ESA - 기존 DKIM 키를 다운타임 없이 교체

목차

소개

이 문서에서는 DNS의 ESA 및 DKIM 공개 키에 있는 기존 DKIM 서명 키를 다운타임 없이 교체하는 방법에 대해 설명합니다.

요구 사항

1. ESA(Email Security Appliance)에 액세스합니다.
2. DNS에 액세스하여 TXT 레코드를 추가/제거합니다.
3. ESA는 이미 DKIM 프로필을 사용하여 메시지에 서명해야 합니다.

새 DKIM 서명 키 만들기

먼저 ESA에서 새 DKIM 서명 키를 생성해야 합니다.

1. Mail Policies(메일 정책) > Signing Keys(서명 키)로 이동하여 "Add Key..."를 선택합니다.
2. DKIM 키의 이름을 지정하고 새 개인 키를 생성하거나 기존 키에 붙여넣습니다. **참고:***대부분의 경우 2048비트 개인 키 크기를 선택하는 것이 좋습니다.*
3. 변경 사항을 커밋합니다.
   참고:이 변경은 DKIM 서명 또는 메일 흐름에 영향을 주지 않습니다.DKIM 서명 키를 추가하려고 하는데 아직 DKIM 서명 프로필에 적용하지 않습니다.

새 DKIM 서명 프로필을 생성하고 DNS에 DNS 레코드 게시

다음으로, 새 DKIM 서명 프로필을 생성하고, 해당 DKIM 서명 프로필에서 DKIM DNS 레코드를 생성하고, 해당 레코드를 DNS에 게시해야 합니다.

1. Mail Policies(메일 정책) > Signing Profiles(서명 프로필)로 이동하여 "Add Profile...(프로필 추가...)"을 클릭합니다. "Profile Name(프로필 이름)" 필드에 프로필을 설명하는 이름을 지정합니다."도메인 이름" 필드에 도메인을 입력합니다."Selector" 필드에 새 선택기 문자열을 입력합니다.
   참고: *선택기는 지정된 도메인에 대해 여러 DKIM DNS 레코드를 허용하는 데 사용되는 임의의 문자열입니다.선택기를 사용하여 DNS에서 둘 이상의 DKIM DNS 레코드를 도메인에 허용합*

니다.기존 DKIM 서명 프로파일과 다른 새 선택기를 사용하는 것이 중요합니다.
"Signing Key" 필드의 이전 섹션에서 만든 DKIM 서명 키를 선택합니다.서명 프로필의 맨 아래에 새 "User"를 추가합니다. 이 사용자는 사용되지 않는 자리 표시자 전자 메일 주소여야 합니다. **주의:***이 서명 프로필의 사용자로 사용하지 않는 이메일 주소를 추가해야 합니다.그렇지 않으면 이 프로필은 DKIM TXT 레코드가 게시되기 전에 아웃바운드 메시지에 서명하여 DKIM 확인에 실패할 수 있습니다.사용하지 않는 이메일 주소를 사용자로 추가하면 이 서명 프로파일이 아웃바운드 메시지에 서명하지 않습니다.*Submit(제출)을 클릭합니다.

2. 여기에서 방금 생성한 서명 프로필에 대한 "DNS Text Record" 열에서 "Generate"를 클릭하고 생성된 DNS 레코드를 복사합니다.다음과 비슷한 모양이어야 합니다.

```
selector2._domainkey.example.com. IN TXT "v=DKIM1;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMaX6wMAk4iQoLNWiEkj0BrIRMDHXQ7743OQUOYZQqEXS
s+jMGomOknAZJpjR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qj1CSc1LTMdV0HWAi2AGsVOT8BdFHkyxg40
oyGWgktzc1q7zIgWM8usHfKVWFzYgnattNzyEqHsfI7lGilz5gdHBOvmF8LrDSfN"
"KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkrl9riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN
QZ1PrS6Zwr7ZxSRa316Oxc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB;"
```

3. 변경 사항을 커밋합니다.
4. 2단계에서 DKIM DNS TXT 레코드를 DNS에 제출합니다.
5. DKIM DNS TXT 레코드가 완전히 전파될 때까지 기다립니다.

이전 서명 프로필을 삭제하고 새 서명 프로필에서 자리 표시자 사용자를 제거합니다.

DKIM TXT 레코드가 DNS에 제출되고 해당 레코드가 전파되었는지 확인한 후 다음 단계는 이전 서명 프로파일을 삭제하고 새 서명 프로파일에서 자리 표시자 사용자를 제거하는 것입니다.

> **참고:** *다음 단계를 진행하기 전에 ESA 컨피그레이션 파일을 백업하는 것이 좋습니다.이전 DKIM 서명 프로필을 삭제하고 이전 구성으로 돌아가야 하는 경우 백업된 구성 파일을 쉽게 로드할 수 있기 때문입니다.*

1. Mail Policies(메일 정책) > Signing Profiles(서명 프로필)로 이동하여 이전 DKIM 서명 프로필을 선택하고 "Delete(삭제)"를 클릭합니다.
2. 새 DKIM 서명 프로필로 이동하여 현재 자리 표시자 사용자를 선택하고 "제거"를 클릭합니다.
3. "Submit(제출)"을 클릭합니다.
4. "Test Profile(테스트 프로필)" 열에서 새 DKIM 서명 프로필에 대해 "Test(테스트)"를 클릭합니다.테스트가 성공한 경우 다음 단계로 진행합니다.그렇지 않은 경우 DKIM DNS TXT 레코드가 완전히 전파되었는지 확인합니다.
5. 변경 사항을 커밋합니다.

DKIM 통과를 확인하기 위해 메일 흐름 테스트

이제 DKIM 구성을 더 이상 수행할 수 없습니다.그러나 DKIM 서명을 테스트하여 예상대로 아웃바운드 메시지에 서명하고 DKIM 확인을 통과하는지 확인해야 합니다.

1. ESA를 통해 DKIM이 ESA에서 서명하도록 하고 다른 호스트에서 DKIM을 확인하도록 메시지를 보냅니다.
2. 메시지가 다른 쪽 끝에 수신되면 "Authentication-Results" 헤더에 대한 메시지 헤더를 확인합니다. 헤더의 DKIM 섹션을 찾아 DKIM 확인을 통과했는지 확인합니다.헤더는 다음과 비슷해

야 합니다.

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

3. 헤더 "DKIM-Signature(DKIM-서명)"를 찾고 올바른 선택기와 도메인이 사용되고 있는지 확인합니다.

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

4. DKIM이 의도한 대로 작동하고 있다고 판단되면 이전 DKIM TXT 레코드를 제거하기 전에 최소 1주 동안 기다립니다.이렇게 하면 이전 DKIM 키로 서명된 모든 메시지가 처리됩니다.