클라우드 게이트웨이 골드 컨피그레이션 구성

목차

소개

이 문서에서는 Cisco Secure Email Cloud Gateway에 제공되는 Gold Configuration에 대한 심층 분석을 설명합니다. Cisco Secure Email 클라우드 고객을 위한 Gold Configuration은 Cloud Gateway 및 Cisco Secure Email and Web Manager 모두에 대한 모범 사례 및 제로 데이 컨피그레이션입니다. Cisco Secure Email Cloud 구축에서는 클라우드 게이트웨이와 하나 이상의 Email and Web Manager를 모두 사용합니다. 컨피그레이션 및 모범 사례의 일부는 중앙 집중식 관리를 위해 관리자에게 Email and Web Manager에 있는 격리를 사용하도록 지시합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco Secure Email Gateway 또는 Cloud Gateway, UI 및 CLI 관리 모두
- Cisco Secure Email Email Email and Web Manager, UI 레벨 관리
- Cisco Secure Email Cloud 고객은 CLI 액세스를 요청할 수 있습니다. 다음을 참조하십시오. CLI(Command Line Interface) 액세스

사용되는 구성 요소

이 문서의 정보는 Cisco Secure Email Cloud 고객 및 관리자를 위한 Gold 컨피그레이션 및 모범 사례 권장 사항에 나와 있습니다.

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.

관련 제품

이 문서는 다음 항목에도 적용됩니다.

- Cisco Secure Email Gateway 온프레미스 하드웨어 또는 가상 어플라이언스
- Cisco Secure Email and Web Manager 온프레미스 하드웨어 및 가상 어플라이언스

정책 격리

Cisco Secure Email Cloud 고객을 위해 Email and Web Manager에서 격리를 구성하고 유지 관리합니다. 이메일 및 웹 관리자에 로그인하여 격리를 확인하십시오.

- 계정 인수
- 스푸핑 차단(_S)
- 첨부 파일 차단(_O)
- 차단 목록
- DKIM_FAIL
- DMARC_격리
- DMARC_거부
- 위조 이메일
- 부적절한 콘텐츠
- 매크로
- 열기 릴레이
- SDR_데이터

- SPF_하드웨어 실패
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_악성

클라우드 게이트웨이 골드 컨피그레이션

> **경고**: 프로덕션 환경에서 컨피그레이션 변경 사항을 커밋하기 전에 이 문서에 제공된 모범 사례를 기반으로 한 컨피그레이션 변경 사항을 검토하고 이해해야 합니다. 구성을 변경하기 전에 Cisco CX 엔지니어, DSM(Designated Service Manager) 또는 어카운트 팀에 문의하십시오.

기본 설정

메일 정책 > 수신인 테이블(RAT)

Recipient Access Table(수신자 액세스 테이블)은 퍼블릭 리스너에서 수락할 수신자를 정의합니다. 적어도 표에는 주소와 해당 주소를 승인 또는 거부할지 여부가 지정됩니다. 필요에 따라 도메인을 추가하고 관리하려면 RAT를 검토하십시오.

Network(네트워크) > SMTP Routes(SMTP 경로)

SMTP 경로 대상이 Microsoft 365인 경우 "4.7.500 Server 사용 중"으로 Office365 Throttling CES New Instance를 참조하십시오. "나중에 다시 시도하십시오".

보안 서비스

나열된 서비스는 제공된 값을 가진 모든 Cisco Secure Email Cloud 고객에게 구성됩니다.

IronPort 안티스팸(IPAS)

- Always scan 1M(항상 스캔 1M) 및 Never scan 2M(스캔 2M 안 함)을 활성화하고 구성합니다.
- 단일 메시지 검사 시간 제한: 60초

URL 필터링

- URL 분류 및 평판 필터 사용
- (선택 사항) "bypass_urls"라는 URL 허용 목록을 만들고 구성합니다.
- 웹 상호 작용 추적 사용
- 고급 설정: URL 조회 시간 초과: 15초본문 및 첨부 파일에서 스캔되는 최대 URL 수: 400메시지의 URL 텍스트 및 HREF 재작성: 아니요URL 로깅: 사용
- (선택 사항) AsyncOS 14.2 for Cloud Gateway에서는 URL 회귀적 판정 및 URL 교정을 사용할

