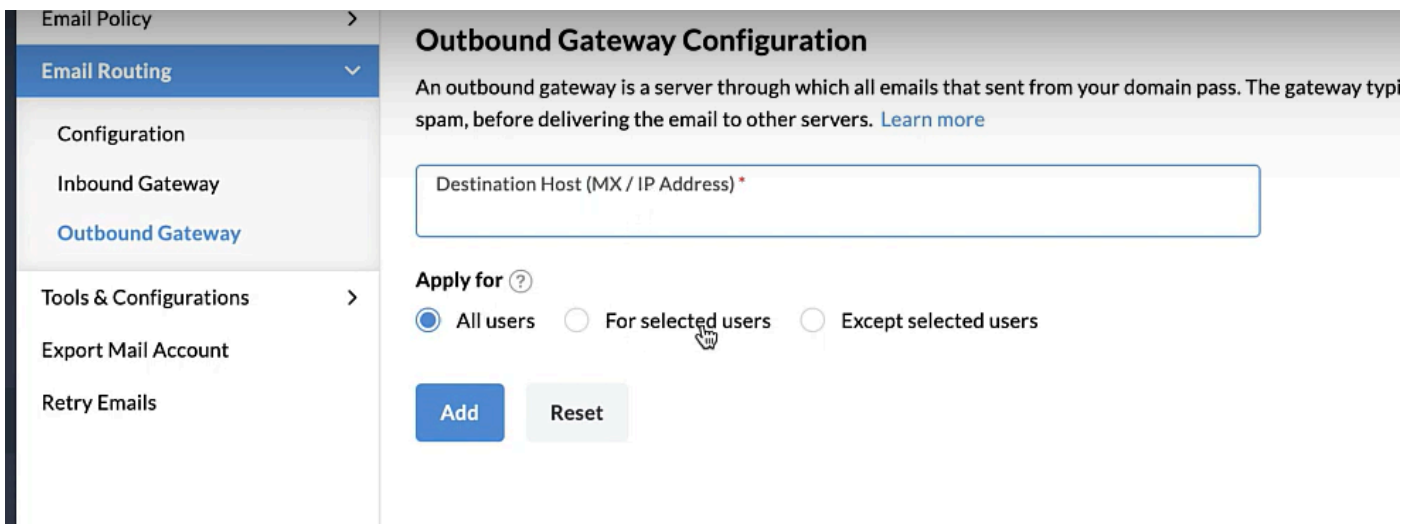
인바운드 게이트웨이:

Zoho 계정에 구성된 도메인에 대한 이메일을 수신하는 Cisco ESA 서버의 IP 주소를 추가합니다



아웃바운드 게이트웨이:

발신 이메일의 대상 호스트(MX 레코드 또는 IP 주소)를 지정합니다.



인바운드 및 아웃바운드 모두에 대해 Cisco Email Gateway 구성

Cisco Secure Email에서 Zoho Mail로 메일 구성(인바운드)

수신자 액세스 테이블

도메인에 대한 메일을 수락하도록 RAT(Recipient Access Table)를 구성합니다.

1. Mail Policies(메일 정책) > Recipient Access Table (RAT)(수신자 액세스 테이블(RAT))로 이동합니다.
2. Add Recipient를 클릭합니다.
3. Recipient Address 필드에 도메인을 추가합니다.

- 기본 작업인 Accept(수락)를 선택합니다.
- Submit(제출)을 클릭합니다.
- UI 오른쪽 상단에서 Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션 변경 사항을 저장합니다.

Recipient Details					
Order:	<input type="text" value="1"/>				
Recipient Address: ?	<input type="text" value="your_domain_here.com"/>				
Action:	Accept ▾				
	<input type="checkbox"/> Bypass LDAP Accept Queries for this Recipient				
Custom SMTP Response:	<input checked="" type="radio"/> No <input type="radio"/> Yes				
	<table border="1"> <tr> <td>Response Code:</td> <td><input type="text" value="250"/></td> </tr> <tr> <td>Response Text:</td> <td><div style="border: 1px solid gray; height: 100px;"></div></td> </tr> </table>	Response Code:	<input type="text" value="250"/>	Response Text:	<div style="border: 1px solid gray; height: 100px;"></div>
Response Code:	<input type="text" value="250"/>				
Response Text:	<div style="border: 1px solid gray; height: 100px;"></div>				
Bypass Receiving Control: ?	<input checked="" type="radio"/> No <input type="radio"/> Yes				

SMTP 경로

Cisco Secure Email에서 Zoho Mail 도메인으로 메일을 전달하도록 SMTP 경로를 설정합니다.

