

# 스푸핑을 방지하기 위한 ESA SMTP 인증 조건

## 목차

[소개](#)

[사전 요구 사항](#)

[배경 정보](#)

[필터 만들기](#)

[규칙 예](#)

[관련 정보](#)

## 소개

이 문서에서는 SMTP(Simple Mail Transfer Protocol) 인증 사용자를 기반으로 필터를 생성하고 사용자 이름을 X-헤더에 기록하는 방법에 대해 설명합니다.

## 사전 요구 사항

AsyncOS 버전 6.5 이상에 대해 알고 있는 것이 좋습니다.

## 배경 정보

SMTP 인증 기능을 사용하면 ESA(Email Security Appliance)에 연결하고 메일을 보내기 위해 클라이언트에 대해 SMTP 인증을 사용할 수 있습니다. 이 기능을 통해 인증된 사용자는 릴레이할 수 있으므로 사용자는 Cisco ESA를 통해 전송되는 이메일에서 "From:" 필드를 위조할 수 있습니다. 사용자가 위조하지 못하도록 하기 위해 ESA AsyncOS 버전 6.5 이상에는 인증된 SMTP 사용자 이름 및 메일 보낸 사람 이메일 주소에 대한 비교를 허용하는 메시지 필터 조건이 포함됩니다.

## 필터 만들기

메시지 필터 조건을 사용하면 관리자는 SMTP 인증 세션을 통해 아웃바운드 릴레이된 이메일을 비교하는 다음 섹션의 예제 규칙과 유사한 필터를 작성할 수 있습니다. SMTP 자격 증명이 손상된 경우 이메일을 보내는 시스템은 일반적으로 다음과 같이 메일로 사용할 여러 주소를 생성합니다. 헤더. 메시지 필터 조건은 사용자 이름 및 메일이 보낸 사람:헤더 일치 그렇지 않으면 이메일은 위조된 메일 보낸 사람:으로 간주되며 메시지 필터 작업이 활성화됩니다. 메시지 필터 작업은 최종 작업이 될 수 있습니다. 예제 규칙은 격리 작업을 보여줍니다. 필터 조건의 구문은 다음과 같습니다.

```
smtp-auth-id-matches("<target>" [, "<sieve-char>"])
```

필터는 다음 대상 중 하나에 대한 비교를 허용합니다.

- **봉투 보낸 사람:** 메일 보낸 사람:SMTP 대화에서 확인할 수 있습니다
- **보낸 사람 주소:** 다음에서 구문 분석된 주소를 **비교합니다.**헤더.보낸 사람:헤더. 하나만 일치해야 합니다.
- **보낸 사람:** 발신자에 지정된 주소를 **비교합니다.**헤더.
- **모두:** 인증된 SMTP 세션 중에 생성된 메시지(ID와 상관없이)와 일치시킵니다.
- **None:** 인증된 SMTP 세션 동안 생성되지 않은 메시지(예: SMTP 인증이 **선택되는** 경우)와 일치시킵니다.

SMTP 인증 ID	SIEVE 문자 비교 주소	일치 여부
사용자	otheruser@example.com	아니요
사용자	someuser@example.com	예
사용자	someuser@face.localhost	예
일부 사용자	someuser@example.com	예
사용자	someuser+folder@example.com	아니요
사용자	+ someuser+folder@example.com	예
someUser@example.com	someuser@forged.com	아니요
someUser@example.com	someuser@example.com	예
someUser@example.com	someuser@example.com	예

이 변수 대체 **\$SMTPAuthID**는 릴레이에 사용된 원래 인증 자격 증명의 헤더에 포함할 수 있도록 생성되었습니다.

## 규칙 예

```
Msg_Authentication: if (smtp-auth-id-matches("*Any"))
{
  # Always include the original authentication credentials in a
  # special header.
  insert-header("X-SMTPAUTH", "$SMTPAuthID");

  if (smtp-auth-id-matches("*FromAddress", "+") and
      smtp-auth-id-matches("*EnvelopeFrom", "+"))
  {
    # Username matches. Verify the domain
    if (header('from') != "(?i)@(?::example\.com|example\.com)" or mail-from !=
"(?i)@(?::example\.com|\.com)"
    {
      # User has specified a domain which cannot be authenticated
      quarantine("forged");
    }
  } else {
    # User claims to be an completely different user
    quarantine("forged");
  }
}
```

**참고:** 이 필터는 위조된 격리가 있다고 가정합니다.

## 관련 정보

- [IronPort AsyncOS Advanced User Guide for IronPort Email Security Appliances](#)
- [기술 지원 및 문서 - Cisco Systems](#)