바운스 확인 및 대상 제어를 위한 모범 사례 가이드

목차

소개

제어되지 않는 대용량 이메일 전달으로 수신인 도메인이 마비될 수 있습니다.AsyncOS는 Email Security 서비스가 열 연결 수 또는 각 대상 도메인으로 보낼 메시지 수를 정의하여 메시지 전달을 완벽하게 제어할 수 있습니다.

이 문서에서는 다음을 다룹니다.

1. 반송 공격으로부터 조직을 보호하기 위한 반송 확인 설정
2. 대상 제어 테이블을 사용하여 올바른 인접 디바이스 정책 실행
3. 메시지를 안전하게 전달하도록 DANE(Named Entities)의 SMTP DNS 기반 인증 구축

바운스 확인

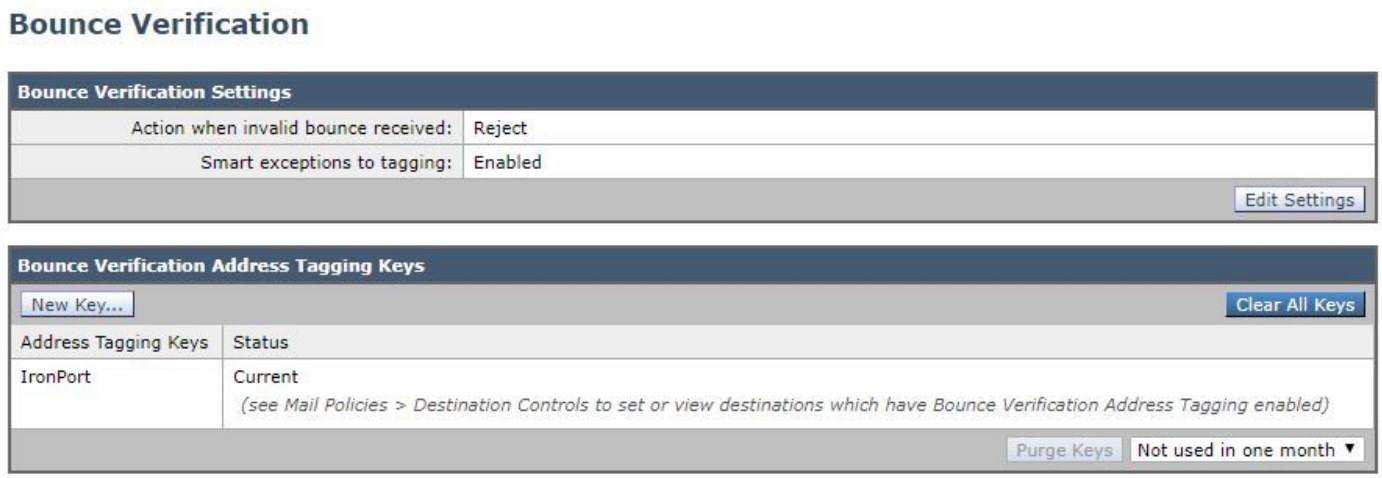
바운스 확인을 활성화하면 백분산/반송 공격을 효과적으로 차단할 수 있습니다. 바운스 확인 뒤의 개념은 간단합니다.먼저, 메시지를 ESA.모든 반송 메시지에서 해당 마크업을 찾습니다. 마크업이 있으면 사용자 환경에서 시작된 메시지의 반송 입니다.마크업이 없으면 반송이 거짓으로 생성되어 거부되거나 삭제될 수 있습니다.

예: MAIL FROM: joe@example.com 메일 받는 사람: prvs=joe=123ABCDEFG@example.com.예시의 123.. 문자열은 반송 ESA 어플라이언스에서 전송할 때 봉투 발신자에 추가되는 확인 태그다음 경우 메시지 바운스, 바운스된 메시지의 봉투 수신자 주소에 바운스 확인 태그 - ESA에서 합법적인 바운스임을 알 수 있습니다. 메시지.

