Filtri dei contenuti ESA per messaggi e-mail con più allegati

Sommario

Introduzione

In questo documento viene descritto il funzionamento delle condizioni di filtro dei contenuti negativi per i messaggi e-mail che contengono più allegati su Cisco Email Security Appliance (ESA).

Problema

Si utilizza un filtro contenuti che consente determinati tipi di allegati di posta elettronica, mentre altri tipi di allegati devono essere contrassegnati per la quarantena. Quando arriva un messaggio di posta elettronica con più allegati, uno da consentire e un altro da contrassegnare per la quarantena, il filtro identifica l'intero messaggio come *consentito*.

Di seguito è riportato il filtro dei contenuti utilizzato:

```
if attachment filename != (list of attachments), then quarantine
```

Questa condizione e questa azione funzionano come previsto se il messaggio e-mail ha un unico allegato, ma non funzionano correttamente per i messaggi che contengono più allegati diversi.

Scenario di esempio

Di seguito sono riportati i tipi di allegati consentiti:

- **rar**
- **pdf**
- **jpg**

Tutti gli altri allegati devono essere inviati in quarantena, come specificato dalla condizione e dall'azione del filtro.

Condizione filtro

Di seguito è riportata la condizione di filtro utilizzata:

```
if attachment filename != (rar|pdf|jpg)
```

Operazione filtro

L'operazione filtro utilizzata è la seguente:

```
quarantine
```

In genere, se il messaggio di posta elettronica contiene un allegato **pdf** e un allegato **txt**, è consigliabile metterlo in quarantena perché l'allegato **txt** non è presente nell'elenco degli allegati consentiti. Tuttavia, questo filtro dei contenuti non funziona come previsto perché corrisponde all'allegato **pdf** nel messaggio e lo consente direttamente, anche se ha un allegato **txt**.

Soluzione

Non è possibile mettere in quarantena l'e-mail con l'allegato **del testo** per questi motivi:

- Le condizioni degli allegati sono valide per **tutti** gli allegati inclusi in un messaggio.
- Il confronto negativo **!=** verifica se **uno** degli allegati corrisponde.

Come descritto, se **uno** degli allegati è consentito, ad esempio se corrisponde a **!=**, l'intero messaggio viene considerato *consentito*. Non c'è modo di aggirare tutto questo; è semplicemente il modo in cui funzionano queste condizioni.

L'unica altra soluzione è invertire la logica e bloccare allegati specifici, non solo gli allegati che non sono presenti nella lista bianca.