Cisco ESA(Email Security Appliance)에서 인증서 확인을 위한 알고리즘은 무엇입니까?

목차

소개

TLS를 사용하여 Cisco ESA(Email Security Appliance)를 통해 이메일을 전송하는 경우 'Verify' 또는 'Hosted Verify' 옵션을 사용하여 인증서 확인을 수행하도록 선택할 수 있습니다. 이는 TLS를 통한 이메일 전달을 보호하는 데 있어 매우 중요한 부분이며, 이 확인이 어떻게 수행되는지 파악하는 것이 중요합니다.

Cisco ESA(Email Security Appliance)에서 인증서 확인을 위한 알고리즘은 무엇입니까?

두 가지 알고리즘이 있습니다. 하나는 '확인' 옵션과 다른 하나는 '호스팅 확인' 옵션입니다. 일반적으로 'Hosted Verify' 옵션은 더 다양한 시나리오와 호환되므로 권장됩니다.

배경 정보

- 이 문서는 AsyncOS 8.0.1 이상 버전을 기반으로 합니다. 이전 버전의 AsyncOS는 동작이 약간 다를 수 있습니다.
- 달리 지정하지 않는 한 와일드카드 매칭이 지원됩니다.
- 각 알고리즘은 성공적인 일치 후 중지되고 후속 검사가 평가되지 않습니다.
- CLI 명령 tlsverify**는** '확인 알고리즘'을 사용합니다.

정의

- CN:인증서 주체의 일부인 공통 이름입니다.
- SAN:Subject Alternate Name(주체 대체 이름) 확장명을 X.509로 지정합니다. 이 문서에서 사용할 때는 SAN 필드에 포함된 모든 DNS 이름을 지칭합니다.
- 이메일 도메인:수신자 이메일 주소의 도메인 부분입니다. 예를 들어, 'user@example.com'에 전달할 때 이메일 도메인은 'example.com'입니다.
- MX 호스트 이름:이메일 도메인의 MX 레코드의 호스트 이름입니다.
- PTR 호스트 이름:ESA가 연결하는 IP 주소의 DNS PTR 조회에서 반환되는 호스트 이름입니다.
- SMTP 경로 호스트 이름:이 대상에 대해 SMTP 경로가 구성된 경우 SMTP 경로에 사용되는 호

스트 이름입니다.

호스트 검증 알고리즘

1. 인증서에 SAN 특성이 포함된 경우 *이* 특성만 사용되며 CN은 무시됩니다. CN은 인증서에 SAN 특성이 없는 경우에만 사용됩니다. 이는 RFC 6125를 준수합니다.
2. 인증서가 이메일 도메인에 대해 확인됩니다.
3. 인증서가 존재할 수 있는 SMTP 경로 호스트 이름에 대해 확인됩니다.
4. 인증서가 MX 호스트 이름에 대해 확인됩니다.
5. 이전 확인 중 성공하지 못한 경우 확인이 실패합니다.

알고리즘 확인

1. SAN 특성은 이메일 도메인에 대해 확인됩니다.
2. CN이 이메일 도메인에 대해 확인됩니다. **참고:**와일드카드 일치는 지원되지 않습니다.
3. SAN 특성은 PTR 호스트 이름에 대해 확인됩니다.
4. 이전 확인 중 성공하지 못한 경우 확인이 실패합니다.