SPF 구성 및 모범 사례

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 SPF(Sender Policy Framework)를 사용하는 다양한 시나리오에 대해 설명합니다.

사전 요구 사항

Cisco에서는 다음 주제를 알고 있는 것이 좋습니다.

- Cisco ESA
- 모든 버전의 AsyncOS

SPF란 무엇입니까?

SPF(Sender Policy Framework)는 이메일 스푸핑을 수신하여 해당 도메인의 관리자가 승인한 호스트에서 도메인에서 들어오는 메일이 전송되는지 확인하는 메커니즘을 제공하여 이메일 스푸핑을 탐지하도록 설계된 간단한 이메일 검증 시스템입니다.도메인에 대해 인증된 전송 호스트 목록은 해당 도메인의 DNS(Domain Name System) 레코드에 특수 형식의 TXT 레코드 형식으로 게시됩니다.이메일 스팸 및 피싱은 종종 위조 발신자 주소를 사용하므로 SPF 레코드를 게시 및 검사하는 것이 안티스팸 기술로 간주될 수 있습니다.

ESA에 성능에 큰 영향을 미칩니까?

CPU 잠재 고객은 성능에 큰 영향을 미치지 않습니다.그러나 SPF 확인을 활성화하면 DNS 쿼리 및 DNS 트래픽의 수가 증가합니다.모든 메시지에 대해 ESA는 1~3개의 SPF DNS 쿼리를 시작해야 할 수 있으며, 이로 인해 DNS 캐시가 이전보다 빨리 만료될 수 있습니다.따라서 ESA는 다른 프로세스에 대해서도 더 많은 쿼리를 생성합니다.

이전 정보 외에도, SPF 레코드는 일반 DNS 레코드보다 클 수 있는 TXT 레코드이며 일부 추가 DNS

트래픽을 유발할 수 있습니다.

SPF는 어떻게 활성화합니까?

다음 지침은 SPF 확인 설정에 대한 Advance User Guide에서 제공됩니다.

기본 메일 플로우 정책에서 SPF/SIDF(System Independent Data Format)를 활성화하려면

1. Mail **Policies(메일 정책) > Mail Flow Policy(메일 플로우 정책)를 클릭합니다**.
2. Default **Policy Parameters를 클릭합니다**.
3. 기본 정책 매개변수에서 **Security Features** 섹션을 확인합니다.
4. SPF/SIDF Verification(SPF/SIDF 확인) 섹션에서 **Yes(예)**를 클릭합니다.
5. 적합성 레벨을 설정합니다(기본값은 SIDF 호환). 이 옵션을 사용하면 사용할 SPF 또는 SIDF 확인의 표준을 결정할 수 있습니다.SIDF 적합성 외에도 SPF와 SIDF를 결합하는 SIDF-compatible을 선택할 수 있습니다.적합성 레벨 세부 정보는 최종 *사용 설명서*에서 확인할 수 있습니다.
6. SIDF 호환 가능 레벨을 선택하는 경우, Resent-Sender가 있는 경우 확인이 PRA ID의 **Pass** 결과를 None으로 다운그레이드할지 여부를 구성합니다.또는 재전송:메시지에 있는 헤더입니다.보안을 위해 이 옵션을 선택할 수 있습니다.
7. SPF의 적합성 수준을 선택하는 경우 HELO ID에 대해 테스트를 수행할지 여부를 구성합니다.이 옵션을 사용하여 HELO 검사를 비활성화하여 성능을 향상시킬 수 있습니다.spf-passed 필터 규칙이 먼저 PRA 또는 MAIL FROM IDENTITIES를 검사하기 때문에 유용할 수 있습니다.어플라이언스는 SPF 적합성 레벨에 대해 HELO 확인만 수행합니다.

SPF 확인 결과에 대한 작업을 수행하려면 콘텐츠 필터를 추가하십시오.

1. 각 SPF/SIDF 확인 유형에 대한 spf-status 콘텐츠 필터를 만듭니다.이름 지정 규칙을 사용하여 확인 유형을 지정합니다.예를 들어, **SPF**/SIDF 확인을 전달하는 메시지에 SPF-**Passed**를 사용하거나 확인 중에 일시적인 오류로 인해 전달되지 않은 메시지에 대해 SPF-**TempErr**을 사용합니다.spf-status 콘텐츠 필터 생성에 대한 자세한 내용은 GUI에서 spf-status Content Filter Rule을 참조하십시오.
2. 일부 SPF/SIDF 확인 메시지를 처리한 후 **Monitor > Content Filters**를 클릭하여 각 SPF/SIDF 확인 콘텐츠 필터를 트리거한 메시지 수를 확인합니다.

"헬로 테스트"가 켜지고 꺼진 것은 무엇을 의미합니까?Helo 테스트가 특정 도메인에서 실패하면 어떻게 됩니까?

SPF의 적합성 수준을 선택하는 경우 HELO ID에 대해 테스트를 수행할지 여부를 구성합니다.이 옵션을 사용하여 HELO 검사를 비활성화하여 성능을 향상시킬 수 있습니다.spf-passed 필터 규칙이 먼저 PRA 또는 MAIL FROM IDENTITIES를 검사하기 때문에 유용할 수 있습니다.어플라이언스는 SPF 적합성 레벨에 대해 HELO 확인만 수행합니다.

유효한 SPF 레코드

SPF HELO 검사를 전달하려면 각 전송 MTA에 대해 SPF 레코드(도메인과 별개)를 포함해야 합니다. 이 레코드를 포함하지 않을 경우 HELO 확인은 HELO ID에 대한 **None** 판정을 초래할 수 있습니다.도메인에 보낸 SPF가 높은 수의 **None** 판정을 반환한다는 것을 알게 되면 이러한 발신자는 각 전

송 MTA에 대해 SPF 레코드를 포함하지 않을 수 있습니다.

메시지/콘텐츠 필터가 구성되지 않은 경우 메시지가 전달됩니다.다시, 모든 SPF/SIDF 판정에 대해 메시지/콘텐츠 필터를 사용하여 특정 작업을 수행할 수 있습니다.

하나의 외부 도메인에만 사용할 수 있는 가장 좋은 방법은 무엇입니까?

특정 도메인에 대해 SPF를 활성화하려면 SPF가 활성화된 메일 플로우 정책으로 새 발신자 그룹을 정의해야 할 수 있습니다.앞서 설명한 대로 필터를 생성합니다.

의심되는 스팸에 대한 SPF 검사를 활성화할 수 있습니까?

Cisco Anti-Spam은 스팸 점수를 계산하는 동안 상당한 요인을 고려합니다.확인 가능한 SPF 레코드를 보유하면 스팸 점수가 줄어들지만, 의심스런 스팸으로 그러한 메시지가 포착될 가능성은 여전히 있습니다.

가장 좋은 방법은 Allowlist the sender IP address 또는 CREATE a message filter to skip spam check with multiple conditions (remote-ip, mail-from, X-skipspamcheck header 등)(발신자 IP 주소를 허용하거나 여러 조건(remote-ip, mail-from, X-skipspamcheck 헤더 등)으로 스팸 검사를 건너뛰도록 메시지 필터를 생성하는 것입니다. 송신 서버에서 헤더를 추가하여 다른 사용자가 보낸 메시지 유형을 식별할 수 있습니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 이메일 인증 모범 사례 - SPF/DKIM/DMARC 구축
- 기술 지원 및 문서 – Cisco Systems