수 있습니다. 제공되는 릴리스 정보 및 Secure Email Gateway 및 Cloud Gateway의 URL 필터링 구성 참조

그레이메일 탐지

- Always scan 1M(항상 스캔 1M) 및 Never scan 2M(스캔 2M 안 함) 활성화 및 구성
- 단일 메시지 검사 시간 제한: 60초

신종 바이러스 필터

- 적응 규칙 활성화
- 검사할 최대 메시지 크기: 2백만
- 웹 상호 작용 추적 사용

Advanced Malware Protection > 파일 평판 및 분석

- 파일 평판 사용
- 파일 분석 사용 파일 분석에 대한 파일 유형을 검토하려면 전역 설정을 참조하십시오.

메시지 추적

- 거부된 연결 로깅 사용(필요한 경우)

시스템 관리

사용자(시스템 관리 > 사용자)

- **로컬 사용자 계정 및** 암호 설정과 관련된 암호 정책을 검토하고 **설정해야 합니다.**
- 가능한 경우 인증을 위해 LDAP(Lightweight Directory Access Protocol)를 구성하고 활성화합니다(**System Administration > LDAP**).

로그 서브스크립션(System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션))

- 구성되지 않은 경우 다음을 생성하고 활성화합니다. 컨피그레이션 기록 로그URL 평판 클라이언트 로그
- Log Subscriptions Global Settings(로그 서브스크립션 전역 설정)에서 설정을 편집하고 To(대상), From(발신), Reply-To(**회신** 대상), Sender(발신자)**에 헤더를 추가합니다**.

추가 구성(선택 사항)

검토하고 고려할 추가 서비스:

시스템 관리 > LDAP

- LDAP를 구성하는 경우 SSL이 활성화된 LDAP를 권장합니다

URL 방어

- URL 방어를 위한 최신 구성 모범 사례는 Configure URL Filtering for Secure Email Gateway and Cloud Gateway를 참조하십시오.
- Cisco는 또한 URL 방어에 대해 심층적으로 연구합니다. URL Defense Guide를 참조하십시오.

- URL Defense Guide에 포함된 몇 가지 예도 이 문서에 포함되어 있습니다.

SPF

- SPF(Sender Policy Framework) DNS 레코드는 클라우드 게이트웨이 외부에서 생성됩니다. 따라서 Cisco는 모든 고객이 보안 상태에 SPF, DKIM 및 DMARC 모범 사례를 구축할 것을 적극 권장합니다. SPF 유효성 검사에 대한 자세한 내용은 SPF 컨피그레이션 및 모범 사례를 참조하십시오.
- Cisco Secure Email Cloud 고객의 경우 모든 호스트를 더 쉽게 추가할 수 있도록 할당 호스트 이름별로 모든 클라우드 게이트웨이에 대한 매크로가 게시됩니다.
- 현재 DNS TXT(SPF) 레코드(있는 경우) 내에서 ~all 또는 -all보다 먼저 배치합니다.

```
exists:%{i}.spf.<allocation>.iphmx.com
```

> **참고**: SPF 레코드가 **~all 또는** -all로 **끝나야 합니다**. 변경 전후에 도메인의 SPF 레코드를 확인합니다.

- SPF에 대한 자세한 정보 및 툴:
  SPF 레코드 검사기 - 무료 SPF 조회(dmarcian.com)SPF 레코드 구문 테이블 - Everything SPF - dmarcian.com

추가 SPF 예

- SPF의 좋은 예는 클라우드 게이트웨이에서 이메일을 수신하고 다른 메일 서버에서 아웃바운드 이메일을 보내는 경우입니다. "a:" 메커니즘을 사용하여 메일 호스트를 지정할 수 있습니다.

```
v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~all
```

- 클라우드 게이트웨이를 통해서만 아웃바운드 이메일을 전송하는 경우 다음을 사용할 수 있습니다.

```
v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~all
```

- 이 예에서 "ip4:" 또는 "ip6:" 메커니즘은 IP 주소 또는 IP 주소 범위를 지정합니다.

```
v=spf1 exists:%{i}.spf.<allocation>.iphmx.com ip4:192.168.0.1/16 ~all
```

CLI 레벨 변경

- 사전 요구 사항에 설명된 대로 Cisco Secure Email Cloud 고객은 CLI 액세스를 요청할 수 있습니다. CLI(Command Line Interface) 액세스를 참조하십시오.

