ESA 이메일 암호화 컨피그레이션 예

목차

소개

이 문서에서는 ESA(Email Security Appliance)에서 이메일 암호화를 설정하는 방법에 대해 설명합니다.

사전 요구 사항

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 모델:모든 C-Series 및 X-Series
- 봉투 암호화(PostX) 기능 설치됨

구성

ESA에서 이메일 암호화 사용

GUI에서 다음 단계를 완료합니다.

1. Security Services(보안 서비스)에서 **Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화) > Enable Email Encryption(이메일 암호화 활성화)**을 선택하고 **Edit Settings(설정 편집)**를 클릭합니다.

2. 새 암호화 프로파일을 생성하려면 Add Encryption Profile을 클릭합니다.

3. Key **Service Type(키 서비스 유형)**에 대해 Cisco Registered Envelope Service 또는 Cisco IronPort Encryption Appliance(암호화 어플라이언스를 구매한 경우)를 선택합니다.

4. Submit **and Commit Changes를 클릭합니다**.

5. Encryption Profile(암호화 프로파일)이 생성되면 Cisco의 CRES(Registered Envelope Service) 서버에 이를 프로비저닝할 수 있는 옵션이 제공됩니다.새 프로필 옆에 프로비저닝 버튼이 표시됩니다.Provision(프로비저닝)을 **클릭합니다**.

발송 컨텐트 필터 만들기

암호화 프로파일을 구현하기 위한 발신 콘텐츠 필터를 생성하려면 GUI에서 다음 단계를 완료합니다. 다음 예에서는 필터가 제목 헤더에 "Secure:" 문자열이 있는 발신 메시지에 대해 암호화를 트리거합니다.

1. Mail Policies(메일 정책)에서 Outgoing Content Filters(발신 콘텐츠 필터)를 선택하고 Add Filter(필터 **추가)를** 클릭합니다.

2. subject == "Secure:" 및 Encrypt and Deliver Now(Final Action)의 작업으로 Subject Header 조건이 있는 새 필터를 추가합니다. Submit(제출**)을 클릭합니다**.

3. Mail Policies(메일 정책)에서 Outgoing Mail Policies(발신 메일 정책)를 선택하고 기본 메일 정책 또는 적절한 메일 정책에서 이 새 필터를 활성화합니다.

4. 변경 사항을 커밋합니다.

다음을 확인합니다.

이 섹션에서는 암호화가 작동하는지 확인하는 방법에 대해 설명합니다.

1. 확인하려면 **보안**을 사용하여 새 메일을 **생성합니다.**제목에 있는 이메일을 웹 계정(Hotmail, Yahoo, Gmail)으로 보내 암호화되었는지 확인합니다.

2. Outgoing Content Filter(발신 콘텐츠 필터)를 통해 메시지가 암호화되는지 확인하려면 다음 섹션에 설명된 대로 메일 로그를 확인합니다.

Mail_logs에서 암호화 필터 처리 확인

이러한 mail_log 항목은 Encrypt_Message라는 암호화 필터와 일치하는 메시지를 보여줍니다.

```
Wed Oct 22 17:06:46 2008 Info: MID 116 was generated based on MID 115 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:07:22 2008 Info: MID 118 was generated based on MID 117 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:31:21 2008 Info: MID 120 was generated based on MID 119 by encrypt
filter ''Encrypt_Message
```

이 섹션에 표시된 로그에서 정보를 수집하기 위해 grep 또**는** findevent 명령을 사용하는 방법에 대한 지침은 ESA Message Disposition Decision을 참조하십시오.

문제 해결

암호화 필터가 트리거되지 않으면 테스트 메시지가 사용하는 메일 정책에 대한 메일 로그를 확인합니다.필터가 이 메일 정책에서 활성화되었는지, 그리고 Skip Remaining Content Filters(**나머지 콘텐츠 필터 건너뛰기**) 작업을 사용하여 이 정책에 활성화된 이전 필터가 없는지 확인합니다.

메시지 추적의 메시지가 콘텐츠 필터를 통한 암호화를 트리거하기 위해 올바른 문자열 또는 지정된 제목 태깅을 사용하는지 확인합니다.