Cisco RES:TLS를 사용하여 암호화되지 않은 RES 회신을 보호하는 방법

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)와 연계하여 사용자가 해독할 필요가 없는 Cisco CRES(Registered Envelope Service)의 회신을 보호하기 위해 TLS(Transport Layer Security)를 사용하는 방법에 대해 설명합니다.

Cisco RES:TLS를 사용하여 암호화되지 않은 RES 회신을 보호하는 방법

기본적으로 보안 이메일에 대한 회신은 Cisco RES에 의해 암호화되어 메일 게이트웨이로 전송됩니다.그런 다음 최종 사용자가 Cisco RES 자격 증명으로 열도록 암호화된 메일 서버로 통과합니다.

사용자가 보안 응답을 열기 위해 Cisco RES로 인증해야 할 필요성을 피하기 위해 Cisco RES는 TLS를 지원하는 메일 게이트웨이에 "암호화되지 않은" 형태로 제공합니다. 대부분의 경우 메일 게이트웨이는 ESA이며 이 문서가 적용됩니다.

그러나 외부 스팸 필터와 같이 ESA 앞에 다른 메일 게이트웨이가 있는 경우 ESA에서 인증서/TLS/메일 흐름 컨피그레이션이 필요하지 않습니다.이 경우 이 문서의 솔루션 섹션에서 1~3단계를 건너뛸 수 있습니다.이 환경에서 작동하는 데 암호화되지 않은 회신의 경우 외부 스팸 필터(메일 게이트웨이)는 TLS를 지원해야 하는 어플라이언스입니다.TLS를 지원하는 경우 Cisco RES에서 이를 확인하고 "암호화되지 않은" 회신을 설정해 이메일을 안전하게 보호할 수 있습니다.

발신자 정책 프레임워크

SPF(Sender Policy Framework) 확인 실패를 방지하려면 mx:res.cisco.com, mxnat1.res.cisco.com 및 mxnat3.res.cisco.com을 SPF 레코드에 추가해야 합니다. 또는 SPF 레코드에 spfc.**spf.cisco.com**을 '포함'할 수 있습니다.

예:

```
 ~ dig txt spfc._spf.cisco.com +short
"v=spf1 mx:res.cisco.com mx:sco.cisco.com ~all"
```

SPF 레코드에 Cisco RES를 추가하는 위치와 방법은 네트워크 토폴로지에서 DNS(Domain Name System)가 구현되는 방식에 따라 달라집니다. 자세한 내용은 DNS 관리자에게 문의하십시오.

DNS가 Cisco RES를 포함하도록 구성되지 않은 경우 보안 작성 및 보안 응답이 생성되어 호스팅된 키 서버를 통해 전달되는 경우 발신 IP 주소가 수신자의 끝에 나열된 IP 주소와 일치하지 않아 SPF 확인 오류가 발생합니다.

호스트 이름 및 IP 주소

호스트 이름	IP 주소	레코드 유형
res.cisco.com	184.94.241.74	A
mxnat1.res.cisco.com	208.90.57.32	A
mxnat2.res.cisco.com	208.90.57.33	A
mxnat3.res.cisco.com	184.94.241.96	A
mxnat4.res.cisco.com	184.94.241.97	A
mxnat5.res.cisco.com	184.94.241.98	A
mxnat6.res.cisco.com	184.94.241.99	A
mxnat7.res.cisco.com	208.90.57.34	A
mxnat8.res.cisco.com	208.90.57.35	A
esa1.cres.iphmx.com	68.232.140.79	MX
esa2.cres.iphmx.com	68.232.140.57	MX
esa3.cres.iphmx.com	68.232.135.234	MX
esa4.cres.iphmx.com	68.232.135.235	MX

참고: 호스트 이름 및 IP 주소는 서비스/네트워크 유지 관리 또는 서비스/네트워크 증가에 따라 변경될 수 있습니다. 일부 호스트 이름과 IP 주소가 서비스에 사용되는 것은 아닙니다. 여기에 참고용으로 제공됩니다.

솔루션

1. ESA에 서명된 인증서 및 중간 인증서를 가져오고 설치합니다. **참고**: 어플라이언스에 제공되는 데모 인증서로 인해 CRES 확인 프로세스가 실패하므로 서명 기관으로부터 중간 인증서를 얻는 것이 중요합니다.

2. 새 메일 플로우 정책을 만듭니다. GUI에서 Mail Policies(**메일 정책) > Mail Flow Policies(메일 플로우 정책) > Add Policy(정책 추가)...를** 선택합니다..이름을 입력하고 *보안 기능*을 제외한 다른 모든 항목은 기본값으로 둡니다.*TLS.*이 값을 **필수**로 **설정합니다**.
3. 새 발신자 그룹을 만듭니다. GUI에서 Mail Policies(**메일 정책) > HAT Overview(HAT 개요) > Add Sender Group...을** 선택합니다..이름을 입력하고 주문 번호를 #1로 설정합니다. 선택적 코멘트를 입력할 수도 있습니다.2단계에서 생성한 메일 플로우 정책을 선택합니다. 그 밖의 모든 항목은 비워 둡니다.Submit **and Add Senders >>를 클릭합니다**.
4. Sender 필드에 다음 IP 범위 및 호스트 이름을 입력합니다.
```
.res.cisco.com
.cres.iphmx.com
208.90.57.0/26 (current CRES IP network range)
204.15.81.0/26 (old CRES IP network range)
```
5. 변경 사항을 제출하고 커밋합니다.
6. ESA가 Cisco RES 서버의 TLS에 대해 준비되었다고 확신한 후 내 도메인이 Cisco RES와 TLS를 지원하는지 테스트하려면 어떻게 합니까? 단계를 따라 Cisco RES 서버에 TLS를 사용하도록 요청합니다.

관련 정보

- Cisco RES:키 서버의 IP 주소 및 호스트 이름
- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems