Почему ESA обрабатывает результат аутентификации DKIM permfail как hardfail?

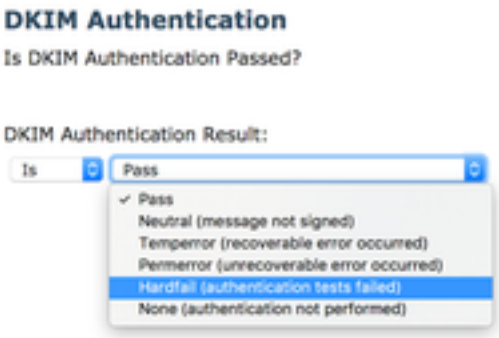
Содержание

Введение

Этот документ описывает подробные данные об обработке результатов аутентификации DKIM на Email Security Appliance (ESA).

Почему ESA обрабатывает результат аутентификации DKIM permfail как hardfail?

Условие фильтра контента ESA Аутентификация DKIM имеет несколько опций availabe как образ ниже, выделяет.



Если условие Результат аутентификации DKIM настроен к соответствие на Hardfail, это будет включать сообщения, которые обнаруживаются как permfail в почтовом файле журнала и отслеживании сообщений как показано в примере ниже:

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

ESA рассматривает permfail как hardfail и помещает результат в заголовок Результатов аутентификации как dkim=hardfail. Существует различие между именованием ESA событий DKIM и именованием RFC6376. В то время как фильтр контента использует другие названия события, в заголовках Результатов аутентификации (и отслеживание сообщений) ESA должен показать надлежащие строки RFC6376.

Сопоставление события для RFC6376. PERMFAIL == Фильтр контента ESA Hardfail

Большинство сбоев проверки происходит из-за подписи и сбоев проверки хэша тела сообщения. Ошибки проверки хэша тела указывают, что тело сообщения не согласовывает

с хэшем (дайджест) значения в подписи. Ошибки проверки подписи указывают, что значение подписи правильно не проверяет поля заголовка со знаком (включая саму подпись) на сообщении. Существует несколько причин для этих двух ошибок: сообщение, возможно, модифицировалось (возможно, списком рассылки или средством передачи) в пути; подпись или значения хеш-функции, возможно, были вычислены или применены неправильно подписывающим лицом; неправильное значение с открытым ключом, возможно, было публиковано в DNS; или сообщение, возможно, имитировалось объектом не во владении секретным ключом, должен был вычислить корректную подпись. Очень трудно отличить эти причины анализом сообщения, невзирая на то, что IP-адрес происхождения может предоставить некоторую полезную судебную экспертизу в случае спуфинга. Однако по причинам конфиденциальности мы надеваем? t имеют доступ к самим сообщениям, таким образом, какой-либо такой анализ isn? t возможный. Существует много сообщений чей Дон подписей? t проверяют по другим причинам, часто из-за ошибок конфигурации, которых легко избегают, в (селекторных) записях с открытым ключом, публикованных в DNS. Для получения дополнительной информации см. ссылку ниже.

Дополнительные сведения

- Распространенные ошибки, причиняющие сбои проверки DKIM