Configurazione del filtro in ingresso in base alla verifica DKIM in ESA

Introduzione

In questo documento viene descritto come configurare Email Security Appliance (ESA) in modo da eseguire qualsiasi azione sulla verifica DKIM (Domain Keys Identified Email) tramite un filtro contenuti o messaggi in arrivo.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ESA
- Conoscenze base della configurazione del filtro contenuti
- Conoscenze base della configurazione dei filtri messaggi
- Centralizzazione delle conoscenze relative alla configurazione di regole, virus ed epidemie di quarantena

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1. Configurare la verifica DKIM

Verificare che la verifica DKIM sia abilitata. Selezionare **Mail Policies > Mail Flow Policies** (Policy di posta > Criteri flusso di posta).

Per configurare la verifica DKIM sull'ESA è simile alla verifica SPF. Nei **Parametri predefiniti** dei criteri di flusso della posta, è sufficiente attivare Verifica DKIM **su Attiva**.

Passaggio 2. Verifica dell'azione finale

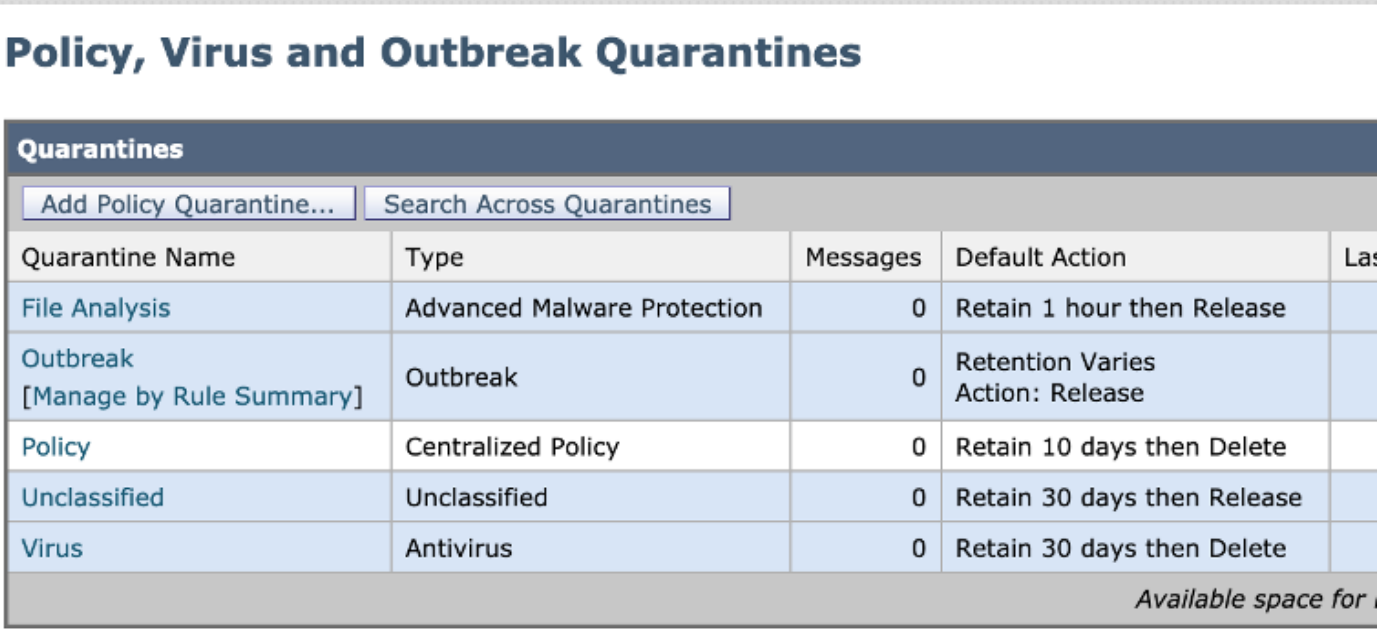
In primo luogo, indicare l’azione da intraprendere in relazione alla verifica DKIM. Esempio: al rilascio, aggiungere un tag o una quarantena. Se l'azione finale consiste nel mettere in quarantena la posta, esaminare le quarantene configurate.

