스팸 격리 서비스에 대해 ESA와 SMA 간의 TLS를 활성화하는 방법

목차

소개

이 문서에서는 ESA(Email Security Appliance)와 SMA(Security Management Appliance) 간 TLS(Transport Layer Security)를 스팸 격리 서비스용 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

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. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

이 기능은 공식적인 지원 기능은 아니므로 다음 지침에 따라 이 작업을 수행할 수 있습니다. 이 기능은 통합되는 동안 이 용도로 몇 가지 개선 요청이 생성됩니다.

구성

1. 마스크되지 않은 비밀번호로 SMA에서 최신 컨피그레이션 파일을 다운로드합니다.
2. 텍스트 편집기에서 구성 파일을 엽니다.
3. 컨피그레이션 파일에서 **euq_listener**를 찾습니다.

4. 기본 HAT 설정에 대한 섹션을 찾을 때까지 몇 줄 아래로 스크롤합니다.

값이 0이면 TLS가 꺼져 있고 STARTTLS가 제공되지 않음을 나타냅니다. 값이 1이면 TLS가 기본 설정됨을 나타내고 값이 2이면 TLS가 필요합니다.

5. 값을 예를 들어 1로 변경하고 컨피그레이션 파일을 저장한 후 SMA에 다시 업로드합니다.
6. ESA에서 **Mail Policies(메일 정책) > Destination Controls(대상 제어)로 이동하고** 도메인에 대한 새 항목을 추가합니다. .euq.queue에서 **TLS Support Preferred를** 선택합니다.
7. ESA에서 포트 6025의 SMA IP로 수동 텔넷 테스트를 실행하여 STARTTLS가 제공되는지 확인합니다.

참고: .euq.queue는 최종 사용자 격리에 대한 배달 큐의 특수 이름입니다.

메시지가 중앙 집중식 스팸 격리로 전송되면 ESA는 이제 TLS 연결을 설정하고 암호화된 SMTP 대화로 메시지를 전달하려고 시도해야 합니다.