CRES를 사용하는 Cisco Email Security Appliance에서 생성된 보안 봉투의 만료 시간을 미리 설정할 수 있습니까?

목차

소개
RES를 사용하는 Cisco Email Security Appliance에서 생성된 보안 봉투의 만료 시간을 미리 설정할 수 있습니까?
메시지에 암호화 헤더 삽입
절차
다음 작업
암호화 헤더
암호화 헤더 예
오프라인 열기 봉투 키 캐싱 활성화
Javascript가 없는 봉투 활성화
메시지 만료 활성화
암호 해독 애플릿 비활성화

소개

이 문서에서는 Cisco RES(Registered Envelope Service)를 구현하는 Cisco ESA(Email Security Appliance)에서 생성되는 보안 봉투의 만료 시간을 설정하는 방법에 대해 설명합니다.

RES를 사용하는 Cisco Email Security Appliance에서 생성된 보안 봉투의 만료 시간을 미리 설정할 수 있습니까?

예, 암호화를 위해 플래그가 지정될 발신 메시지에 SMTP 헤더를 추가할 수 있습니다. 여기에는 'X-PostX-ExpirationDate' 헤더가 포함됩니다.

다음은 Email Security Appliance 사용 설명서의 일부입니다.

메시지에 암호화 헤더 삽입

AsyncOS에서는 콘텐츠 필터 또는 메시지 필터를 사용하여 메시지에 SMTP 헤더를 삽입하여 메시지에 암호화 설정을 추가할 수 있습니다.암호화 헤더는 연결된 암호화 프로파일에 정의된 암호화 설정을 재정의할 수 있으며 지정된 암호화 기능을 메시지에 적용할 수 있습니다.

절차

1단계 Mail Policies(메일 정책) > Outgoing Content Filters(발신 콘텐츠 필터) 또는 Incoming Content Filter

신 콘텐츠 필터)로 이동합니다.

2단계 Filters(필터) 섹션에서 Add Filter(필터 추가)를 클릭합니다.

3단계 Actions(작업) 섹션에서 Add Action(작업 추가)을 클릭하고 Add/Edit Headerer를 선택하여 암호화 헤
메시지에 삽입하여 추가 암호화 설정을 지정합니다.
예를 들어, Registered Envelope를 보낸 후 24시간 후에 만료되도록 하려면 X-PostX-ExpirationDate
더 이름으로 입력하고 헤더 값으로 +24:00:00을 입력합니다.

다음 작업

관련 항목

- 암호화 콘텐츠 필터 만들기에 대한 자세한 내용은 콘텐츠 필터를 사용하여 메시지 암호화 및 즉시 전달을 참조하십시오.
- 메시지 필터를 사용하여 헤더를 삽입하는 방법에 대한 자세한 내용은 메시지 필터를 사용하여 이메일 정책 적용을 참조하십시오.

암호화 헤더

다음 표에는 메시지에 추가할 수 있는 암호화 헤더가 표시됩니다.

표 3. 이메일 암호화 헤더

MIME 헤더	설명	가치
X-PostX-Reply-Enabled	메시지에 대해 안전한 회신을 활성화할지 여부를 나타내며 메시지 표시줄에 회신 단추를 표시합니다.이 헤더는 메시지에 암호화 설정을 추가합니다.	회신 단추를 표시할지 여 를 나타내는 부울입니다 추를 표시하려면 true로 합니다.기본값은 false입 .
X-PostX-Reply-All-Enabled	메시지에 대해 보안 "reply all"을 사용하도록 설정할지 여부를 나타내며 메시지 표시줄에 Reply All(모두 회신) 단추를 표시합니다.이 헤더는 기본 프로파일 설정을 재정의합니다.	Reply All(모두 회신) 단 표시할지 여부를 나타내 부울입니다.단추를 표시 면 true로 설정합니다.기 은 false입니다.
X-PostX-Forward-Enabled	보안 메시지 전달을 활성화할지 여부를 나타내며 메시지 표시줄에 전달 단추를 표시합니다.이 헤더는 기본 프로파일 설정을 재정의합니다.	전달 단추를 표시할지 여 를 나타내는 부울입니다 추를 표시하려면 true로 합니다.기본값은 false입 .
X-PostX-Send-Return-Receipt	읽음 확인 기능을 사용할지 여부를 나타냅니다.수신자가 Secure Envelope(보안 봉투)를 열면 발신자가 영수증을 받습니다.이 헤더는 기본 프로파일 설정을 재정의합니다.	읽음 확인 메일을 보낼지 부를 나타내는 부울입니 .단추를 표시하려면 true 설정합니다.기본값은 fa 니다.
X-PostX-ExpirationDate	보내기 전에 등록된 봉투의 만료 날짜를 정의합니다.키 서버는 만료일 이후에 등록된 봉투에 대한 액세스를 제한합니다.등록된 봉투에 메시지가 만료되었음을 나타내는 메시지가 표시됩니다.이 헤더는 메시지에 암호화 설정을 추가합니다.	상대 날짜 또는 시간을 하는 문자열 값입니다.상 적인 시간, 분, 초의 경우 +HH:MM:SS 형식, 상대 일의 경우 +D 형식을 사 니다.기본적으로 만료 날

