메일 플로우 정책 및 대상 제어 관련 매개변수 이해

목차

소개

이 문서에서는 ESA(Email Security Appliance)의 몇 가지 컨피그레이션 측면에 대해 발신자 제한 및 전달 방법에 대해 설명합니다.이 문서에서 설명하는 기능은 메일 플로우 정책 및 대상 제어입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 메일 플로우 정책 및 대상 제어에 대한 기본 이해
- ESA 컨피그레이션에서 이러한 기능의 사용에 대해 잘 알고 있음

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.

메일 플로우 정책 및 대상 컨트롤의 장점

이 두 기능 모두 가지는 매우 중요한 기능 중 하나는 속도 제한/조절(Rate Limiting/Throttling)입니다.이러한 측면을 통해 관리자는 어떤 트래픽이 자유로이 흐르도록 해야 하는지, 어떤 트래픽을 제한적으로 허용할 것인지를 제어할 수 있습니다.

메일 플로우 정책

이는 이메일 트래픽 변조를 수행하는 ESA의 발신자 그룹에 적용되는 정책입니다.

Mail Flow Policies(메일 플로우 정책)는 이메일이 Inbound(인바운드) 또는 Outbound(아웃바운드)인 것과 관계없이 항상 ESA로 수신되는 트래픽에 적용됩니다.

메일 플로우 정책은 백엔드에서 해당 정책에 대해 선택한 연결 동작과 관련하여 작동합니다.ESA에서 사용할 수 있는 다양한 연결 동작은 다음과 같습니다.

1. 수락
2. 거부
3. 릴레이
4. TCP 거부
5. 계속

수락:연결이 수락되고 수신자 액세스 테이블(퍼블릭 리스너용)을 비롯한 리스너 설정에 의해 이메일 수신이 추가로 제한됩니다. 이 연결 동작은 이메일을 인바운드 메시지로 간주합니다.

거부:연결하려는 클라이언트는 4XX 또는 5XX SMTP 상태 코드를 가져옵니다.수락된 이메일이 없습니다.이는 주로 블랙리스팅 발신자에 사용됩니다.

릴레이:연결이 수락됩니다.수신자에 대한 수신은 허용되며 수신자 액세스 테이블에 의해 제한되지 않습니다.이렇게 하면 이메일이 아웃바운드 이메일로 처리됩니다.

TCP 거부:TCP 레벨에서 연결이 거부됩니다.

계속:HAT의 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 정책의 구성 요소

최대연결당 메시지 수:원격 호스트로부터의 연결당 이 리스너를 통해 전송할 수 있는 최대 메시지 수각 ICID는 하나의 연결을 나타냅니다.

최대메시지당 수신자 수:이 메일 플로우 정책을 사용하여 처리된 이 호스트에서 수락될 메시지당 최대 수신자 수

최대메시지 크기:메일 플로우 정책에 태그가 지정된 이 리스너가 수락할 메시지의 최대 크기입니다.가능한 가장 작은 최대 메시지 크기는 1킬로바이트입니다.

최대단일 IP에서 동시 연결:단일 IP 주소에서 이 리스너에 연결할 수 있는 최대 동시 연결 수.

사용자 지정 SMTP 배너 코드:이 리스너와의 연결이 설정될 때 반환되는 SMTP 코드.

사용자 지정 SMTP 배너 텍스트:이 리스너와의 연결이 설정될 때 반환되는 SMTP 배너 텍스트.이 필드에서 일부 변수를 사용할 수 있습니다.

Override SMTP Banner Hostname(SMTP 배너 호스트 이름 재정의): 기본적으로 어플라이언스는 원격 호스트에 SMTP 배너를 표시할 때 리스너 인터페이스와 연결된 호스트 이름을 포함합니다(예: 220-hostname ESMTP). 여기에 다른 호스트 이름을 입력하여 이 배너를 재정의하도록 선택할 수 있습니다.또한 배너에 호스트 이름을 표시하지 *않도록* 선택하려면 호스트 이름 필드를 비워 둘 수 있습니다.