- Se non si utilizza la gestione centralizzata:

Selezionare **ESA >Monitor> Policy, Virus and Outbreak Quarantines**.

- Se è stata configurata la gestione centralizzata (SMA):

Passare a **SMA >Email >Message Quarantine >Policy, Virus and Outbreak Quarantines**, come mostrato nell'immagine:

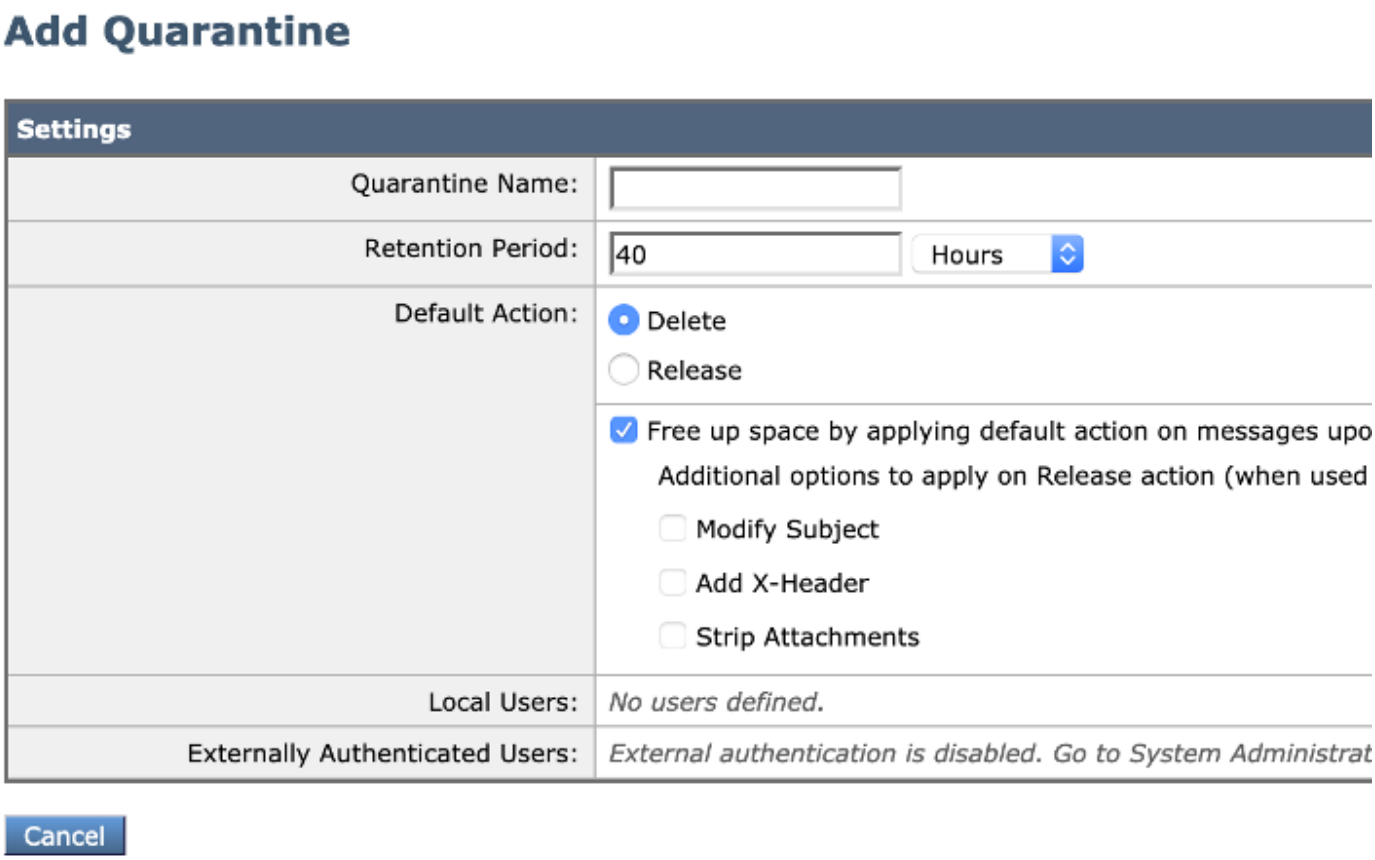


In assenza di quarantena specifica per i servizi **DKIM**/Domain-based Message Authentication, Reporting & Conformance (DMARC)/Sender Policy Framework (SPF). Si consiglia di crearne uno.