스푸핑 방지 필터

- 스푸핑 방지를 위한 모범 사례 가이드를 반드시 검토하십시오.
- 이 가이드에서는 이메일 스푸핑 방지를 위한 구성 모범 사례와 구성 모범 사례를 제공합니다

헤더 필터 추가

- CLI만 해당, addHeaders 메시지 필터를 쓰고 활성화하십시오.

```
addHeaders:  if (sendergroup != "RELAYLIST")
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
    insert-header("X-IronPort-MID", "$MID");
    insert-header("X-IronPort-Reputation", "$Reputation");
    insert-header("X-IronPort-Listener", "$RecvListener");
    insert-header("X-IronPort-SenderGroup", "$Group");
    insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

호스트 액세스 테이블(메일 정책 > HAT(Host Access Table))

HAT 개요 > 추가 발신자 그룹

- ESA 사용 설명서: 메시지 처리를 위한 발신자 그룹 생성 BYPASS_SBRS - 평판을 건너뛰는 소스의 경우 더 높은 곳에 배치합니다.MY_TRUSTED_SPOOF_HOSTS - 스푸핑 필터의 일부 TLS_REQUIRED - TLS 강제 연결용

미리 정의된 SUSPECTLIST 발신자 그룹에서

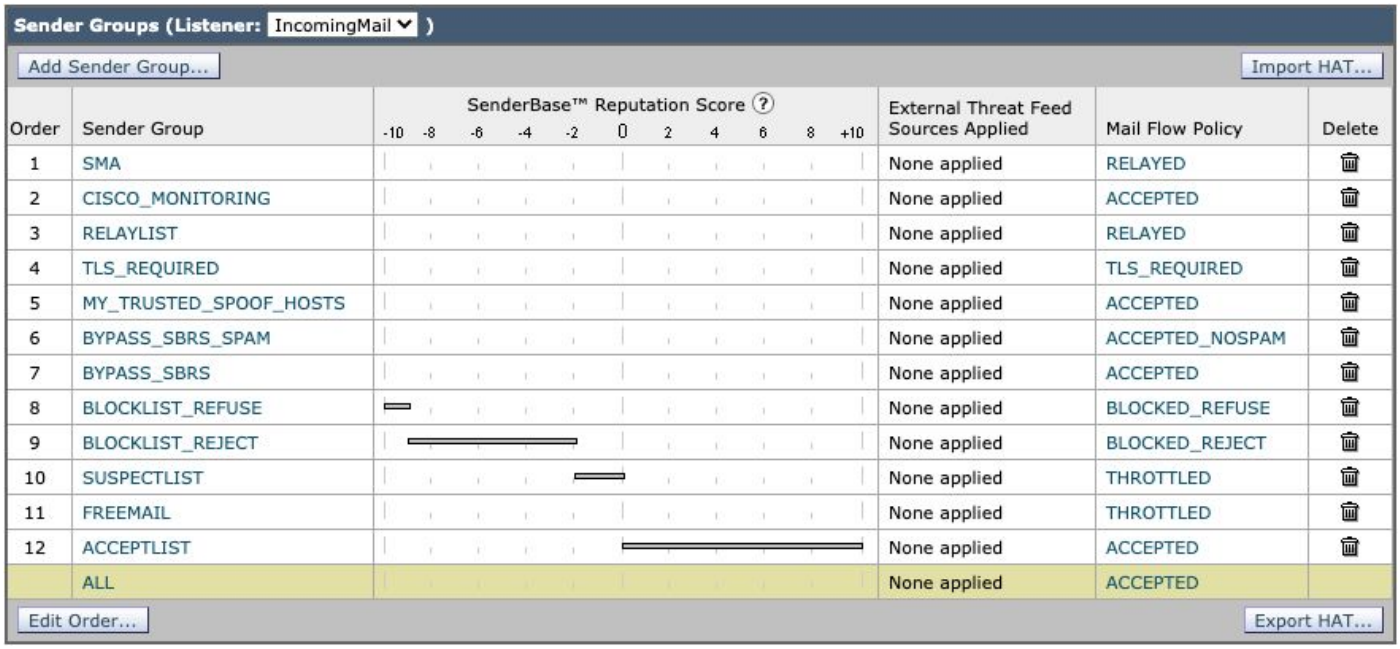
- ESA 사용 설명서: 발송인 확인: 호스트 "SBRS Scores on None"을 활성화합니다.(선택 사항) "연결 호스트 PTR 레코드 조회가 임시 DNS 실패로 인해 실패함"을 활성화합니다.

적극적인 HAT 샘플

- BLOCKLIST_REFUSE [-10.0 ~ -9.0] 정책: 차단_거부
- BLOCKLIST_REJECT [-9.0 ~ -2.0] 정책: 차단_거부
- SUSPECTLIST [-2.0 ~ 0.0 및 SBRS 점수 "없음"] 정책: 조절된
- ACCEPTLIST [0.0 ~ 10.0] 정책: 수락됨

> **참고:** HAT 예에서는 추가로 구성된 MFP(Mail Flow Policy)를 보여줍니다. MFP에 대한 자세한 내용은 배포한 Cisco Secure Email Gateway용 AsyncOS의 해당 버전에 대한 사용 설명서의 "이메일 파이프라인 이해 > 수신/수신"을 참조하십시오.

HAT 예:



메일 플로우 정책(기본 정책 매개변수)

기본 정책 매개변수

보안 설정

- TLS(Transport Layer Security)를 기본 설정으로 설정
- SPF(Sender Policy Framework) 활성화
- DKIM(DomainKeys Identified Mail) 사용
- DMARC(Domain-based Message Authentication, Reporting, and Conformance) 확인 및 집계 피드백 보고서 보내기

> **참고:** DMARC를 구성하려면 추가 튜닝이 필요합니다. DMARC에 대한 자세한 내용은 배포한 Cisco Secure Email Gateway용 AsyncOS의 해당 버전에 대한 사용 설명서의 "이메일 인증 > DMARC 확인"을 참조하십시오.

수신 메일 정책

기본 정책은 다음과 유사하게 구성됩니다.

안티스팸

- 기본 임계값에 임계값이 남아 있는 상태로 활성화됩니다. (점수를 변경하면 오탐이 증가할 수 있습니다.)

안티바이러스

- 메시지 검사: **바이러스만 검사** "X-헤더 포함"에 대한 확인 확인란이 활성화됨
- 검사할 **수 없는 메시지** 및 **바이러스 감염 메시지**의 경우 **Archive Original Message를 No로 설정합니다**

AMP

- **메시지** 오류**에 대한 검사 불가능한 작업**의 경우 **Advanced** 및 Add **Custom Header to Message**, X-TG-MSGERROR, value를 사용합니다. 맞아
