Configure ESA SMTP Authentication Matching to Prevent From Address Spoofing

Contents

- Introduction
- Prerequisites
- Background Information
- Create a Filter
    - Example Rule
- Related Information

Introduction

This document describes how to create a message filter that compares the SMTP authenticated username to the header **From:** address.

Prerequisites

Cisco recommends that you have knowledge of Cisco AsyncOS for Email version 15.0 and later.

Background Information

The SMTP authentication function allows customers to use SMTP authentication for their email clients to connect to and send mail through the Cisco Email Security Appliance (ESA). Because the feature allows an authenticated session to relay outbound mail, a client can spoof the header **From:** address. To help prevent spoofing, Cisco AsyncOS for Email version 6.5 and later includes a message filter condition that compares the authenticated SMTP username to the header **From:** address and logs the username in an X-header.

Create a Filter

The message filter condition allows an administrator to write a filter (for example, the rule in the next section) that compares messages relayed outbound during an SMTP authenticated session. If SMTP credentials are compromised, the sending client often generates multiple header **From:** addresses. This condition allows messages to be delivered only when the authenticated username matches the header **From:** address; otherwise, the message is treated as a spoofed header **From:** and the configured message filter action is applied. The message filter action can be any final action; the example rule uses a quarantine action. The filter condition has this syntax:

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

The optional **sieve-char** parameter specifies a delimiter character (for example, +) used to ignore the portion of the comparison address after that character. This is commonly used for plus-addressing, as shown in the table.

The filter permits a comparison against one of these targets:

- **EnvelopeFrom:** Compares the address specified in **Mail From:** in the SMTP conversation.
- **FromAddress:** Compares addresses parsed out of the **From:** header. Since multiple addresses are permitted in the **From:** header, only one must match.
- **Sender:** Compares the address specified in the **Sender:** header.
- **Any:** Matches messages that were created during an authenticated SMTP session (regardless of the identity).
- **None:** Matches messages that were not created during an authenticated SMTP session (for example, when SMTP authentication is preferred).

SMTP AUTH ID	SIEVE CHAR	COMPARISON ADDRESS	MATCHES?
someuser		otheruser@example.com	No
someuser		someuser@example.com	Yes
someuser		someuser@face.localhost	Yes
SomeUser		someuser@example.com	Yes
someuser		someuser+folder@example.com	No
someuser	+	someuser+folder@example.com	Yes
someUser@example.com		someuser@forged.com	No
someUser@example.com		someuser@example.com	Yes
someUser@example.com		someuser@example.com	Yes

This variable substitution, **$SMTPAuthID**, allows inclusion of the authenticated username in message headers for messages relayed during an authenticated SMTP session.

Example Rule

```
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" or mail-from != "(?i)@example\.com")
        {
            # User has specified a domain which cannot be authenticated.
            quarantine("forged");
        }
```

```
    }
    else
    {
        # User claims to be a completely different user.
        quarantine("forged");
    }
}
```

Note: This filter assumes a quarantine named **forged** exists.

Related Information

- **Cisco AsyncOS Advanced User Guide for Cisco Email Security Appliances**
- **Technical Support & Documentation - Cisco Systems**