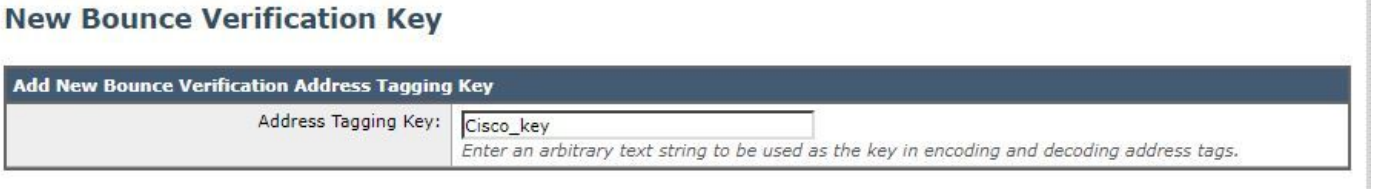
기본적으로 시스템 전체에서 바운스 확인 태그 지정을 활성화하거나 비활성화할 수 있습니다.다음을 수행할 수 있습니다. 또한 특정 도메인에 대한 바운스 확인 태깅을 활성화 또는 비활성화합니다.대부분의 경우 모든 도메인에 기본적으로 활성화되어 있습니다.

ESA 컨피그레이션

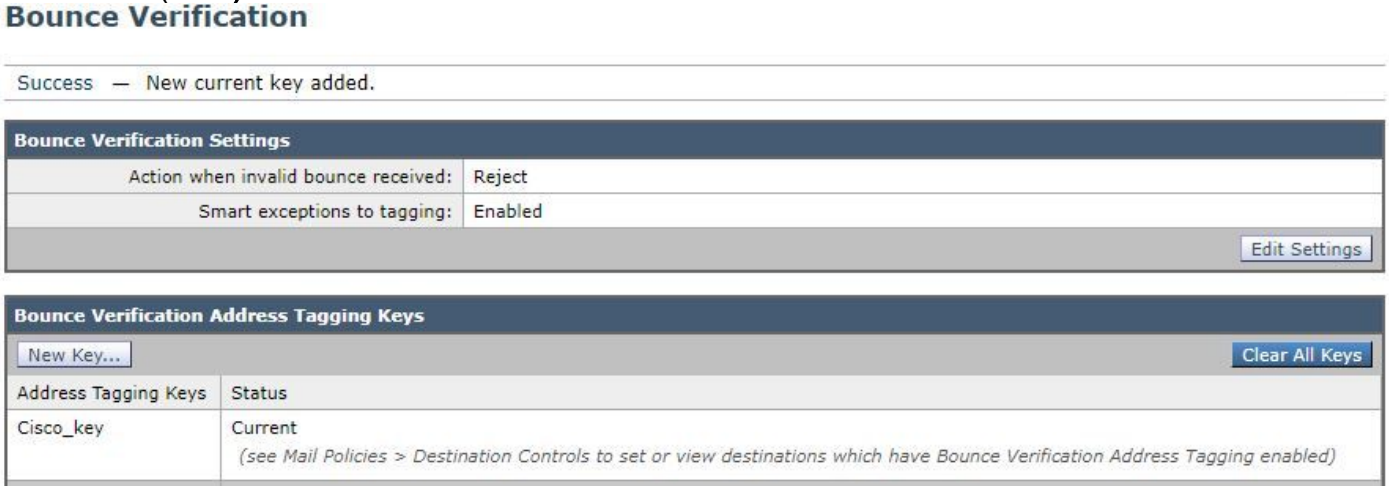
- Mail Policies(**메일 정책) > Bounce Verification(바운스 확인)으로** 이동하고 **New Key(새 키)**를 클릭합니다.



- 인코딩 및 디코딩 주소 태그의 키로 사용할 임의의 텍스트를 입력합니다.예: "Cisco_key"

