Filter to handle messages that skipped DMARC verification

Contents

[Introduction](#)
[Requirements](#)
[Prerequistes](#)
[Background Information](#)
[Workaround Filter](#)
[Related Information](#)

Introduction

This document describes how to create a filter to action emails which skipped Domain-based Message Authentication, Reporting And Conformance (DMARC) verification in the Email Security Appliance (ESA) and Cloud Email Security (CES).

Requirements

Prerequistes

- AsyncOS 11.1.2 and onwards.
- Understanding of DMARC. (https://tools.ietf.org/html/rfc7489#page-56)
- ESA/CES with DMARC verification enabled.

Background Information

ESA/CES with DMARC verification configured on the mail flow policies, where message tracking/mail_logs are yielding the log line: **DMARC: Verification skipped (Sending domain could not be determined)**".

This log line means that ESA/CES has detected more than one domain identity in the from header and when there are more than one email address in the header, this header will be skipped in most DMARC implementations.Processing headers with more than one domain identity are exposed as out-of-scope in the DMARC specification.

Workaround Filter

Cisco AsyncOS 11.1.2 version and the subsequent releases adds a new feature where the device will include a new x-header that captures different DMARC verification results with a unique value based on the DMARC verification result.

There are four header values that available to filter- validskip, invalidskip, temperror and

permerror.

> **Note**: For the cases where DMARC verification could not be performed because there were special characters or the from headers are malformed or DMARC check failed because of some other non-conformity valid skip or invalid skip, the x-header added will be: **X-Ironport-Dmarc-Check-Result:** invalidskip or validskip.

> **Note**: This filter can be deployed on both the Message filters (CLI restricted) and the Content filters.

Header values:

- **Valid skip** covers the cases where the DMARC verification could not be performed when there is a from header or no DMARC record.
- **Invalid skip** covers the cases where there are invalid characters in the from header, multiple from headers, multiple domain entities in the from header, the sender address has non-US-ASCII characters and if there is an error in parsing values in the from header field.
- **Permerror** covers cases when a permanent error occurred during DMARC evaluation, such as encountering a syntactically incorrect DMARC record. A later attempt is unlikely to produce a final result.
- **Temperror** will cover cases when temporary error occurred during DMARC evaluation.A later attempt might produce a final result.

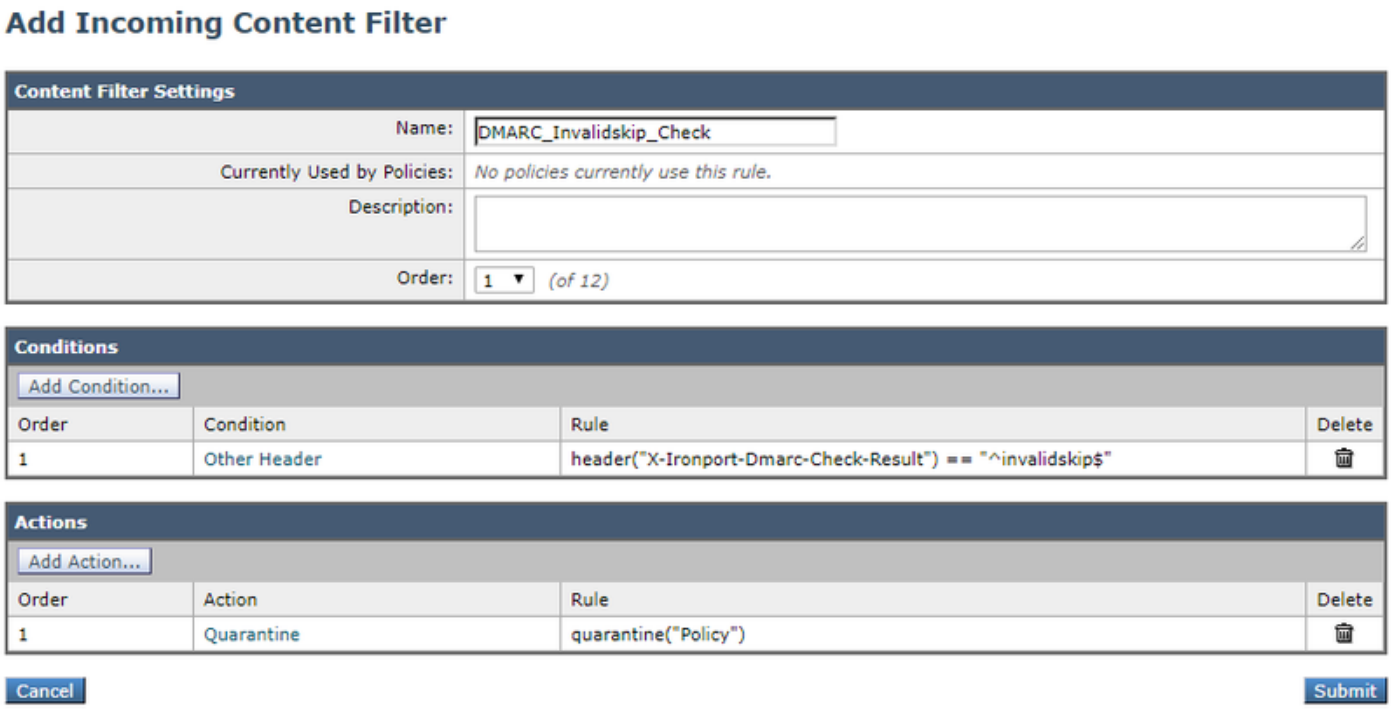
The following is the DMARC filter that checks the **"X-Ironport-Dmarc-Check-Result"** for an **invalidskip** and proceeds to quarantine it.

The action can be customized to other requirements where needed.

Message Filter

```
Quarantine_messages_DMARC_skip:
if header("X-Ironport-Dmarc-Check-Result") == "^invalidskip$"
{
quarantine("Policy");
}
```

Content Filter



Related Information

- [Cisco Email Security Appliance - End-User Guides]
- [Technical Support & Documentation - Cisco Systems]
- [What is DMARC?]