- 속도 **제한에 대한 검사 불가능한 작업**의 경우 **Advanced** 및 Add **Custom Header to Message**, X-TG-RATELIMIT, value를 사용합니다. 맞아
- 파일 **분석이 보류 중인 메시지**의 경우 **메시지에 적용된 작업**: "격리"를 사용하십시오.

그레이메일

- 각 판정(Marketing, Social, Bulk)에 대해 검사가 활성화되며 Prepend for **Add Text to Subject**(제목**에 텍스트 추**가 **앞에 추가됨)이** 수행됩니다.
- 대량 **메일에 대한 작업**의 경우 **고급** 및 사용자 **지정 헤더 추가(선택 사항)를** 사용합니다. X-Bulk, 값: 맞아

콘텐츠 필터

- Enabled(활성화됨) 및 URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT이 선택됩니다
- 이러한 콘텐츠 필터는 이 가이드의 뒷부분에서 제공합니다

신종 바이러스 필터

- 기본 위협 레벨은 3입니다. 보안 요구 사항에 맞게 조정하십시오. 메시지의 위협 수준이 이 임계값과 같거나 이를 초과하면 메시지가 Outbreak Quarantine(신종 바이러스 격리)으로 이동합니다. (1=최저 위협, 5=최고 위협)
- 메시지 수정 사용
- "모든 메시지에 대해 사용"으로 설정된 URL 재작성
- 제목 앞에 추가: [가능한 $threat_category 사기]

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	BLOCKLIST	Disabled	Disabled	(use default)	Disabled	BLOCKLIST_QUARANTINE	Disabled	(use default)	
2	ALLOWLIST	Disabled	(use default)	(use default)	Disabled	(use default)	Disabled	(use default)	
3	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SDR	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop ...	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Unsubscribe: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE DKIM_FAILURE SPF_HARDFAIL EXECUTIVE_SPOOF ...	Retention Time: Virus: 1 day Other: 4 hours	Not Available	

정책 이름(표시)

- **차단 목록 메일 정책**
  BLOCKLIST 메일 정책은 Advanced Malware Protection을 제외한 모든 서비스를 비활성화하고 QUARANTINE 작업을 사용하여 콘텐츠 필터에 대한 링크로 구성되어 있습니다.

- **허용 목록 메일 정책**
  ALLOWLIST 메일 정책에는 URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT 또는 선택한 컨피그레이션의 콘텐츠 필터에 대해 Antispam, Graymail Disabled 및 Content Filters가 활성화되어 있습니다.

- **메일 정책 ALLOW_SPOOF**
  ALLOW_SPOOF 메일 정책에는 URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, SDR 또는 선택한 컨피그레이션의 콘텐츠 필터에 대해 활성화된 콘텐츠 필터와 함께 모든 기본 서비스가 활성화되어 있습니다.

발송 메일 정책

기본 정책은 다음과 유사하게 구성됩니다.

안티스팸

- 비활성화됨

안티바이러스

- 메시지 검사: **바이러스만 검사** "X-헤더 포함"의 확인란을 선택 취소합니다.
- (선택 사항) 모든 메시지의 경우: **Advanced**(고급) > **Other Notification(**기타 알림)에서 "Others(기타)"를 활성화하고 관리자/SOC 연락처 이메일 주소를 포함합니다.

지능형 악성코드 차단

- 파일 평판만 활성화