메일 흐름 제한

최대시간당 수신자 수:이 리스너가 원격 호스트에서 수신할 시간당 최대 수신자 수발신자 IP 주소당 수신자 수는 전역적으로 추적됩니다.그러나 각 리스너는 자체 속도 제한 임계값을 추적하지만, 모든 리스너가 단일 카운터에 대해 검증하기 때문에 동일한 IP 주소(발신자)가 여러 리스너에 연결하는 경우 속도 제한이 초과될 가능성이 높습니다.이 필드에서 일부 변수를 사용할 수 있습니다.

최대시간당 수신자 코드:호스트가 이 리스너에 대해 정의된 시간당 최대 수신자 수를 초과할 때 반환되는 SMTP 코드

최대시간당 수신자 텍스트:호스트가 이 리스너에 대해 정의된 시간당 최대 수신자 수를 초과할 때 반환되는 SMTP 배너 텍스트

봉투 발신자에 대한 속도 제한

최대시간 간격당 수신자 수:mail-from 주소를 기반으로 이 리스너가 고유한 봉투 발신자로부터 수신할 지정된 기간 동안의 최대 수신자 수.수신자 수는 전역적으로 추적됩니다.각 리스너는 자체 속도 제한 임계값을 추적합니다.그러나 모든 리스너가 단일 카운터에 대해 검증되므로 동일한 메일 수신 주소의 메시지를 여러 리스너에서 수신하는 경우 속도 제한이 초과될 가능성이 높습니다.

발신자 속도 제한 오류 코드:봉투(envelope)가 이 리스너에 대해 정의된 시간 간격의 최대 수신자 수를 초과할 때 반환되는 SMTP 코드입니다.

발신자 속도 제한 오류 텍스트:봉투 발신자가 이 리스너에 대해 정의된 시간 간격의 최대 수신자 수를 초과할 때 반환되는 SMTP 배너 텍스트

예외: 특정 봉투 발신자를 정의된 속도 제한에서 제외하려면 봉투 발신자가 포함된 주소 목록을 선택합니다.

주소 목록은 메일 정책 > 주소 목록에서 정의됩니다(전체 이메일 주소, 도메인, IP 주소를 면제에 사용할 수 있음).

Flow Control에 SenderBase 사용:이 리스너의 SenderBase Reputation Service에 대해 "조회"를 활성화합니다.

IP 주소의 유사성별 그룹화:대규모 CIDR 블록에서 리스너의 HAT(Host Access Table)에 있는 항목을 관리하는 동안 IP 주소별로 수신 메일을 추적하고 속도를 제한하는 데 사용됩니다.속도 제한을 위해 유사한 IP 주소를 그룹화하는 동시에 해당 범위 내의 각 IP 주소에 대한 개별 카운터를 유지할

수 있는 유효 비트 범위(0~32)를 정의합니다.

참고:"Use SenderBase"를 비활성화해야 합니다.

디렉토리 수집 공격 방지(DHAP)

최대시간당 올바르지 않은 수신인 수:이 리스너가 원격 호스트에서 수신할 시간당 최대 잘못된 수신자 수이 임계값은 총 RAT 거부 및 SMTP call-ahead 서버 거부 수와 SMTP 대화에서 삭제되거나 작업 대기열에서 반송된 잘못된 LDAP 수신자에 대한 총 메시지 수를 나타냅니다(관련 리스너의 LDAP 수락 설정에서 구성됨).

SMTP 대화 내에서 DHAP 임계값에 도달하면 연결 삭제:

유효하지 않은 수신자의 임계값에 도달하면 어플라이언스는 호스트에 대한 연결을 삭제합니다.

최대시간당 올바르지 않은 수신인 코드:연결을 삭제할 때 사용할 코드를 지정합니다.기본 코드는 550입니다.

최대시간당 올바르지 않은 수신인 텍스트:끊어진 연결에 사용할 텍스트를 지정합니다.기본 텍스트는 "잘못된 수신자가 너무 많습니다.

보안 기능

스팸/AMP/바이러스/발신자 도메인 평판 확인/보안 침해 필터/고급 피싱 보호/그레이메일/콘텐츠 및 메시지 필터:여기에서 보안 엔진/검사 및 필터의 관련 검사를 활성화하거나 비활성화할 수 있습니다.