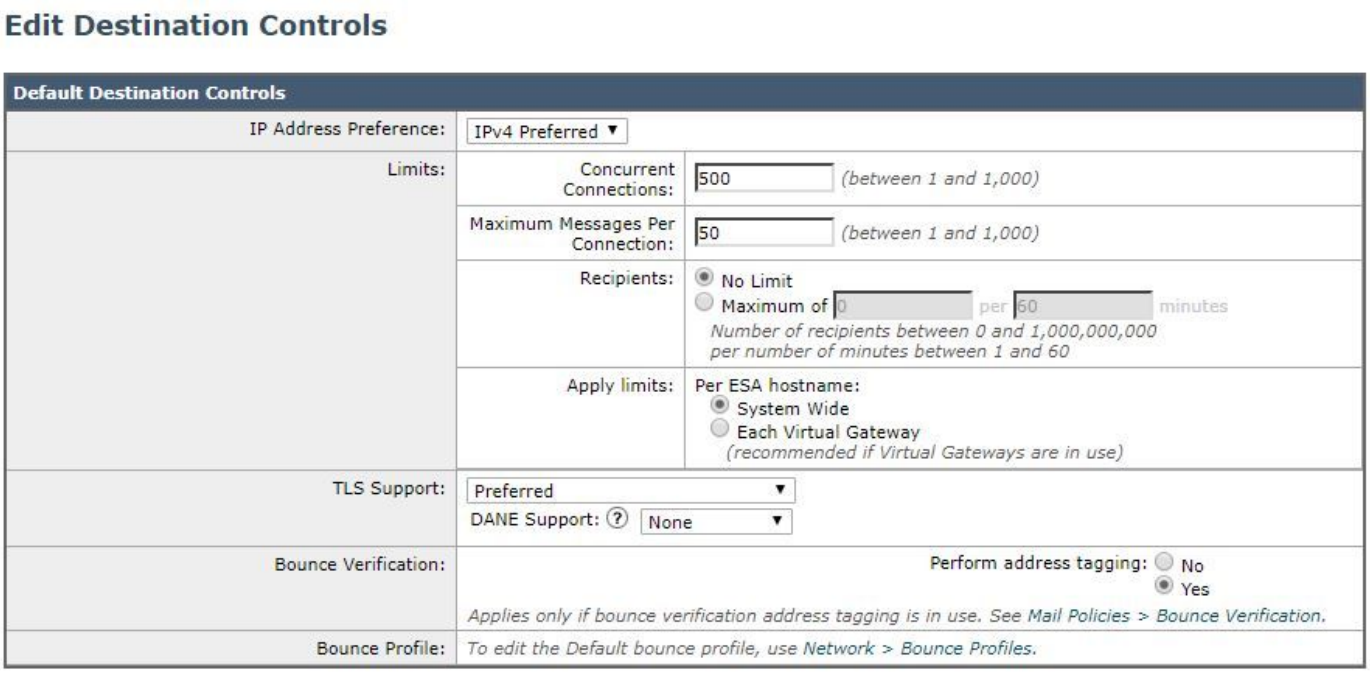


- Submit(제출)을 클릭하고 새 주소 태깅 키를 확인합니다.

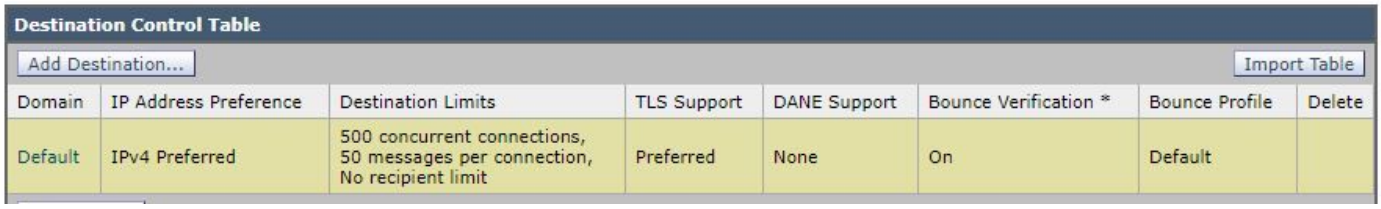


이제 "기본" 도메인에 대해 바운스 확인을 활성화하겠습니다.

- Mail Policies(**메일 정책) > Destination Controls(대상 제어)**로 이동하고 Default(기본값)를 **클릭합니다.**
- 바운스 **확인 구성:주소 태깅 수행:**예



- Submit and **Commit 변경 사항을 클릭합니다.**이제 기본 도메인에 대해 바운스 검증이 켜져 있습니다.



대상 제어 테이블 사용

제어되지 않은 이메일 전달은 수신자 도메인을 압도할 수 있습니다.ESA는 어플라이언스가 열 연결 수 또는 개수를 정의하여 메시지 전달 어플라이언스가 각 대상 도메인으로 전송할 메시지 대상 제어 테이블은 ESA가 원격 대상에 제공할 수 있습니다.또한 이러한 대상에 TLS 사용을 시도하거나 적용하는 설정을 제공합니다.ESA는 Destination Control Table에 대한 기본 컨피그레이션으로 구성됩니다.