	Cisco Registered Envelope Service를 사용하는 경우 http://res.cisco.com의 웹 사이트에 로그인하여 메시지 관리 기능을 사용하여 메시지를 보낸 후 메시지의 만료일을 설정, 조정 또는 제거할 수 있습니다.	는 없습니다.
X-PostX-ReadNotificationDate	보내기 전에 등록된 봉투의 "읽기 기준" 날짜를 정의합니다.이 날짜까지 등록된 봉투를 읽지 않은 경우 로컬 키 서버에서 알림을 생성합니다.이 헤더에 등록된 봉투는 Cisco Registered Envelope Service에서 작동하지 않으며 로컬 키 서버에서만 작동합니다.이 헤더는 메시지에 암호화 설정을 추가합니다.	상대 날짜 또는 시간을 하는 문자열 값입니다.상적인 시간, 분, 초의 경우 +HH:MM:SS 형식, 상대일의 경우 +D 형식을 사니다.기본적으로 만료 는 없습니다.
X-PostX-Suppress-Applet-For-Open	암호 해독 애플릿을 비활성화할지 여부를 나타냅니다.암호 해독 애플릿을 사용하면 브라우저 환경에서 메시지 첨부 파일을 열 수 있습니다.애플릿을 비활성화하면 메시지 첨부 파일이 키 서버에서 해독됩니다.이 옵션을 비활성화하면 메시지를 여는 데 시간이 오래 걸릴 수 있지만 브라우저 환경에 종속되지 않습니다.이 헤더는 기본 프로파일 설정을 재정의합니다.	해독 애플릿을 비활성화여부를 나타내는 부울입.애플릿을 비활성화하려true로 설정합니다.기본false입니다.
X-PostX-Use-Script	JavaScript 제외 봉투를 보낼지 여부를 나타냅니다.JavaScript가 없는 봉투는 수신자의 컴퓨터에서 로컬로 봉투를 여는 데 사용되는 JavaScript가 포함되지 않은 등록된 봉투입니다.수신자는 Open Online 메서드 또는 Open by Forwarding 메서드를 사용하여 메시지를 확인해야 합니다.수신인 도메인의 게이트웨이가 JavaScript를 제거하고 암호화된 메시지를 비활성화하는 경우 이 헤더를 사용합니다.이 헤더는 메시지에 암호화 설정을 추가합니다.	JavaScript 애플릿을 포야 하는지 여부를 나타내부울입니다.JavaScript 봉투를 보내려면 false로정합니다.기본값은 true다.
X-PostX-Remember-Envelope-Key-Checkbox	봉투(Envelope) 오프라인 열기 시 봉투 전용 키 캐싱을 허용할지 여부를 나타냅니다.봉투 키 캐싱을 사용하면 수신자가 올바른 암호를 입력하고 "이 봉투의 암호 기억" 확인란을 선택하면 특정 봉투에 대한 암호 해독 키가 수신자의 컴퓨터에 캐시됩니다.그런 다음 수신자는 컴퓨터에서 봉투를 다시 열기 위해 암호를 다시 입력할 필요가 없습니다.이 헤더는 메시지에 암호화 설정을 추가합니다.	봉투 키 캐싱을 활성화"Remember the passwfor this envelope" 확인표시할지 여부를 나타내부울입니다.기본값은 fa니다.

암호화 헤더 예

이 섹션에서는 암호화 헤더의 예를 제공합니다.

오프라인 열기 봉투 키 캐싱 활성화

봉투 키 캐싱이 활성화된 등록된 봉투를 보내려면 메시지에 다음 헤더를 삽입합니다.

```
X-PostX-Remember-Envelope-Key-:
```

"Remember the password for this envelope"(이 봉투의 비밀번호 저장) 확인란이 등록된 봉투에 표시됩니다.

Javascript가 없는 봉투 활성화

JavaScript가 없는 등록된 봉투를 보내려면 메시지에 다음 헤더를 삽입합니다.

```
X-PostX-Use-Script:
```

수신자가 securedoc.html 첨부 파일을 열면 Registered Envelope(등록된 봉투)가 Open Online(온라인 열기) 링크와 함께 표시되고 Open(열기) 버튼이 비활성화됩니다.

메시지 만료 활성화

메시지를 보낸 후 24시간 후에 만료되도록 메시지를 구성하려면 메시지에 다음 헤더를 삽입합니다.

```
X-PostX-:+24:00:00
```

수신자는 사용자가 메시지를 보낸 후 24시간 동안 암호화된 메시지의 내용을 열고 볼 수 있습니다.그런 다음 Registered Envelope에 봉투가 만료되었음을 나타내는 메시지가 표시됩니다.

암호 해독 애플릿 비활성화

암호 해독 애플릿을 비활성화하고 키 서버에서 메시지 첨부 파일을 해독하려면 다음 헤더를 메시지에 삽입합니다.

```
X-PostX-Suppress-Applet-For-Open:
```

> **참고:**해독 애플릿을 비활성화하면 메시지를 여는 데 시간이 더 걸릴 수 있지만 브라우저 환경에 종속되지 않습니다.