ESA 리스너에서 인바운드 연결 암호화를 위한 TLS 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[GUI를 통해 리스너에 대한 HAT 메일 플로우 정책에서 TLS 활성화](#)
[CLI를 통해 리스너에 대한 HAT 메일 플로우 정책에서 TLS 활성화](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 ESA(Email Security Appliance)의 리스너에서 TLS(Transport Layer Security)를 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 모든 AsyncOS 버전의 ESA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

인바운드 연결을 위해 암호화가 필요한 모든 리스너에 대해 TLS를 활성화해야 합니다.인터넷을 접하는 리스너(퍼블릭 리스너)에서 TLS를 활성화할 수 있지만 내부 시스템(프라이빗 리스너)용 리스너는 사용할 수 없습니다. 또는 모든 리스너에 대해 암호화를 활성화할 수도 있습니다.기본적으로 프라이빗 또는 퍼블릭 리스너는 TLS 연결을 허용하지 않습니다.인바운드(수신) 또는 아웃바운드(전송) 이메일에 대해 TLS를 활성화하려면 리스너의 HAT(Host Access Table)에서 TLS를 활성화해야 합니다.또한 프라이빗 및 퍼블릭 리스너에 대한 메일 플로우 정책 설정은 기본적으로 TLS가 '꺼짐'으로 설정되어 있습니다.

구성

리스너에서 TLS에 대해 세 가지 설정을 지정할 수 있습니다.

설정	의미
아니요	TLS는 수신 연결에 허용되지 않습니다.리스너에 대한 연결에는 암호화된 SMTP(Simple Mail Transfer Protocol) 대화가 필요하지 않습니다.어플라이언스에서 구성하는 모든 리스너의 기본 설정입니다.
기본 설정	MTA(Message Transfer Agents)에서 리스너로의 수신 연결에 TLS가 허용됩니다.
필수	MTA에서 리스너로의 수신 연결에는 TLS가 허용되며, STARTTLS 명령이 수신될 때까지 ESA는 No Operation(NOOP), EHLO 또는 QUIT 이외의 모든 명령에 오류 메시지로 응답합니다.TLS가 '필수'인 경우 발신자가 TLS로 암호화하기를 원하지 않는 이메일은 전송되기 전에 ESA에서 거부하므로 암호화되지 않은 상태로 전송되지 않습니다.

GUI를 통해 리스너에 대한 HAT 메일 플로우 정책에서 TLS 활성화

다음 단계를 완료하십시오.

1. Mail Flow Policies(메일 플로우 정책) 페이지에서 정책을 수정할 리스너를 선택한 다음 수정할 정책 이름의 링크를 클릭합니다.기본 정책 매개변수를 수정할 수도 있습니다. Edit Mail Flow Policies 페이지가 표시됩니다.
2. "Encryption and Authentication(암호화 및 인증)" 섹션의 "Use TLS:" 필드에서 리스너에 대해 원하는 TLS 레벨을 선택합니다.
3. Submit(제출)**을 클릭합니다**.
4. Commit **Changes(변경 사항 커밋)**를 클릭하고 필요한 경우 선택 설명을 추가한 다음 **Commit Changes(변경 사항 커밋)를 클릭하여** 변경 사항을 저장합니다.

   참고:리스너를 생성할 때 개별 퍼블릭 리스너에 TLS 연결에 대한 특정 인증서를 할당할 수 있습니다.

CLI를 통해 리스너에 대한 HAT 메일 플로우 정책에서 TLS 활성화

1. 구성할 **리스너를** 선택하려면 listenerconfig > edit 명령을 사용합니다.
2. 리스너의 **기본 HAT** 설정을 편집하려면 hostaccess > default 명령을 사용합니다.
3. 프롬프트가 표시되면 TLS 설정을 변경하려면 다음 중 하나를 입력합니다.

```
Do you want to allow encrypted TLS connections?

   1. No
   2. Preferred
   3. Required
```

```
[1]>3

You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.
```

이 예에서는 리스너와 함께 사용할 수 있는 유효한 인증서가 있는지 확인하기 위해 certconfig 명령을 사용하라는 메시지를 표시합니다.인증서를 생성하지 않은 경우 리스너는 어플라이언스에 사전 설치된 데모 인증서를 사용합니다.테스트 목적으로 데모 인증서와 함께 TLS를 활성화할 수 있지만, 안전하지 않으며 일반적인 용도로 권장되지 않습니다.리스너에 인증서를 할당하려면 listenerconfig > edit > certificate 명령을 사용합니다.TLS를 구성하면 CLI의 리스너 요약에 설정이 반영됩니다.

```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: Required
```

4. 변경을 활성화하려면 commit 명령을 입력합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- 텍스트 메일 로그 파일을 사용하고 다음 문서를 참조하십시오. ESA에서 TLS를 전송 또는 수신하는지 확인
- 메시지 추적 사용:GUI:Monitor(모니터링) > Message Tracking(메시지 추적)
- 보고 사용:GUI:Monitor(모니터링) > TLS Connections(TLS 연결)
- checktls.com과 같은 서드파티 웹 사이트 사용

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

TLS 연결이 필요한 도메인에 메시지를 전달할 때 TLS 협상이 실패할 경우 ESA에서 알림을 전송할지 여부를 지정할 수 있습니다.경고 메시지에는 실패한 TLS 협상에 대한 대상 도메인의 이름이 포함됩니다.ESA는 시스템 경고 유형에 대한 경고 심각도 레벨 알림을 수신하도록 설정된 모든 수신자에게 경고 메시지를 전송합니다.GUI의 System Administration(시스템 관리) > Alerts(알림) 페이지(또는 CLI의 alertconfig 명령을 통해 알림 수신자를 관리할 수 있습니다.

관련 정보

- 최종 사용자 가이드 AsyncOS for Email
- 기술 지원 및 문서 – Cisco Systems