Why is the ESA handling DKIM authentication result permfail as hardfail?

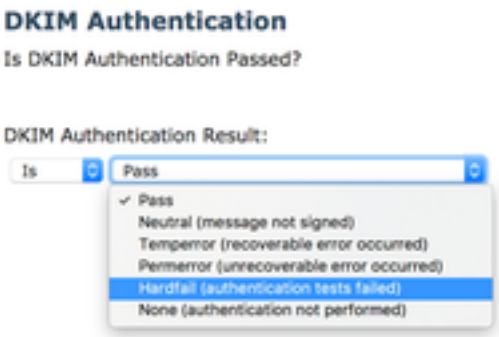
Contents

Introduction

This document describes details about DKIM authentication results handling on the Email Security Appliance (ESA).

Why is the ESA handling DKIM authentication result permfail as hardfail?

The ESA content filter condition DKIM Authentication has several options availabe as the image below is highlighting.



If the condition DKIM Authentication Result is configured to match on Hardfail it will include messages that show up as permfail in the mail log file and message tracking as shown in the example below:

```
Message 815204 DKIM: permfail body hash did not verify [final] (d=sub.example.com s=selector1-sub-com i=@sub.example.com)
```

The ESA considers permfail as hardfail and puts the result into the Authentication-Results header as dkim=hardfail. There is a difference between ESA's naming of DKIM events and RFC6376 naming. In Authentication-Results headers (and message tracking) ESA needs to show proper RFC6376 strings, while the content filter uses different event names.

The event mapping for RFC6376.PERMFAIL == ESA Content Filter Hardfail

The majority of verification failures are due to signature and message body hash verification failures. Body hash verification errors indicate that the body of the message does not agree with the hash (digest) value in the signature. Signature verification errors indicate that the signature

value does not correctly verify the signed header fields (including the signature itself) on the message. There are several causes for these two errors: the message may have been modified (perhaps by a mailing list or forwarder) in transit; the signature or hash values may have been calculated or applied incorrectly by the signer; the wrong public key value may have been published in DNS; or the message may have been spoofed by an entity not in possession of the private key needed to calculate a correct signature. It is very hard to distinguish these causes by analysis of the message, although the origin IP address may provide some helpful forensics in the case of spoofing. However, for privacy reasons we don't have access to the messages themselves, so any such analysis isn't possible. There is a number of messages whose signatures don't verify for other reasons, often because of easily avoided configuration errors in the public key (selector) records published in DNS. For more details please refer to the link below.

Related Information

- **Common Errors Causing DKIM Verification Failures**