암호화 및 인증:이 리스너에 대한 SMTP 대화에서 설정을 Off, Prefer 또는 Require TLS(Transport Layer Security)로 수정할 수 있습니다.

클라이언트 인증서가 유효한 경우 Verify Client Certificate(클라이언트 인증서 확인) 옵션은 Email Security Appliance에서 사용자의 메일 애플리케이션에 대한 TLS 연결을 설정하도록 지시합니다.

TLS Preferred(TLS 기본 설정)의 경우, 사용자에게 인증서가 없는 경우 어플라이언스는 비 TLS 연결을 허용하지만, 사용자에게 잘못된 인증서가 있는 경우 연결을 거부합니다.

TLS Required(TLS 필수) 설정의 경우 이 옵션을 선택하면 어플라이언스에서 연결을 허용하려면 사용자에게 유효한 인증서가 있어야 합니다.

SMTP 인증:리스너에 연결하는 원격 호스트의 SMTP 인증을 허용, 허용 안 함 또는 필요

TLS 및 SMTP 인증이 모두 활성화된 경우:SMTP 인증을 제공하기 위해 TLS 필요

도메인 키/DKIM 서명:이 리스너에서 도메인 키 또는 DKIM 서명 사용

DKIM 확인:DKIM 확인을 활성화합니다.

S/MIME 암호 해독/확인:S/MIME 암호 해독 또는 확인을 활성화합니다.

처리 후 서명:S/MIME 확인 후 메시지에서 디지털 서명을 유지할지 또는 제거할지를 선택합니다.

S/MIME 공개 키 수집:S/MIME 공개 키 수집을 활성화합니다.

확인 실패 시 인증서 수집:서명된 수신 메시지의 확인이 실패할 경우 공개 키를 수집할지 여부를 선택합니다.

업데이트된 인증서 저장:업데이트된 공개 키 수집 여부 선택

SPF/SIDF 확인: 이 리스너에서 SPF/SIDF 서명을 활성화합니다.

적합성 수준:SPF/SIDF 적합성 레벨을 설정합니다.SPF, SIDF 또는 SIDF Compatible 중에서 선택할 수 있습니다.

'Resent-Sender:' 또는 'Resent-From:'이 사용된 경우 다운그레이드 PRA 확인 결과:SIDF 호환 가능 레벨을 선택하는 경우 PRA ID 확인 결과 전달(Resent-Sender가 있는 경우)을 None(없음)으로 다운그레이드할지 여부를 구성합니다.또는 재전송:메시지에 있는 헤더

HELO 테스트:HELO ID에 대해 테스트를 수행할지 여부를 구성합니다(SPF 및 SIDF 호환 적합성 레벨에 사용).

DMARC 확인:이 리스너에서 DMARC 확인 사용

DMARC 확인 프로필 사용:이 리스너에서 사용할 DMARC 확인 프로필을 선택합니다.메일 정책 —> DMARC —> 프로파일 추가에서 동일한 항목이 생성됩니다.

DMARC 피드백 보고서:DMARC 집계 피드백 보고서 전송을 활성화합니다.

바운스 확인

태그 없는 반송을 유효한 것으로 고려:반송 확인 태깅이 활성화된 경우에만 적용됩니다.기본적으로 어플라이언스는 Bounce Verification(바운스 확인) 설정에 따라 태그되지 않은 반송이 유효하지 않은 것으로 간주하며 반송 또는 사용자 지정 헤더를 추가합니다.태그되지 않은 반송을 유효하게 고려하도록 선택하면 어플라이언스는 반송 메시지를 수락합니다.

발신자 확인

봉투 발신자 DNS 확인:

발신자는 다양한 이유로 확인되지 않을 수 있습니다.확인되지 않은 발신자는 다음 범주로 분류됩니다.

- 연결 호스트 PTR 레코드가 DNS에 없습니다.
- 연결 호스트 PTR 레코드 조회가 임시 DNS 실패로 인해 실패했습니다.
- 연결 호스트 역방향 DNS 조회(PTR)가 정방향 DNS 조회(A)와 일치하지 않습니다.

Sender Verification 기능을 활성화하거나 비활성화할 수 있습니다.