- **속도 제한에 대한 검사 불가 작업**: 고급 **사용** 및 **메시지에 사용자 지정 헤더 추가**: X-TG-RATELIMIT, 값: "참"
- **악성코드 첨부 파일이 있는 메시지**: 고급 **사용** 및 **메시지에 사용자 지정 헤더 추가**: X-TG-OUTBOUND, 값: "악성코드가 탐지됨"

그레이메일

- 비활성화됨

콘텐츠 필터

- Enabled(활성화됨) 및 TG_OUTBOUND_MALICIOUS, Strip_Secret_Header, EXTERNAL_SENDER_REMOVE, ACCOUNT_TAKEOVER 또는 선택한 콘텐츠 필터가 선택됩니다.

신종 바이러스 필터

- 비활성화됨

DLP

- DLP 라이센싱 및 DLP 컨피그레이션에 따라 활성화합니다.

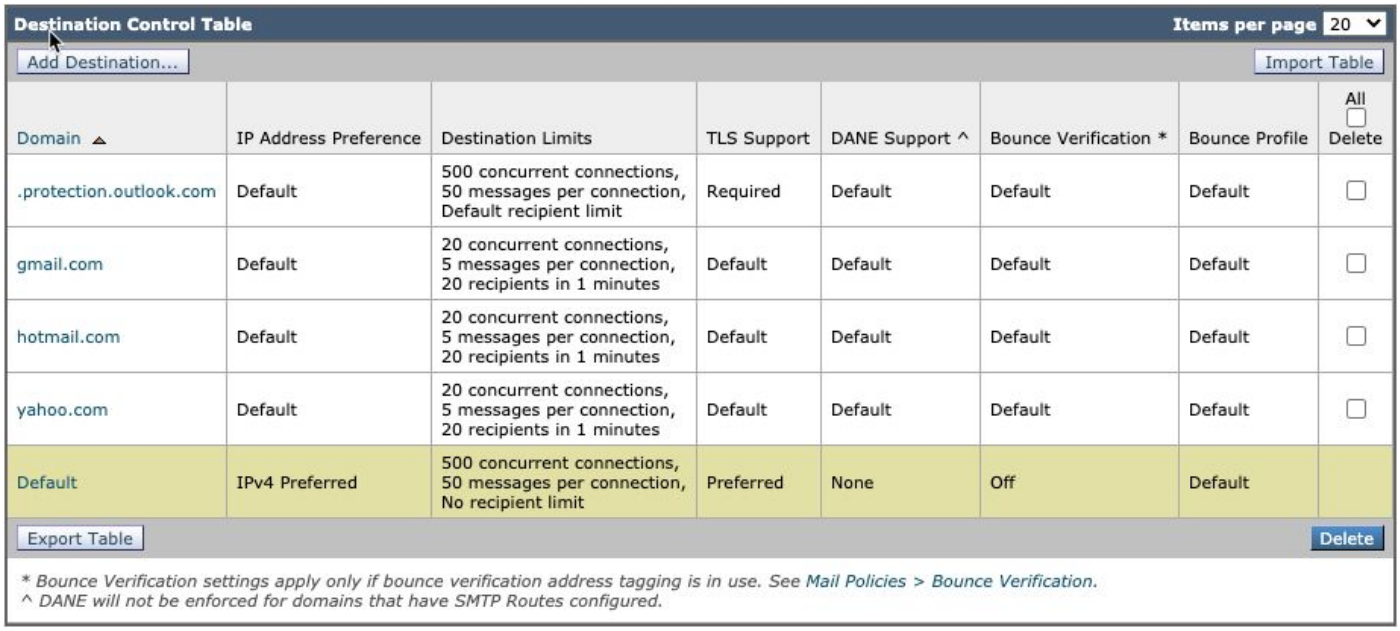
기타 설정

사전 (메일 정책 > 사전)

- 비속어 및 **Sexual_Content 사전 사용 및** 검토
- 모든 경영진 이름으로 위조된 이메일 탐지를 위한 Executive_FED 사전 생성
- 정책, 환경, 보안 제어에 필요한 대로 제한된 키워드 또는 기타 키워드에 대한 추가 사전을 만듭니다

대상 제어(메일 정책 > 대상 제어)

- Default 도메인의 경우 TLS 지원**을 Preferred**로 **구성합니다**
- 웹 메일 도메인의 대상을 추가하고 더 낮은 임계값을 설정할 수 있습니다
- 자세한 내용은 Rate Limit Your Outbound Mail with Destination Control Settings 가이드를 참조하십시오.



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
.protection.outlook.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	☐
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	☐
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	☐
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	☐
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	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.

콘텐츠 필터

> **참고:** 콘텐츠 필터에 대한 자세한 내용은 배포한 Cisco Secure Email Gateway용 AsyncOS의 해당 버전에 대한 사용 설명서의 "콘텐츠 필터"를 참조하십시오.

수신 콘텐츠 필터

URL_QUARANTINE_MALICIOUS

조건: URL Reputation; url-reputation(-10.00, -6.00, "bypass_urls", 1, 1)

작업: 격리: quarantine("URL_MALICIOUS")

URL_REWRITE_SUSPICIOUS

조건: URL Reputation; url-reputation(-5.90, -5.60, "bypass_urls", 0, 1)

작업: URL 평판; url-reputation-proxy-redirect(-5.90, -5.60,"",0)

URL_부적절

조건: URL 범주; url-category (['Adult', '아동 학대 콘텐츠', 'Extreme', 'Hate Speech', '불법 행위', '불법 다운로드', '불법 약물', '음란물', '필터 회피'], 'bypass_urls', 1, 1)

작업: 격리; 중복 격리("INAPPROPRIATE_CONTENT")

DKIM_실패

조건: DKIM 인증; dkim-authentication == hardfail

작업: 격리; 중복 격리("DKIM_FAIL")

SPF_하드웨어 실패

조건: SPF 확인, spf-status == 실패

작업: 격리; 중복 격리("SPF_HARDFAIL")

이그제큐티브_스푸핑

조건: 위조 이메일 탐지; 위조 이메일 탐지("Executive_FED", 90, "")

조건: 기타 헤더; 헤더("X-IronPort-SenderGroup") != "(?i)allowspoof"