Durante la messa in quarantena di criteri, virus ed epidemie, selezionare **Add Policy Quarantine** (Aggiungi quarantena criteri):

Qui è possibile impostare:

- Nome quarantena: ad esempio **DkimQuarantine**
- Periodo di conservazione: Dipende dalle esigenze dell'organizzazione e dall'azione predefinita. Dopo il periodo di conservazione dell'e-mail verrà eliminato o rilasciato e consegnato, in base alla selezione effettuata, come mostrato nell'immagine:

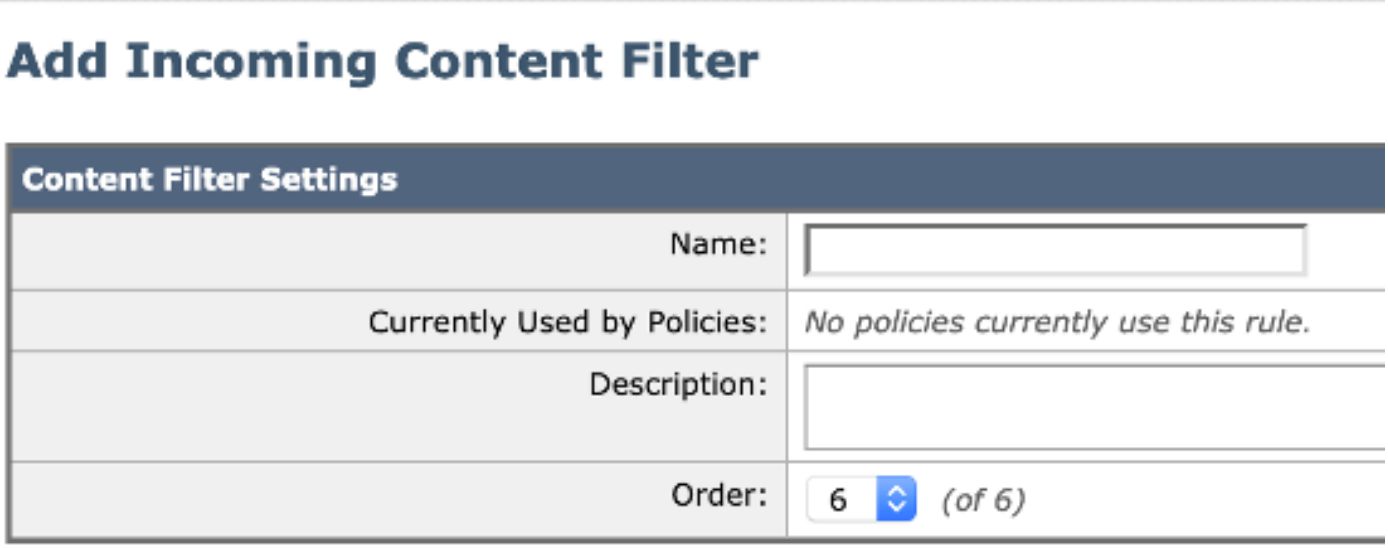


Passaggio 3. Filtro in ingresso per ESA

r. Creare un filtro dei contenuti in arrivo per ESA:

Selezionare **ESA > Mail Policies > Incoming Content Filters > Add Filter (Policy di posta > Filtri contenuti in arrivo > Aggiungi filtro).**

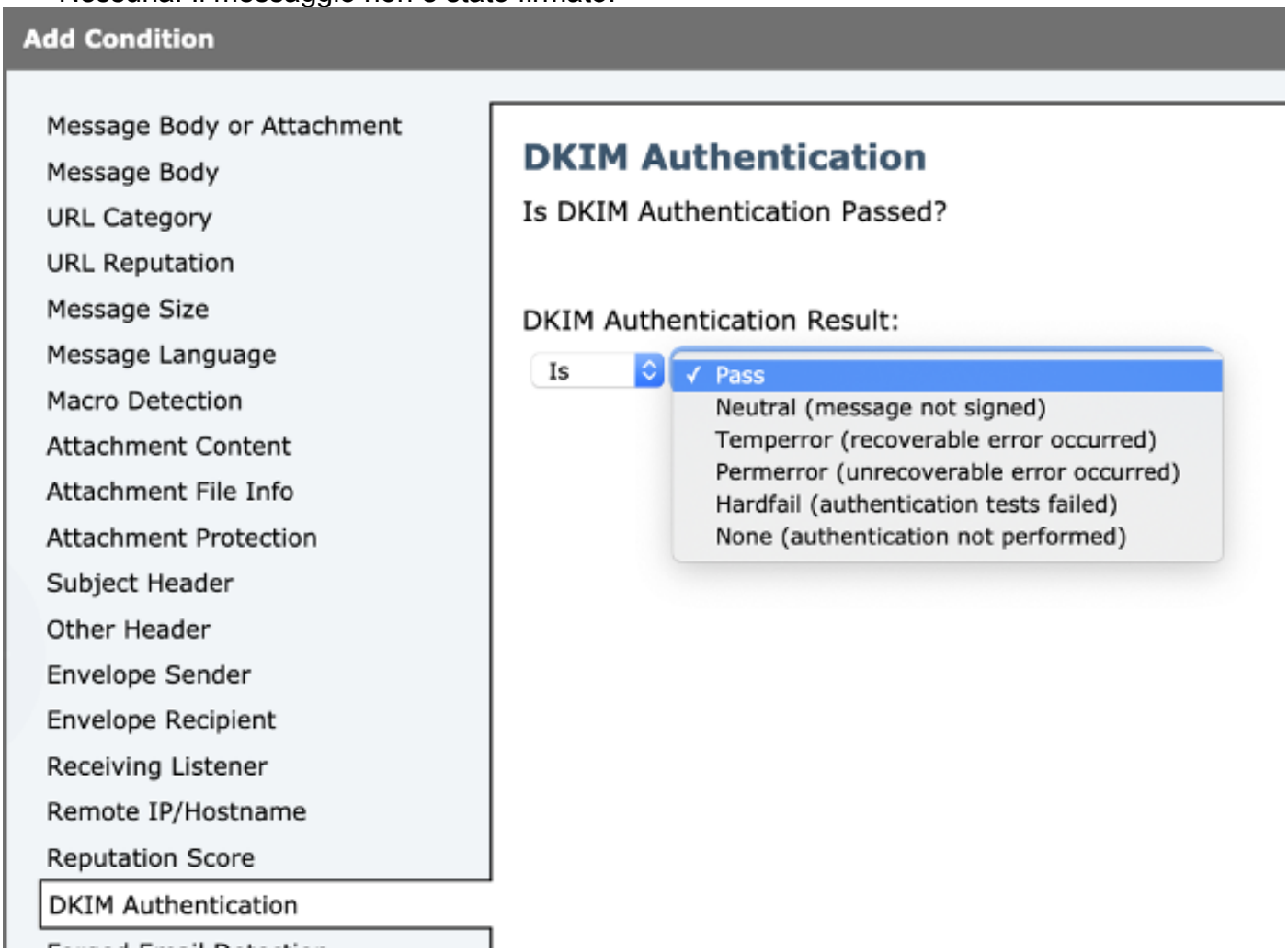
- Prima sezione: È possibile configurare il **Nome**, la **Descrizione** e l'**Ordine** del filtro:



- Seconda sezione: Aggiungi condizione. È possibile aggiungere più di una condizione ed è possibile configurare più filtri contenuti per eseguire azioni sulla verifica DKIM:

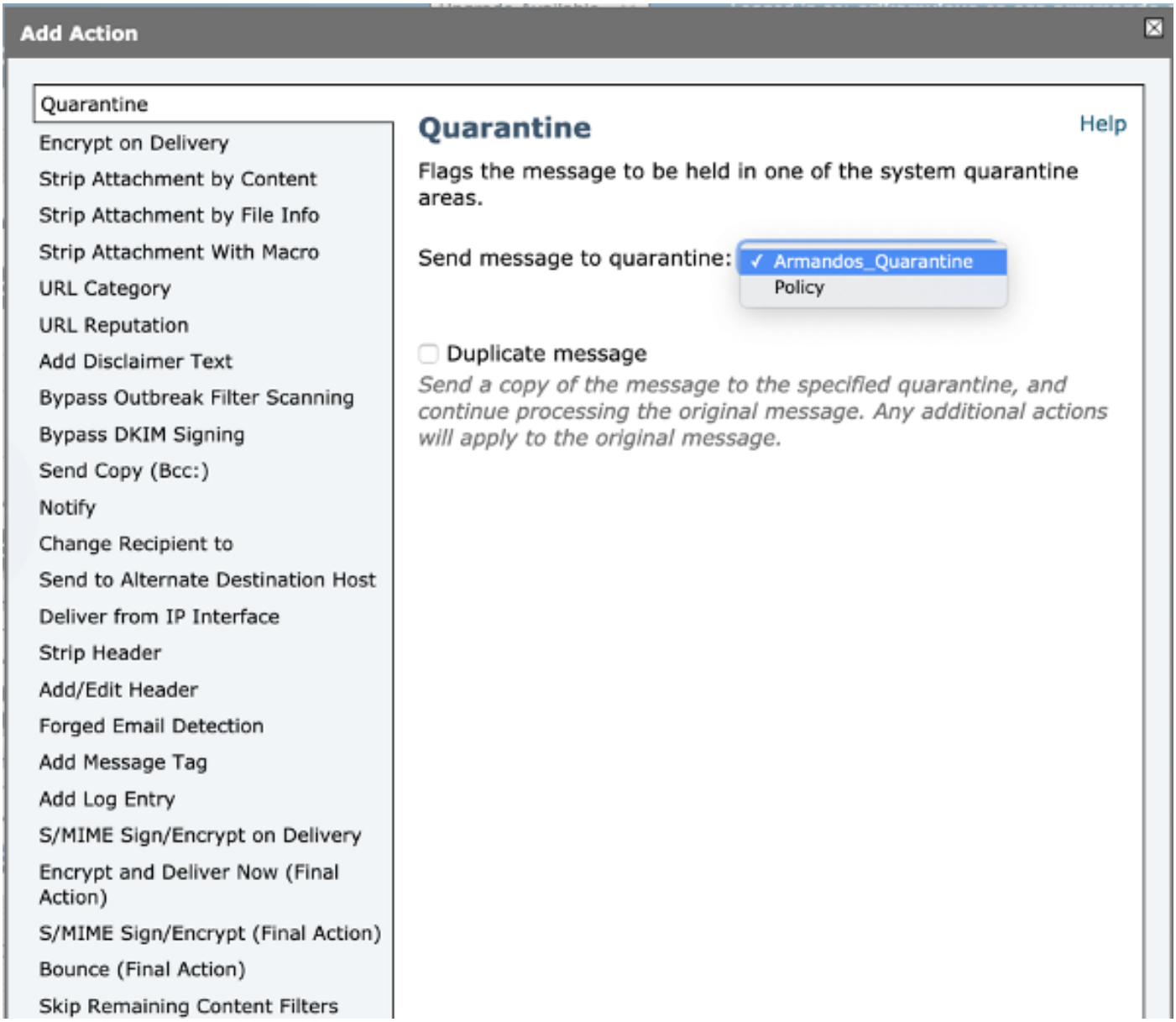
Risultati di autenticazione previsti e significato:

- Superato: Il messaggio ha superato i test di autenticazione.
- Neutro: Autenticazione non eseguita.
- Temperatura: Si è verificato un errore reversibile.
- Errore: Errore irreversibile.
- Errore hardware: Test di autenticazione non riusciti.
- Nessuna. Il messaggio non è stato firmato.



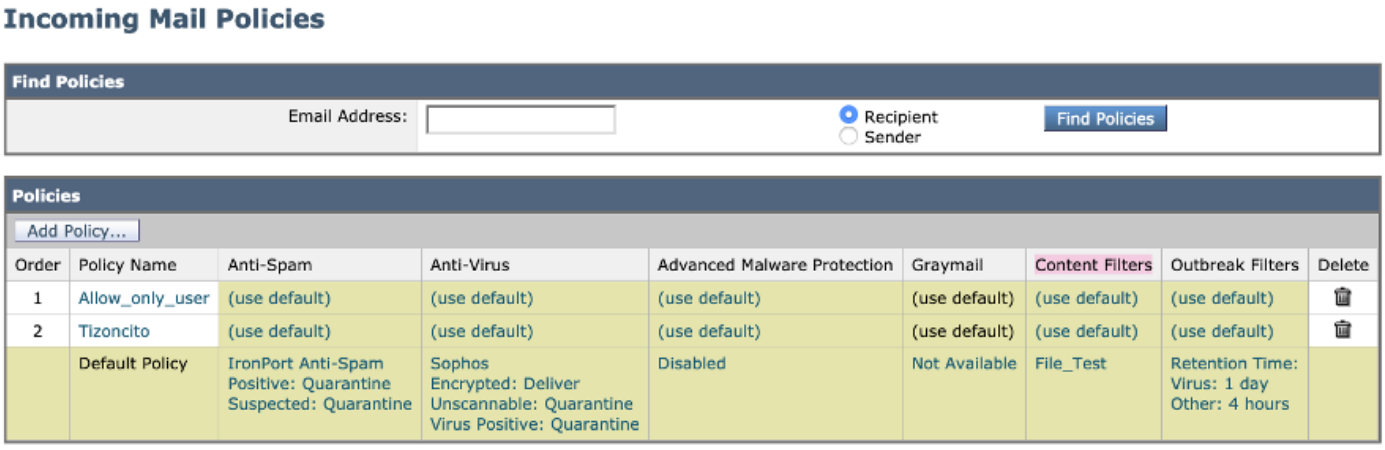
Nota: Requisiti per la verifica DKIM: Il mittente deve firmare il messaggio prima di poterlo verificare. Il dominio di invio deve avere una chiave pubblica disponibile nel DNS per la verifica.

- Terza sezione: Selezionare un'azione. È possibile aggiungere più di un'azione, ad esempio aggiungere una voce di registro, inviare in quarantena, eliminare l'e-mail, inviare una notifica e così via. In questo caso, selezionare la quarantena configurata in precedenza, come mostrato nell'immagine:



Aggiungi nuovo filtro al criterio flusso di posta:

Una volta creato un filtro. Da ESA aggiungere il filtro in ogni criterio del flusso di posta in cui si desidera verificare DKIM con un'azione finale. Selezionare **ESA> Mail Policies > Incoming Mail Policies** (Policy di posta **> Policy di posta in arrivo**), come mostrato nell'immagine:



Fare clic sulla colonna **Filtri contenuto** e sulla riga **dei criteri flusso di posta**.