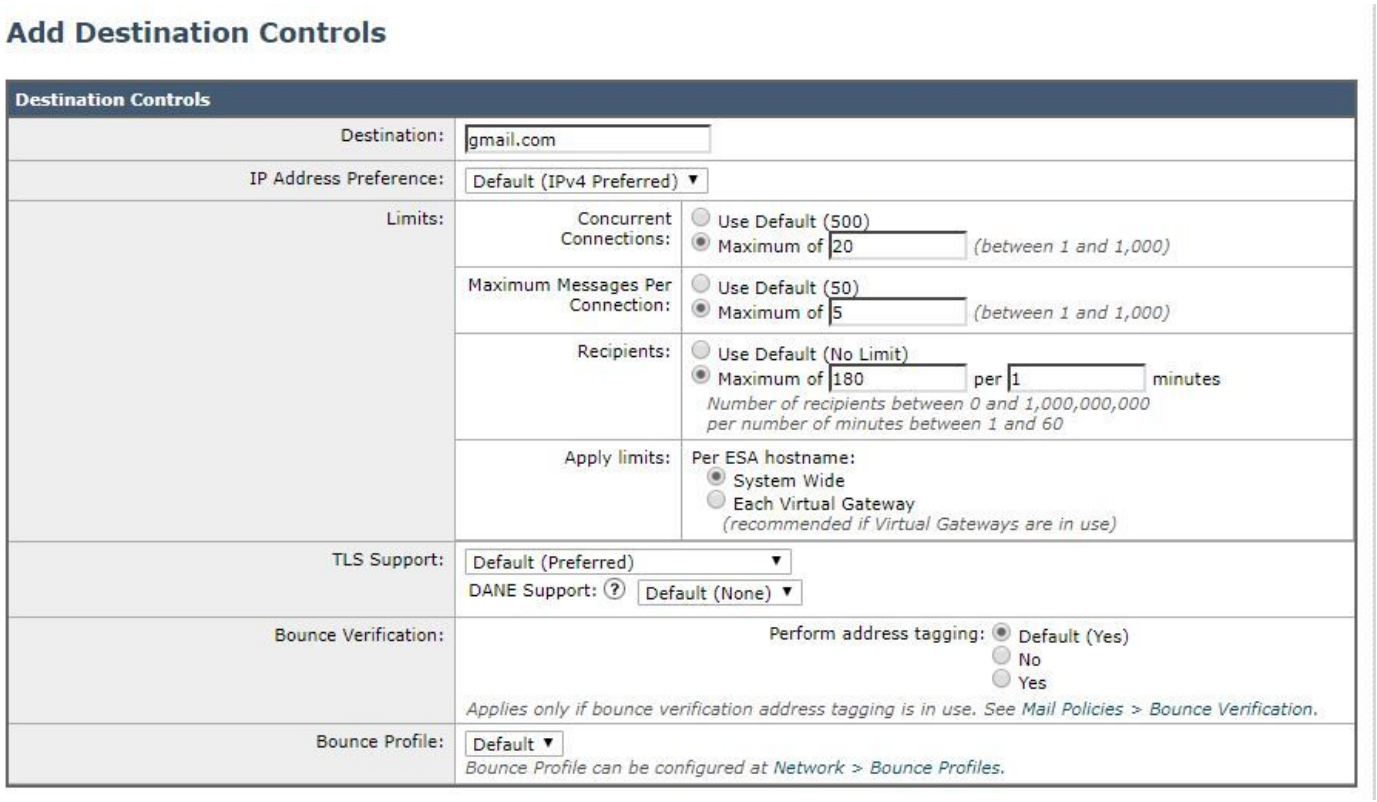
이 문서에서 다룰 내용은 기본값이 적합하지 않은 대상에 대한 제어를 관리하고 구성하는 방법입니다.예를 들어, Google에는 Gmail 사용자가 따라야 하는 수신 규칙 집합이 있거나, Gmail 사용자가 SMTP 4XX 응답 코드를 다시 보내는 것과 너무 빨리 전송한다는 메시지 또는 수신자의 사서함이 저장소 제한을 초과했다는 메시지가 있습니다.Gmail 도메인을 대상 제어 테이블에 추가하여 아래의 Gmail 수신자에게 보내는 메시지의 양을 제한합니다.