*** 적용 규칙 설정: 모든 조건이 일치하는 경우에만**

작업: 헤더 추가/편집; edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1")

작업: 쿼런틴; duplicate-quarantine("FORGED_EMAIL")

도메인_스푸핑

조건: 기타 헤더; header("X-Spoof")

작업: 쿼런틴; duplicate-quarantine("ANTI_SPOOF")

SDR

조건: 도메인 평판; sdr-평판(['지독한'], "")

조건: 도메인 평판, sdr 기간("days", <, 5, "")

*** 적용 규칙 설정: 하나 이상의 조건이 일치하는 경우**

작업: 격리; 중복 격리("SDR_DATA")

TG_RATE_LIMIT

조건: 기타 헤더; 헤더("X-TG-RATELIMIT")

작업: 로그 항목 추가; log-entry("X-TG-RATELIMIT: $filenames")

차단 목록_격리

조건: (None)

작업: 쿼런틴; 쿼런틴("BLOCKLIST")

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_QUARANTINE_MALICIOUS	URL_QUARANTINE_MALICIOUS: if (url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)) { quarantine("URL_MALICIOUS"); }		
2	URL_REWRITE_SUSPICIOUS	URL_REWRITE_SUSPICIOUS: if (url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)) { url-reputation-proxy-redirect(-5.90, -5.60,"",0); }		
3	URL_INAPPROPRIATE	URL_INAPPROPRIATE: if (url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)) { duplicate-quarantine("INAPPROPRIATE_CONTENT"); }		
4	DKIM_FAILURE	DKIM_FAILURE: if (dkim-authentication == "hardfail") { duplicate-quarantine("DKIM_FAIL"); }		
5	SPF_HARDFAIL	SPF_HARDFAIL: if (spf-status == "fail") { duplicate-quarantine("SPF_HARDFAIL"); }		
6	EXECUTIVE_SPOOF	EXECUTIVE_SPOOF: if (forged-email-detection("Executive_FED", 90, "")) AND (header("X-IronPort-SenderGroup") != "(?i)allowspoof") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); duplicate-quarantine("FORGED_EMAIL"); }		
7	DOMAIN_SPOOF	DOMAIN_SPOOF: if (header("X-Spoof")) { duplicate-quarantine("ANTI_SPOOF"); }		
8	SDR	SDR: if (sdr-reputation (['awful'], "")) OR (sdr-age ("days", <, 5, "")) { duplicate-quarantine("SDR_DATA"); }		
9	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-RATELIMIT")) { log-entry("X-TG-RATELIMIT: $filenames"); }		
10	BLOCKLIST_QUARANTINE	BLOCKLIST_QUARANTINE: if (true) { quarantine("BLOCKLIST"); }		
11	SAMPLE_ATTACHMENT_BLOCK	SAMPLE_ATTACHMENT_BLOCK: if (attachment-filetype == "Executable") OR (attachment-filename == "\\.(386|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|url|vb|vbe|vbs|vss|vst|vsw|ws|wsc|wsf|wsh)$") { duplicate-quarantine("BLOCK_ATTACHMENTS"); drop(); }		