- Network(네트워크) > SMTP Routes(SMTP 경로)로 이동합니다.
- Add Route...를 클릭합니다.
 - 수신 도메인: 도메인 이름 입력.
 - 대상 호스트: 원본 Zoho Mail MX 레코드를 추가합니다.
- Submit(제출)을 클릭합니다.
- UI 오른쪽 상단에서 Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션 변경 사항을 저장합니다.

Add SMTP Route

SMTP Route Settings			
Receiving Domain: ?	<input type="text" value="domain.com"/>		
Destination Hosts:	Priority ?	Destination ?	Port
	<input type="text" value="0"/>	<input type="text" value="server.zoho.com"/>	<input type="text" value="25"/>
	<small>(Hostname, IPv4 or IPv6 address.)</small>		<input type="button" value="Add Row"/>
Outgoing SMTP Authentication:	No outgoing SMTP authentication profiles are configured. See Network > SMTP Authentication		
<small>Note: DANE will not be enforced for domains that have SMTP Routes configured.</small>			

대상 제어

알려지지 않은 평판 때문에 Zoho에 의한 제한을 원하지 않으므로 Destination Controls(대상 제어)의 전달 도메인에 자체 제한을 적용합니다.

1. 게이트웨이에 로그인합니다.
2. Mail Policies(메일 정책) > Destination Controls(대상 제어)로 이동합니다.
3. Add Destination을 클릭하고 설정을 구성합니다.
 - 대상: 도메인 이름 입력
 - 동시 연결: 10
 - 연결당 최대 메시지 수: 20
 - TLS 지원: 권장
4. Submit(제출)을 클릭합니다.
5. UI(사용자 인터페이스) 오른쪽 상단에서 Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션 변경 사항을 저장합니다.

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.

Zoho Mail에서 Cisco Secure Email로 메일 구성(아웃바운드)

Cisco Secure Email Gateway에서 RELAYLIST 설정

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

1. 게이트웨이에 로그인합니다.
2. Mail Policies(메일 정책) > HAT Overview(HAT 개요)로 이동합니다.



참고: Listener가 Outgoing용인지 확인합니다. OutgoingMail 또는 MailFlow-Ext 등이 가장 일반적으로 사용되는 이름입니다.

1. Add Sender Group...를 클릭합니다.
2. 발신자 그룹을 다음과 같이 설정합니다.
 - 이름: 릴레이 초호
 - 코멘트: <<enter a comment if you wish to notate your sender group>>
 - 정책: RELAYED
 - Submit and Add Senders를 클릭합니다.
 - 보낸 사람: zoho 기반 도메인의 호스트 이름(예: .zoho.com) 참고: 이. 발신자 도메인 이름의 시작 부분에 (점)이 필요합니다.

3. Submit(제출)을 클릭합니다.
4. UI 오른쪽 상단에서 Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션 변경 사항을 저장합니다.

TLS 활성화

1. <<Back to HAT Overview(HAT 개요로 돌아가기)를 클릭합니다.
2. Mail Flow Policy RELAYED를 클릭합니다. Encryption and Authentication(암호화 및 인증) 섹션 아래에 있는 TLS의 경우 다음을 선택합니다. 기본 설정.
3. Submit(제출)을 클릭합니다.
4. UI 오른쪽 상단에서 Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션 변경 사항을 저장합니다.

다음을 확인합니다.

인바운드 및/또는 아웃바운드 메일 트래픽을 테스트합니다.

Cisco Secure Email and Web Manager(SMA라고도 함)에서 메시지 추적의 메일 로그에서 인바운드 및 아웃바운드 트래픽 모두에 대해 테스트된 메일 로그를 확인합니다.

문제 해결

1. Zoho 및 Cisco CES 모두에서 사용되는 IP 주소 및 호스트 이름을 확인합니다.
2. RAT, SMTP 경로가 모두 올바르게 구성되어 있는지 확인합니다.

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.