대상 제어 테이블에 새 도메인 추가

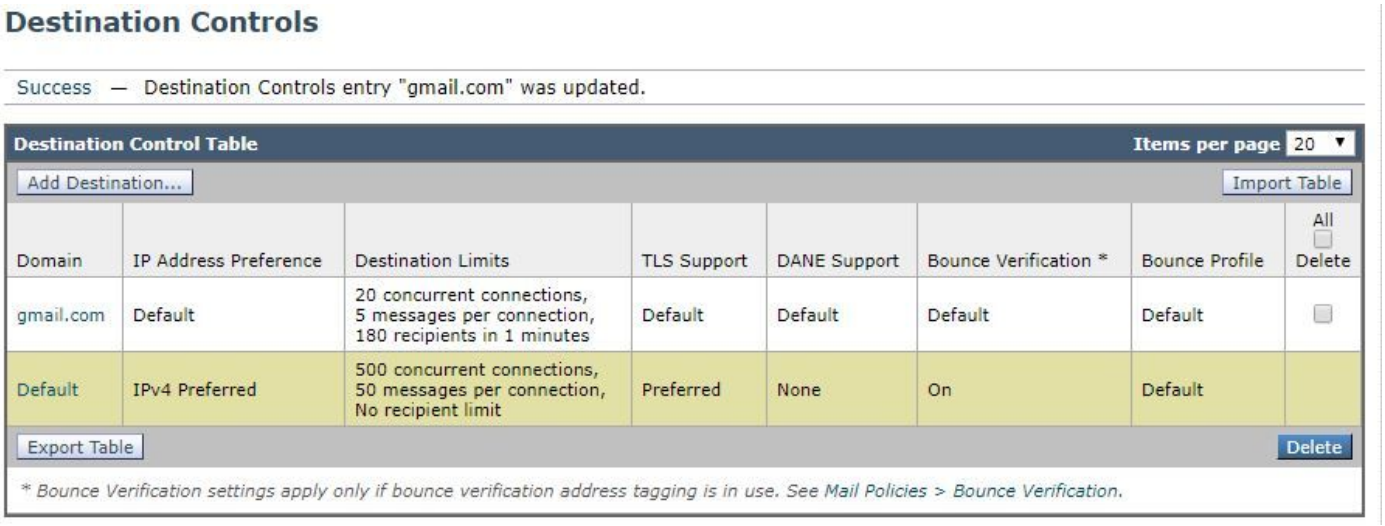
Google은 Gmail에 전송하는 발신자에 대한 제한이 있습니다.수신 제한은 여기에 게시된 Gmail 발신자 제한을 확인하여 확인할 수 있습니다. https://support.google.com/a/answer/1366776?hl=en

좋은 인접 디바이스 정책의 예로 Gmail의 대상 도메인을 설정해 보겠습니다.

- Mail Policies(**메일 정책) > Destination Controls(대상 제어)**로 이동하고 **Add Destination(대상 추가)**을 클릭하고 다음 매개변수를 사용하여 새 프로파일을 생성합니다. **대상:gmail.comIP 주소 기본 설정:IPv4 기본 설정동시 연결:최대 20개연결당 최대 메시지 수:5수신자:1분당 최대 180바운스 확인:주소 태깅 수행:기본값(예)**



• **[전송 및 커밋] 변경**을 누릅니다. 도메인 추가 후 대상 제어 테이블은 다음과 같습니다.
아래 이미지에서 "Destination Limits(대상 제한)" 및 "Bounce Verification(바운스 확인)"이 변경됩니다.



DANE(Named Entities)의 SMTP DNS 기반 인증 구축

SMTP DNS 기반 DANE(Authentication of Named Entities) 프로토콜은 DNS 서버에 구성된 DNSSEC(Domain Name System Security) 확장 및 TLSA 레코드라고도 하는 DNS 리소스 레코드를 사용하여 DNS 이름으로 X.509 인증서를 검증합니다.

TLSA 레코드는 RFC 6698에 설명된 DNS 이름에 사용되는 CA(Certificate Authority), 최종 엔티티 인증서 또는 트러스트 앵커에 대한 세부 정보가 포함된 인증서에 추가됩니다.DNSSEC(Domain Name System Security) 확장은 DNS 보안의 취약성을 해결하여 DNS에 보안을 강화합니다.암호화 키 및 디지털 서명을 사용하는 DNSSEC는 조회 데이터가 정확한지 확인하고 합법적인 서버에 연결합니다.