12	SAMPLE_SPF_SOFTFAIL	SAMPLE_SPF_SOFTFAIL: if (spf-status == "softfail") { duplicate-quarantine("SPF_SOFTFAIL"); }		
13	SAMPLE_MACRO	SAMPLE_MACRO: if (macro-detection-rule (['Adobe Portable Document Format', 'Microsoft Office Files', 'OLE File types'])) { quarantine("MACRO"); }		
14	SAMPLE_ATTACHMENT_PROTECTED	SAMPLE_ATTACHMENT_PROTECTED: if (attachment-protected) { log-entry("Encrypted: $MID"); }		
15	SAMPLE_LANGUAGE_UNKNOWN	SAMPLE_LANGUAGE_UNKNOWN: if (message-language == "unknown") { edit-header-text("Subject", "(.*)", "[SUSPICIOUS]\\1"); }		
16	SAMPLE_INAPPROPRIATE_CONTENT	SAMPLE_INAPPROPRIATE_CONTENT: if (dictionary-match("Profanity", 1)) OR (dictionary-match("Sexual_Content", 1)) { quarantine("INAPPROPRIATE_CONTENT"); }		
17	SAMPLE_REPLY-TO_MISMATCH	SAMPLE_REPLY-TO_MISMATCH: if (header("reply-to")) AND (header("reply-to") != "^$envelopefrom$") { add-heading("SAMPLE_REPLY-TO_WARN"); log-entry("REPLY-TO MISMATCH"); }		
18	SAMPLE_EXTERNAL_SENDER	SAMPLE_EXTERNAL_SENDER: if (subject != "[EXTERNAL]") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); }		
19	SAMPLE_COUNTRY_FILTER	SAMPLE_COUNTRY_FILTER: if (geolocation-rule (['Canada'])) { log-entry("From Canada"); }		

Edit Filter Order...

발송 컨텐트 필터

TG_OUTBOUND_MALICIOUS

조건: 기타 헤더; 헤더("X-TG-OUTBOUND") == 악성코드

작업: 격리; 격리("TG_OUTBOUND_MALWARE")

Strip_Secret_Header

조건: 기타 헤더; 헤더("PLACEHOLDER") == PLACEHOLDER

작업: Strip 헤더; strip-header("X-IronPort-Tenant")

외부_발신자_제거

조건: (None)

작업: 헤더 추가/편집; 헤더 텍스트 편집("제목", "\\[EXTERNAL\\]\\s?", "")

계정 인수

조건: 기타 헤더; 헤더("X-AMP-Result") ==(?i)악성

조건: URL 평판; url-평판(-10.00, -6.00 , "", 1, 1)

*적용 **규칙 설정: 하나 이상의 조건이 일치하는 경우**

작업: 알림;알림("<Insert admin or distro email address>", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING")

작업: duplicate-quarantine("ACCOUNT_TAKEOVER")

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	Stop_O365_OpenRelay	Stop_O365_OpenRelay: if (header("X-IronPort-Tenant") != "placeholder") { duplicate-quarantine("OPEN_RELAY"); }		