발신자 확인 예외 테이블 사용: Sender Verification 도메인 예외 테이블을 사용하여 예외를 허용할 수 있습니다.예외 테이블은 하나만 가질 수 있지만 메일 플로우 정책당 활성화할 수 있습니다.

예외 테이블은 메일 정책 —> 발송인 확인 예외 테이블 —> 발송인 확인 예외 추가

대상 제어

이는 이메일 전송을 제어하는 기능입니다.ESA를 통해 처리를 완료하고 향후 전송을 위해 ESA를 종료하려고 하는 모든 이메일은 Destination Controls 기능을 통해 제어할 수 있습니다.

기본 **대상** 제어 프로파일은 모든 납품에 적용됩니다.경우에 따라 도메인별 전달 제어가 필요한 경우 맞춤형 대상 제어 프로필을 생성해야 합니다.

대상 제어 프로필의 구성 요소

제한

동시 연결 수:어플라이언스가 전송을 완료하기 위해 열려고 시도하는 원격 호스트에 대한 동시 연결(DCID) 수입니다.

연결당 최대 메시지 수:어플라이언스가 새 연결을 시작하기 전에 ESA가 DCID(Connection)를 통해 대상 도메인으로 전송할 메시지 수입니다.

수신자:지정된 기간 동안 어플라이언스가 지정된 원격 호스트로 전송할 수신자 수

제한 적용:이러한 측면은 대상별 및 MGA 호스트 이름별로 지정된 제한을 적용하는 방법을 결정하는 데 도움이 됩니다.

TLS 지원

이렇게 하면 원격 호스트에 대한 TLS 연결을 None/Preferred/Required로 설정할지 여부를 결정할 수 있습니다.

DANE 지원:DANE를 '기회주의적'으로 구성하고 원격 호스트가 DANE를 지원하지 않는 경우, SMTP 대화를 암호화하는 데 기회주의적 TLS를 사용하는 것이 좋습니다.

DANE를 'Mandatory(필수)'로 구성하고 원격 호스트가 DANE를 지원하지 않는 경우 대상 호스트에 대한 연결이 설정되지 않습니다.

DANE를 'Mandatory' 또는 'Opportunistic'으로 구성하고 원격 호스트가 DANE를 지원하는 경우 SMTP 대화를 암호화하는 것이 좋습니다.

참고:SMTP 경로가 구성된 도메인에는 DANE가 적용되지 않습니다.

바운스 확인

이를 통해 바운스 확인을 통해 봉투 발신자 주소 태깅(prvs-xxxxxx-xxxx)을 수행할지 여부를 결정할 수 있습니다.

바운스 확인은 메일 정책 —> 바운스 확인 —> 새 키 추가를 통해 구성할 수 있습니다.

바운스 프로파일

반송 프로파일은 지정된 원격 호스트에 대해 어플라이언스에서 사용할 수 있습니다.이메일의 하드 바운스 전에 ESA의 Delivery Queue에서 전송 문제가 있을 경우 해당 이메일을 얼마나 오래 보관할 것인지 결정합니다.

바운스 프로파일은 네트워크 —> 바운스 프로파일을 통해 설정됩니다.

전역 설정

인증서:이는 SSL/TLS 연결을 설정하는 동안 다음 홉으로 이메일 전송을 시작할 때 사용할 인증서를 정의하는 부분입니다.이러한 측면에서 CA(Certificate Authority) 서명 인증서를 사용하는 것이 좋습니다.

필수 TLS 연결이 실패할 경우 알림 전송: TLS 연결이 필요한 도메인에 메시지를 전달할 때 TLS 협상이 실패할 경우 어플라이언스가 알림을 전송할지 여부를 지정할 수 있습니다.경고 메시지에는 실패한 TLS 협상에 대한 대상 도메인의 이름이 포함됩니다.어플라이언스는 **시스템 경고** 유형에 대한 **경고** 심각도 레벨 알림을 수신하도록 설정된 모든 수신자에게 경고 메시지를 전송합니다.

System Administration(시스템 관리) —> Alerts(경고)를 통해 경고 수신자를 관리할 수 있습니다.