

사용자가 Gmail 이메일에 파일을 첨부하지 못하도록 방지

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[절차](#)

소개

이 문서에서는 Gmail 전자 메일에 파일을 첨부하지 못하게 하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 다음 사항을 권장합니다.

- HTTPS 프록시가 활성화됨
- 데이터 보안 필터 사용

사용되는 구성 요소

이 문서의 정보는 Cisco WSA(Web Security Appliance), AsyncOS 버전 7.1.x 이상을 기반으로 합니다.

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

절차

Gmail은 HTTP 및 HTTPS를 모두 지원합니다.

이는 Settings(설정) > **General(일반)** > **Browser Connection in Gmail**(Gmail의 사용자 인터페이스에서 사용자에게 따라 제어됩니다).

Gmail이 HTTPS를 사용하도록 구성된 경우 Gmail에서 업로드를 제어하려면 WSA에서 암호 해독 정책을 활용해야 합니다.

먼저 설정을 간소화하려면 Gmail에서 HTTP 연결을 테스트해야 합니다. 예를 들어, 이러한 단계는 사용자가 PDF 파일을 업로드하지 못하도록 차단하는 방법을 보여줍니다.

1. Gmail 어카운트에 로그인하고 Settings(설정) > General(일반) > Browser Connection(브라우저 연결)으로 이동합니다.
2. 이 옵션을 항상 https를 사용하지 않도록 설정합니다.
3. 저장한 후 로그아웃하고 다시 로그인합니다.이제 주소 표시줄에 http://이 표시됩니다.
4. Web Security Manager > Data Security를 선택합니다.
5. 해당 데이터 보안 정책에 대해 Content(콘텐츠)를 클릭합니다.
6. PDF를 차단하려면 [파일 형식 차단] 아래에서 문서 유형을 클릭합니다.
7. Portable Document Format (PDF) 확인란을 클릭합니다.
8. 완료되면 변경 내용을 제출하고 커밋합니다.

문제를 해결하려면 데이터 보안 로그를 활성화합니다.System Administration(시스템 관리) > Log Subscription(로그 서브스크립션)에서.

로그는 다음과 같아야 합니다.

액세스 로그 수

```
1268180609.847 1206 10.7.4.227 TCP_DENIED/403 2088 POST
http://mail.google.com/mail/?ui=2&ik=f2587fbf50&view=up&
- NONE/- - BLOCK_ADMIN_IDS-DefaultGroup-test.id-DefaultGroup-NONE-NONE <IW_mail,0.7,0,-,-,-,-,-,
,-,-,-,-,-,1,-,IW_mail,-> -
```

데이터 보안 로그 수

```
Wed Mar 10 11:23:37 2010 Warning: 119 10.7.4.227 - -
<<WSA_6.0.2_GA_Release_Notes.pdf,application/pdf,403283>>
BLOCK_ADMIN_IDS-DefaultGroup-test.id-DefaultGroup-NONE-NONE 0.7 mail.google.com IW_mail
두 로그 모두에서 BLOCK_ADMIN_IDS를 확인합니다.데이터 보안 로그는 업로드된 파일이
application/pdf임을 보여줍니다.
```

참고:Gmail 사용자 인터페이스에 업로드가 실패했음을 나타내는 오류가 표시됩니다.

다음으로, Settings(설정) > General(일반) > Browser Connection(브라우저 연결) 아래에서 HTTPS를 사용하도록 Gmail을 설정하고 이 값을 Always use https(항상 https 사용)로 설정합니다 .변경 내용을 저장하고 로그오프한 후 다시 로그인합니다.

다음 컨피그레이션 단계를 사용하여 HTTPS 액세스에 대한 업로드를 제어할 수 있습니다.

1. Web Security Manager(웹 보안 관리자) > Decryption Policies(암호 해독 정책)를 선택하고 각 암호 해독 정책에 대한 URL Categories(URL 카테고리)를 클릭합니다.
2. URL 카테고리 웹 기반 이메일을 Decrypt로 설정합니다.
3. 지금 Gmail에 PDF 파일을 업로드하려고 하면 이러한 로그가 나타납니다.

액세스 로그 수

```
1268181243.208 628 10.7.4.227 TCP_CLIENT_REFRESH_MISS_SSL/200 64 CONNECT
tunnel://mail.google.com:443/ - DIRECT/mail.google.com
- DECRYPT_WEBCAT-DefaultGroup-test.id-NONE-NONE-DefaultRouting <IW_mail,0.7,-,-,-,-,-,-,
,-,-,-,-,-,IW_mail,-> - 272
```

```
1268181246.378 2976 10.7.4.227 TCP_DENIED_SSL/403 2082 POST
```

<https://mail.google.com:443/mail/?ui=2&ik=f2587fbf50&view=up&>

```
- NONE/- - BLOCK_ADMIN_IDS-DefaultGroup-test.id-DefaultGroup-NONE-NONE <IW_mail,0.7,0,-,-,-  
,-,,-,-,-,-,-,1,-,IW_mail,-> - 273
```

데이터 보안 로그 수

Wed Mar 10 11:34:14 2010 Warning: 273 10.7.4.227 - -

<<WSA_6.0.2_GA_Release_Notes.pdf,application/pdf,403283>>

BLOCK_ADMIN_IDS-DefaultGroup-test.id-DefaultGroup-NONE-NONE 0.7 mail.google.com IW_mail

이 HTTPS 트랜잭션에 대한 BLOCK_ADMIN_IDS가 표시됩니다.

참고:Gmail 사용자 인터페이스에 업로드가 실패했음을 나타내는 오류가 표시됩니다.

추가 참고 사항:

- 이 단계는 특정 파일 유형이 Gmail에 업로드되는 것을 차단하는 방법을 보여줍니다.
- 대부분의 웹 사이트에서도 유사한 단계를 수행할 수 있습니다.
- WSA의 정확한 단계는 현재 구성된 방식에 따라 다를 수 있습니다.