2	TG_OUTBOUND_MALICIOUS	TG_OUTBOUND_MALICIOUS: if (header("X-TG-OUTBOUND") == "MALWARE") { quarantine("TG_OUTBOUND_MALWARE"); }		
3	Strip_Secret_Header	Strip_Secret_Header: if (header("PLACEHOLDER") == "PLACEHOLDER") { strip-header("X-IronPort-Tenant"); }		
4	EXTERNAL_SENDER_REMOVE	EXTERNAL_SENDER_REMOVE: if (true) { edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", ""); }		
5	ACCOUNT_TAKEOVER	ACCOUNT_TAKEOVER: if (header("X-AMP-Result") == "(?i)malicious") OR (url-reputation(-10.00, -6.00 , "", 1, 1)) { notify ("myit@mycompany.com", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING"); duplicate-quarantine("ACCOUNT_TAKEOVER"); }		
6	ENCRYPT_OUT	ENCRYPT_OUT: if (subject == "(?i)*encrypt*") { edit-header-text("Subject", "(?i)*encrypt*\\s?", ""); encrypt-deferred ("CRES_HIGH", "$Subject", 0); }		
7	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-OUTBOUND-RATELIMIT")) { tag-message ("NOOP"); }		

Edit Filter Order...

Cisco Secure Email Cloud 고객의 경우 Gold 컨피그레이션 및 모범 사례 권장 사항에 콘텐츠 필터 예가 포함되어 있습니다. 또한, 컨피그레이션에서 유용할 수 있는 관련 조건 및 작업에 대한 자세한 내용은 "SAMPLE_" 필터를 검토하십시오.

Cisco Live

Cisco Live는 전 세계적으로 많은 세션을 호스팅하며, Cisco Secure Email 모범 사례를 다루는 대면 세션 및 기술 개요를 제공합니다. 이전 세션 및 접속 권한을 보려면 Cisco Live를 방문하십시오 (CCO 로그인 필요).

- Cisco Email Security: 모범 사례 및 미세 조정 - BRKSEC-2131
- DMARCate Your Email Perimeter - BRKSEC-2131
- 이메일 수정! - Cisco Email Security 고급 문제 해결 - BRKSEC-3265
- Cisco Email Security용 API 통합 - DEVNET-2326
- Cisco의 클라우드 이메일 보안으로 SaaS 사서함 서비스 보안 - BRKSEC-1025
- 이메일 보안: 모범 사례 및 미세 조정 - TECSEC-2345
- 250 OK 아님 - Cisco Email Security로 방어하기 - TECSEC-2345
- Cisco Domain Protection 및 Cisco Advanced Phishing Protection: Email Security의 다음 계층 활용! - BRKSEC-1243
- SPF는 "스푸핑"의 약어가 아닙니다! Email Security의 다음 계층을 최대한 활용하십시오! - DGTL-BRKSEC-2327

추가 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

관련 정보

- Cisco Secure Email Security 규정 준수
- 제안 설명: 보안 이메일
- Cisco Universal Cloud 용어
- Cisco 지원 및 다운로드
- [외부] OpenSPF: SPF 기본 정보 및 고급 정보

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.