ESA DHAP 기능 지원

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 DHAP(Directory Harvest Attack Prevention) 기능을 활성화하여 DHA(Directory Harvest Attack)를 방지하는 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA
- 비동기OS

사용되는 구성 요소

이 문서의 정보는 모든 AsyncOS 버전을 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

DHA는 유효한 이메일 주소를 찾기 위해 스패머가 사용하는 기술입니다. DHA가 대상으로 하는 주소를 생성하기 위해 두 가지 주요 기술이 사용됩니다.

- 스패머는 가능한 모든 문자와 숫자 조합의 목록을 만든 다음 도메인 이름을 추가합니다.
- 스팸 발송자는 일반적인 이름, 성, 이니셜을 결합한 목록을 만드는 데 표준 사전 공격을 사용합니다.

DHAP는 LDAP(Lightweight Directory Access Protocol) 수락 검증이 사용될 때 활성화할 수 있는 Cisco Content Security Appliance에서 지원되는 기능입니다. DHAP 기능은 지정된 발신자의 잘못된 수신자 주소 수를 추적합니다.

발신자가 관리자 정의 임계값을 넘으면 발신자를 신뢰할 수 없는 것으로 간주하며, 해당 발신자의 메일은 NDR(Network Design Requirement) 또는 오류 코드 생성 없이 차단됩니다. 발신자의 평판을 기반으로 임계값을 구성할 수 있습니다. 예를 들어, 신뢰할 수 없거나 의심스러운 발신자는 DHAP 임계값이 낮을 수 있으며, 신뢰할 수 있거나 신뢰할 수 있는 발신자는 DHAP 임계값이 높을 수 있습니다.

DHAP 활성화

DHAP 기능을 활성화하려면 Content Security Appliance GUI에서 **Mail Policies(메일 정책) > Host Access Table (HAT)(호스트 액세스 테이블(HAT))**로 이동하고 **Mail Flow Policies(메일 플로우 정책)를 선택합니다**. Policy Name(정책 이름) 열에서 수정할 **정책을** 선택합니다.

HAT에는 원격 호스트로부터의 연결에 대해 작동하는 데 사용되는 4개의 기본 액세스 규칙이 있습니다.

- **수락**: 연결이 수락되고 리스너 설정에 의해 이메일 수락이 추가로 제한됩니다. 여기에는 수신인 테이블(퍼블릭 리스너용)이 포함됩니다.
- **거부**: 처음에는 연결이 허용되지만 연결을 시도하는 클라이언트에서는 4XX 또는 5XX 인사말이 수신됩니다. 수락된 이메일이 없습니다.
- **TCPREFUSE**: TCP 레벨에서 연결이 거부됩니다.
- **릴레이**: 연결이 수락됩니다. 수신자에 대한 수신은 허용되며 Recipient Access Table에 의해 제한되지 않습니다. 도메인 키 서명은 릴레이 메일 플로우 정책에서만 사용할 수 있습니다.

선택한 **정책**의 **Mail Flow Limits(메일 플로우 제한)** 섹션에서 Max(최대)를 설정하여 **DHAP(Directory Harvest Attack Prevention) 컨피그레이션을** 찾아 설정합니다. 시간당 올바르지 않은 수신인 수 Max를 사용자 지정할 수도 있습니다. 시간당 올바르지 않은 수신인 코드 및 최대 원하는 경우 시간당 올바르지 않은 수신인 텍스트

추가 정책에 대해 DHAP를 구성하려면 이 섹션을 반복해야 합니다.

GUI에서 모든 변경 사항을 제출하고 커밋해야 합니다.

> **참고:** Cisco에서는 **원격 호스트** 설정**에서 시간당** 유효하지 않은 최대 수신자 수**에** 5~10**의 최대 수를 사용하는 것을** 권장합니다.

> **참고:** 자세한 내용은 Cisco 지원 **포털**에서 **AsyncOS 사용** 설명서를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.