ESA NDR(Bounce a Bounce) 스톰 경험

목차

[소개](#)
[배경 정보](#)
[조 작업](#)
[백산포](#)
[문제](#)
[솔루션](#)
[바운스 확인](#)
[바운스 확인 주소 태깅 키 구성](#)
[키 제거](#)
[Cisco 바운스 확인 설정 구성](#)
[CLI로 Cisco Bounce Verification 구성](#)
[Cisco 바운스 확인 및 클러스터 구성](#)
[메일 필터](#)
[메일 블록](#)

소개

이 문서에서는 ESA(Email Security Appliance)에서 바운스 스톰을 경험하고 문제에 대한 해결책을 제시하는 문제에 대해 설명합니다.

배경 정보

바운스 스톰은 joe 작업 또는 이메일 스팸의 백분산이라는 부작용입니다.

조 작업

Joe 작업은 스푸핑된 발신자 데이터를 사용하며, 발신자의 평판을 손상시키거나 수신자에게 명확한 발신자에 대한 조치를 취하도록 유도하는 스팸 공격입니다.

백산포

백산지는 스팸 및 기타 메일을 수신하는 이메일 서버가 무해한 당사자에게 반송 메시지를 전송하는 이메일 스팸, 바이러스 및 지렁이의 부작용입니다.이는 피해자의 이메일 주소를 포함하기 위해 원본 메시지 봉투 발신자가 위조되기 때문입니다.이러한 메시지는 수신자가 요청하지 않았으며 서로 상당히 유사하며 대량 양을 제공하므로 원치 않는 대량 이메일 또는 스팸으로 간주됩니다.따라서 이메일 백분산기를 생성하는 시스템은 다양한 DNSBL(Domain Name System Blacklists)에 나열될 수 있으며 인터넷 서비스 제공업체 서비스 약관을 위반할 수 있습니다.

문제

ESA에서 ESA에 삽입된 메시지가 폭증하는 경우 ESA에 반송 폭풍이 발생합니다.이러한 공격 중

수신 연결 수가 급증합니다.어플라이언스에서 작업 대기열 백업을 개발할 수 있습니다.어플라이언스가 이러한 공격의 대상인지 확인하려면 메일 **발신** 주소에 대한 메일 로그**를** 작성합니다.바운스(배달 못 함 보고서 - NDR)에 빈 봉투 메일 보낸 사람 주소**가** 있습니다.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

바운스 스톰이 적용되는 어플라이언스에는 봉투 메일**의** From 주소가 '**<>**'인 대부분의 메시지가 포함됩니다.

솔루션

바운스 스톰을 관리할 수 있는 다양한 옵션이 있습니다.

바운스 확인

이러한 잘못 전달된 반송 공격을 방지하기 위해 AsyncOS에는 Cisco Bounce Verification이 포함됩니다. 이 기능을 활성화하면 ESA를 통해 전송되는 메시지에 대해 봉투 발신자 주소에 태그를 지정합니다.그러면 ESA에서 수신한 바운스 메시지에 대한 Envelope Recipient(봉투 수신자)가 이 태그가 있는지 확인합니다.합법적인 반송 메시지가 수신되면 Envelope Sender 주소에 추가된 태그가 제거되고 반송 메시지가 수신자에게 전달됩니다.태그가 없는 바운스 메시지는 별도로 처리할 수 있습니다.

AsyncOS는 반송을 null 메일 보낸 사람 주소(<>)가 있는 메일**로** 간주합니다. mailer-daemon@example.com 또는 postmaster@example.com과 같은 주소에서 보낸 메시지는 시스템에서 반송 확인으로 간주되지 않으며 반송 확인이 적용되지 않습니다.

바운스 확인 주소 태깅 키 구성

Bounce Verification Address Tagging Keys(바운스 확인 주소 태깅 키) 목록에는 이전에 사용한 현재 키와 삭제되지 않은 키가 표시됩니다.새 키를 추가하려면 다음 단계를 완료하십시오.

1. 의 **메일 정책 > 바운스 확인** 페이지에서 **새 키**를 클릭합니다.
2. 텍스트 문자열을 입력하고 **제출**.
3. 변경 사항을 커밋합니다.

키 제거

풀다운 메뉴에서 제거할 규칙을 선택하고 Purge(제거)를 클릭하면 이전 주소 태그 키를 제거할 수 **있습니다.**

Cisco 바운스 확인 설정 구성

바운스 확인 설정은 잘못된 반송 수신 시 수행할 작업을 결정합니다.

- 선택 **메일 정책 > 바운스 확인**.

- 클릭 **설정 편집**.
- 잘못된 바운스를 거부할지 아니면 메시지에 사용자 지정 헤더를 추가할지를 선택합니다.헤더를 추가하려면 헤더 이름과 값을 입력합니다.
- 선택적으로, 스마트 예외를 활성화합니다.이 설정을 사용하면 내부 메일 서버에서 생성된 수신 메일 메시지 및 바운스 메시지가 바운스 확인 처리(수신 및 발신 메일 모두에 단일 리스너를 사용하는 경우에도)에서 자동으로 제외됩니다.
- 변경 사항을 제출하고 커밋합니다.

CLI로 Cisco Bounce Verification 구성

CLI에서 **bvconfig** 및 **destconfig** 명령을 사용하여 바운스 확인을 구성할 수 있습니다.이러한 명령은 Cisco AsyncOS CLI 참조 설명서에서 설명합니다.

Cisco 바운스 확인 및 클러스터 구성

바운스 확인은 두 Cisco 어플라이언스가 동일한 "바운스 키"를 사용하는 한 클러스터 컨피그레이션에서 작동합니다. 동일한 키를 사용할 경우, 두 시스템 중 어느 것이든 합법적인 반송을 수락할 수 있어야 합니다.수정된 헤더 태그/키는 각 Cisco 어플라이언스에 한정되지 않습니다.

메일 필터

수신 및 전달에 별도의 어플라이언스를 사용하기 때문에 바운스 확인을 사용할 수 없는 경우, 메시지 필터를 설정하여 빈 메일 수신 주소가 있는 메시지를 차단할 수 **있습니다**.

메일 블록

이러한 바운스 메시지는 존재하지 않는 봉투 수신자 주소가 있을 가능성이 높으므로, 이러한 메시지의 영향을 줄이기 위해 대화의 LDAP(Lightweight Directory Access Protocol) 수신자 검증을 통해 잘못된 주소를 차단할 수 있습니다.