ESA에서 DKIM 서명 구성

목차

소개

이 문서에서는 ESA(Email Security Appliance)에서 DKIM(DomainKeys Identified Mail) 서명을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ESA(이메일 보안 어플라이언스) 액세스
- TXT 레코드를 추가/제거하기 위한 DNS 수정 액세스

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

DKIM 서명이 해제되었는지 확인합니다.

모든 메일 플로우 정책에서 DKIM 서명을 해제해야 합니다. 이렇게 하면 메일 흐름에 영향을 주지 않고 DKIM 서명을 구성할 수 있습니다.

1. Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책)로 이동합니다.
2. 각 메일 플로우 정책으로 이동하고 Domain Key/DKIM Signing(도메인 키/DKIM 서명)이 Off(끄기)로 설정되었는지 확인합니다.

DKIM 서명 키 만들기

ESA에서 새 DKIM 서명 키를 만들어야 합니다.

1. Mail Policies(메일 정책) > Signing Keys(서명 키)로 이동하고 Add Key...(키 추가...)를 선택합니다.
2. DKIM 키의 이름을 지정하고 새 개인 키를 생성하거나 현재 키에 붙여넣습니다.

   참고: 대부분의 경우 2048비트 개인 키 크기를 선택하는 것이 좋습니다.

3. 변경 사항을 커밋합니다.

새 DKIM 서명 프로파일 생성 및 DNS 레코드를 DNS에 게시

그런 다음 새 DKIM 서명 프로필을 생성하고 해당 DKIM 서명 프로필에서 DKIM DNS 레코드를 생성한 다음 해당 레코드를 DNS에 게시해야 합니다.

1. Mail Policies(메일 정책) > Signing Profiles(서명 프로필)로 이동하고 Add Profile(프로필 추가)을 클릭합니다.
   1. 프로파일 이름 필드에 프로파일을 설명하는 이름을 지정합니다.
   2. Domain Name(도메인 이름) 필드에 도메인을 입력합니다.
   3. Selector 필드에 새 선택기 문자열을 입력합니다.

      참고: 선택기는 지정된 도메인에 대해 여러 DKIM DNS 레코드를 허용하는 데 사용되는 임의의 문자열입니다.

   4. Signing Key(서명 키) 필드의 이전 섹션에서 생성한 DKIM 서명 키를 선택합니다.
   5. Submit(제출)을 클릭합니다.
2. 여기에서 방금 생성한 서명 프로파일에 대한 DNS Text Record 열에서 Generate를 클릭하고 생성된 DNS 레코드를 복사합니다. 다음과 비슷해야 합니다.

```
selector2._domainkey.domainsite IN TXT "v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMa
```

3. 변경 사항을 커밋합니다.
4. 2단계의 DKIM DNS TXT 레코드를 DNS에 제출합니다.
5. DKIM DNS TXT 레코드가 완전히 전파될 때까지 기다립니다.
6. Mail Policies(메일 정책) > Signing Profiles(서명 프로필)로 이동합니다.
7. Test Profile(테스트 프로파일) 열에서 새 DKIM 서명 프로파일에 대해 Test(테스트)를 클릭합니다. 테스트가 성공하면 이 가이드를 계속 진행합니다. 그렇지 않은 경우 DKIM DNS TXT 레코드가 완전히 전파되었는지 확인합니다.

DKIM 서명 설정

이제 ESA가 DKIM 서명 메시지로 구성되었으므로 DKIM 서명을 켤 수 있습니다.

1. Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책)로 이동합니다.
2. Connection Behavior of Relay가 있는 각 메일 플로우 정책으로 이동하여 Domain Key/DKIM Signing(도메인 키/DKIM 서명)을 On(켜기)으로 설정합니다.

   참고: 기본적으로 Connection Behavior가 Relay인 메일 플로우 정책은 Relayed라는 메일 플로우 정책뿐입니다. DKIM 서명 메시지만 아웃바운드인지 확인해야 합니다.

3. 변경 사항을 커밋합니다.

DKIM 통과 확인을 위해 메일 흐름 테스트

이때 DKIM이 구성됩니다. 그러나 DKIM 서명을 테스트하여 아웃바운드 메시지에 예상대로 서명하고 있으며 DKIM 확인을 통과했는지 확인해야 합니다.

1. ESA를 통해 메시지를 전송하고 ESA에서 서명한 DKIM과 다른 호스트에서 확인한 DKIM을 수신하는지 확인합니다.
2. 메시지가 다른 쪽 끝에서 수신되면 메시지의 헤더에 Authentication-Results 헤더가 있는지 확인합니다. 헤더의 DKIM 섹션을 찾아 DKIM 확인을 통과했는지 확인합니다. 헤더는 다음 예와 유사해야 합니다.
   <#root>

   ```
   Authentication-Results: mx1.domainsite; spf=SoftFail smtp.mailfrom=user1@domainsite;
   dkim=pass
    header.i=none; dmarc=fail (p=none dis=none) d=domainsite
   ```

3. "DKIM-Signature" 헤더를 찾고 올바른 선택기와 도메인이 사용되었는지 확인합니다.

   <#root>

   ```
   DKIM-Signature: a=rsa-sha256;
   d=domainsite
   ;
   s=selector2
   ;
      c=simple; q=dns/txt; i=@domainsite;
      t=1117574938; x=1118006938;
      h=from:to:subject:date;
      bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
      b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
               VoG4ZHRNiYzR
   ```

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 컨피그레이션의 문제를 해결할 수 있는 구체적인 방법이 없습니다.

관련 정보

- Cisco 기술 지원 및 다운로드

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.