

ESA FAQ:메일 플로우 정책이란?

목차

[소개](#)

[메일 플로우 정책이란?](#)

[관련 정보](#)

소개

이 문서에서는 ESA(Email Security Appliance)에서 메일 흐름 정책이 무엇이고 메일 플로우 정책과 연결된 작업에 대해 설명합니다.

메일 플로우 정책이란?

메일 플로우 정책을 사용하면 SMTP 대화 중에 발신자에서 리스너로의 이메일 메시지 흐름을 제어하거나 제한할 수 있습니다.메일 플로우 정책에서 다음 유형의 매개변수를 정의하여 SMTP 대화를 제어합니다.

- 연결 매개 변수(예: 연결당 최대 메시지 수)
- 속도 제한 매개변수(예: 시간당 최대 수신자 수)
- SMTP 대화 중에 전달되는 맞춤형 SMTP 코드 및 응답을 수정합니다.
- 스팸 탐지를 활성화합니다.
- 바이러스 보호를 활성화합니다.
- 암호화(예: TLS를 사용하여 SMTP 연결 암호화)
- DKIM을 사용하여 수신 메일을 확인하는 등의 인증 매개변수

메일 플로우 정책은 원격 호스트의 연결에 대해 다음 작업 중 하나를 수행합니다.

- 수락.연결이 수락되고 RAT(Recipient Access Table)(퍼블릭 리스너용)를 비롯한 리스너 설정에 의해 이메일 수신이 추가로 제한됩니다.
- 거부.처음에는 연결이 허용되지만 연결하려는 클라이언트는 4XX 또는 5XX SMTP 상태 코드를 가져옵니다.수락된 이메일이 없습니다.

참고:또한 SMTP 대화 시작 시간이 아닌 메시지 수신자 레벨(RCPT TO)에서 이 거부를 수행하도록 AsyncOS를 구성할 수 있습니다.이러한 방식으로 메시지를 거부하면 메시지 거부가 지연되고 메시지가 반송되므로 AsyncOS에서 거부된 메시지에 대한 자세한 정보를 유지할 수 있습니다.이 설정은 CLI listenerconfig > **setup** 명령에서 구성합니다.

- TCPREFUSE입니다.TCP 레벨에서 연결이 거부됩니다.
- 릴레이연결이 수락됩니다.수신자에 대한 수신은 허용되며 RAT에 의해 제한되지 않습니다.
- 계속HAT(Host Access Table)의 매핑은 무시되고 HAT의 처리가 계속됩니다.수신 연결이 CONTINUE가 아닌 이후 항목과 일치하면 해당 항목이 대신 사용됩니다.CONTINUE 규칙은

GUI에서 HAT를 쉽게 편집하는 데 사용됩니다.

메일 플로우 정책은 이메일 파이프라인의 시작 단계이므로 원격 호스트가 ESA와의 연결을 설정하려고 할 때 이러한 매개변수가 적용됩니다.

메일 플로우 정책은 지정된 도메인, 이메일 주소 그룹 또는 특정 이메일 주소에서 수신하거나 목적지로 지정된 메일에서 수신할 메일에 적용할 안티스팸, 안티바이러스, 바이러스 전파 확산 및 콘텐츠 필터 매개변수를 정의하는 수신 및 발신 메일 정책과 다릅니다.

기본 메일 플로우 정책을 수정할 수 있으며 새 메일 플로우 정책을 정의할 수 있습니다.

퍼블릭 리스너에는 네 가지 기본 메일 플로우 정책이 정의되어 있습니다.

- 수락됨
- 차단됨
- 제한됨
- 신뢰할 수 있음

프라이빗 리스너는 다음 메일 플로우 정책을 사용합니다.

- 수락됨
- 차단됨
- 릴레이됨

관련 정보

- [Cisco Email Security Appliance - 엔드 유저 가이드](#)
- [기술 지원 및 문서 - Cisco Systems](#)