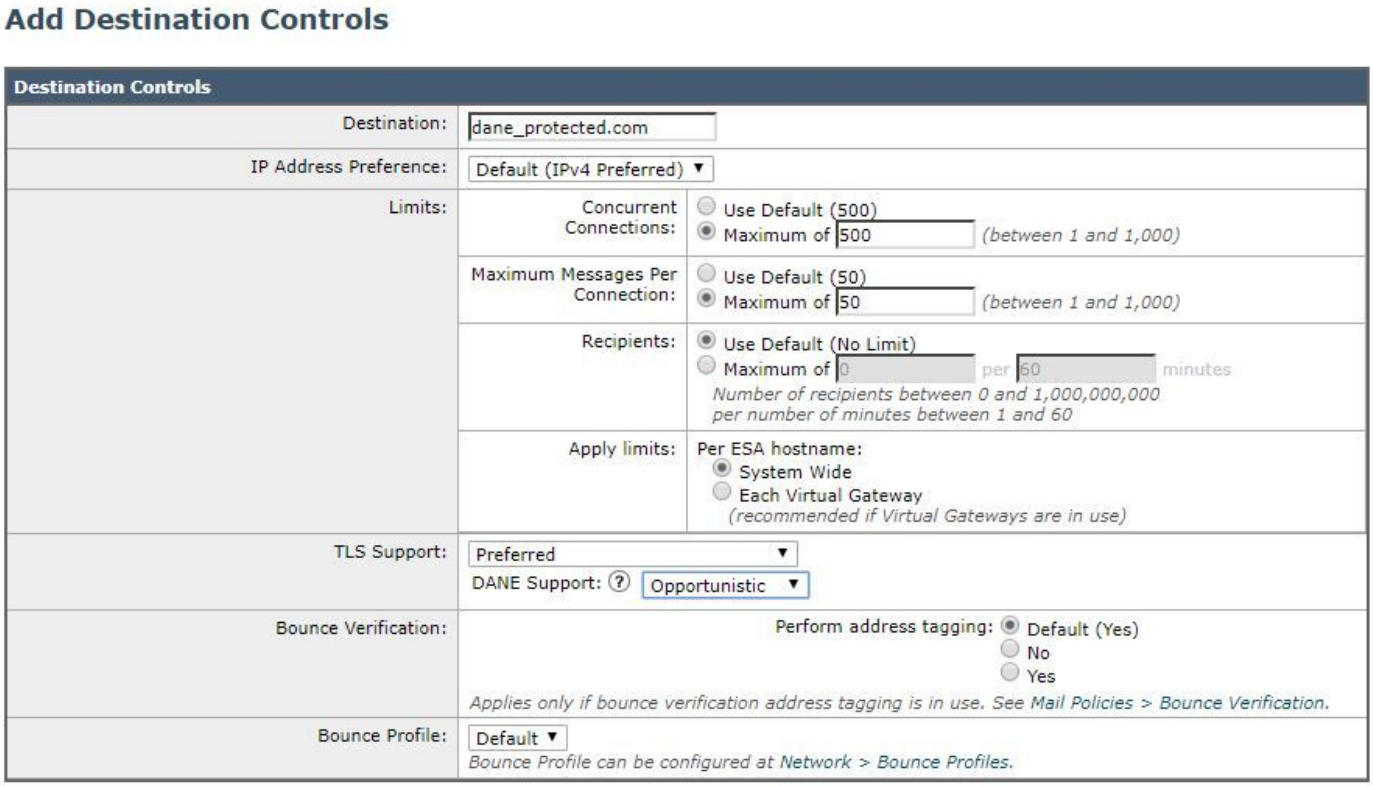
다음은 발신 TLS 연결에 SMTP DANE를 사용할 때의 이점입니다.

- MITM(Man-in-the-Middle) 다운그레이드 공격, 도청 및 DNS 캐시 중독 공격을 방지하여 메시지를 안전하게 전달합니다.
- DNSSEC에서 보호하는 경우 TLS 인증서 및 DNS 정보의 신뢰성을 제공합니다.

ESA 컨피그레이션

ESA에서 DANE를 설정하기 전에 봉투 발신자 및 TLSA 리소스 레코드가 DNSSEC으로 확인되었으며 수신 도메인이 DANE로 보호되었는지 확인하십시오.CLI 명령 daneverify를 사용하여 ESA에서 이 작업을 수행할 수 **있습니다**.

- Mail Policies(**메일 정책) > Destination Controls(대상 제어)**로 이동하고 **Add Destination(대상 추가)**을 클릭하고 다음 매개변수를 사용하여 새 프로파일을 생성합니다. **대상: dane_protected.comTLS 지원:**기본 설정**DANE 지원:**기회주의적



- Submit and **Commit 변경 사항을 클릭합니다.**