Nota: (da utilizzare come impostazione predefinita) non significa che sia configurato come impostazioni predefinite dei criteri. Configurare ogni criterio del flusso di posta con i filtri necessari.

b. Creare un filtro messaggi per ESA:

Il filtro di tutti i messaggi è configurato dalla CLI ESA. Immettere il comando **Filtri** e seguire le istruzioni:

```
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW
Enter filter script.  Enter '.' on its own line to end.
DKIM_Filter:
If (dkim-authentication == "hardfail" )
{
quarantine("DkimQuarantine");
}
.
1 filters added.
```

Dopo aver creato il filtro, esaminare la legenda: **1 filtro aggiunto**.

Le condizioni e le azioni da configurare sono le stesse utilizzate dal filtro dei contenuti in arrivo.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Filtro contenuti in arrivo:

- Dall'interfaccia utente Web ESA (WebUI)

r. Verificare se il filtro è configurato:

Selezionare **ESA > Mail Policies > Incoming Content Filters (Policy di posta > Filtri contenuti in arrivo).** Il filtro deve essere configurato in base all'ordine selezionato in precedenza nell'elenco visualizzato.

b. Verificare se il filtro è applicato:

Selezionare **ESA>Mail Policies > Incoming mail policies** (Policy di posta > **Criteri posta in arrivo)**.

Il nome del filtro deve essere visualizzato nella colonna Filtri contenuto e nella riga dei criteri flusso di posta. Se l'elenco è ampio e non è possibile visualizzarne il nome, fare clic sull'elenco dei filtri per identificare i filtri applicati al criterio.

Filtro messaggi:

```
From ESA CLI:
ESA. com> filters
```

```
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

Num Active Valid Name

  1           Y      Y     DKIM_Filter
```

Nell'elenco viene indicato se il filtro è configurato e attivo.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Verificare la configurazione:

Devi accertarti che:

- Il criterio del flusso di posta dispone di dkim: sulla verifica
- Èpresente un'azione configurata in un filtro contenuti o in un filtro messaggi
- Nel caso di un filtro contenuti, verificare che il filtro sia associato a un flusso di posta

Verifica verifica messaggi:

La verifica dei messaggi ci consente di osservare:

- Il risultato della verifica DKIM, ad esempio: permfail
- Voce di log configurata (se ne è stata configurata una)
- Il filtro applicato (nome e azione eseguita)

Tracciamento dall'ESA:

```
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 From: <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 RID 0 To: <userb@domainb.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 Message-ID '<3903af$2r@mgt.esa.domain.com>Fri Apr 26
11:33:44 2019 Info: MID 86 DKIM: permfail body hash did not verify [final]
Fri Apr 26 11:33:44 2019 Info: MID 86 Subject "Let's go to camp!"
Fri Apr 26 11:33:44 2019 Info: MID 86 ready 491 bytes from <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 matched all recipients for per-recipient policy
Allow_only_user in the inbound table
Fri Apr 26 11:33:46 2019 Info: MID 86 interim verdict using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 interim AV verdict using Sophos CLEAN
Fri Apr 26 11:33:46 2019 Info: MID 86 antivirus negative
Fri Apr 26 11:33:46 2019 Info: MID 86 AMP file reputation verdict : UNSCANNABLE
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: GRAYMAIL negative
Fri Apr 26 11:33:46 2019 Info: MID 86 Custom Log Entry: The content that was found was:
DkimFilter
```

```
Fri Apr 26 11:33:46 2019 Info: MID 86 Outbreak Filters: verdict negative
Fri Apr 26 11:33:46 2019 Info: MID 86 quarantined to "DkimQuarantine" by add-footer filter
'DkimFilter '
Fri Apr 26 11:33:46 2019 Info: Message finished MID 86 done
```

Informazioni correlate

- Procedure ottimali ESA-SPF-DKIM-DMARC
- Guida per l'utente finale di Email Security Appliance
- DKIM RFC4871
- DKIM RFC8301
- DKIM RFC8463
- Documentazione e supporto tecnico – Cisco Systems