Konfigurieren des eingehenden Filters auf Basis der DKIM-Verifizierung in der ESA

Einführung

In diesem Dokument wird beschrieben, wie die E-Mail-Security-Appliance (ESA) so konfiguriert wird, dass alle Maßnahmen zur Überprüfung von Domain Keys Identified E-Mail (DKIM) über eine Konfiguration von Content-Filtern oder Nachrichtenfiltern durchgeführt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ESA
- Grundkenntnisse der Konfiguration von Content-Filtern
- Grundkenntnisse der Konfiguration von Nachrichtenfiltern
- Zentralisierung der Konfigurationskenntnisse in den Bereichen Richtlinien, Viren und Outbreak Quarantine

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt 1: Konfigurieren der DKIM-Verifizierung

Stellen Sie sicher, dass die DKIM-Überprüfung aktiviert ist. Navigieren Sie zu **Mail-Policys > Mail Flow-Policys**.

Die Konfiguration der DKIM-Verifizierung auf der ESA ähnelt der SPF-Verifizierung. In den **Standard-Policy-Parametern** der Mail Flow-Policys aktivieren Sie einfach die DKIM-Verifizierung **ein**.

Schritt 2: Abschließende Aktion überprüfen

Bestimmen Sie zunächst die Maßnahmen, die gemäß der DKIM-Verifizierung ergriffen werden sollen. Beispiel: können Sie ein Tag oder eine Quarantäne hinzufügen. Wenn die letzte Aktion

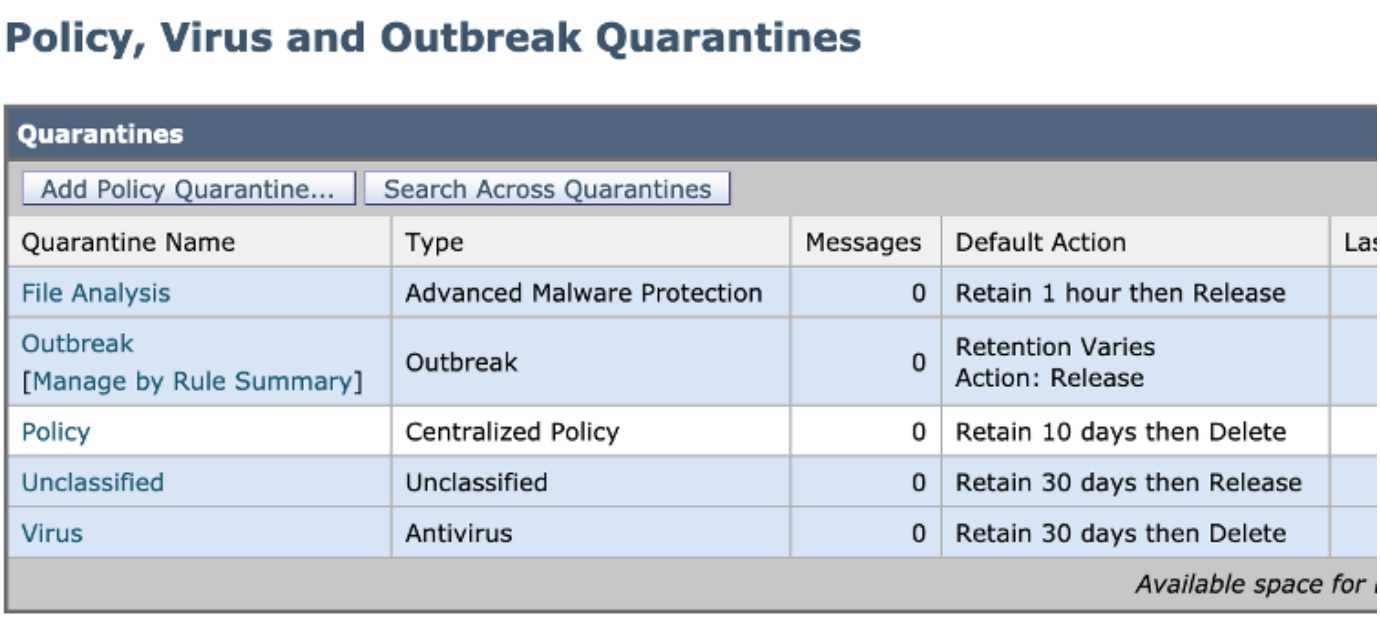
darin besteht, die E-Mail zu isolieren, überprüfen Sie die konfigurierte Quarantäne.

- Wenn Sie keine zentrale Verwaltung verwenden:

Navigieren Sie zu **ESA >Monitor> Policy, Virus and Outbreak Quarantines**.

- Wenn Sie eine zentrale Verwaltung (SMA) konfiguriert haben:

Navigieren Sie zu **SMA >Email >Message Quarantine > Policy, Virus and Outbreak Quarantines**, wie im Bild gezeigt:

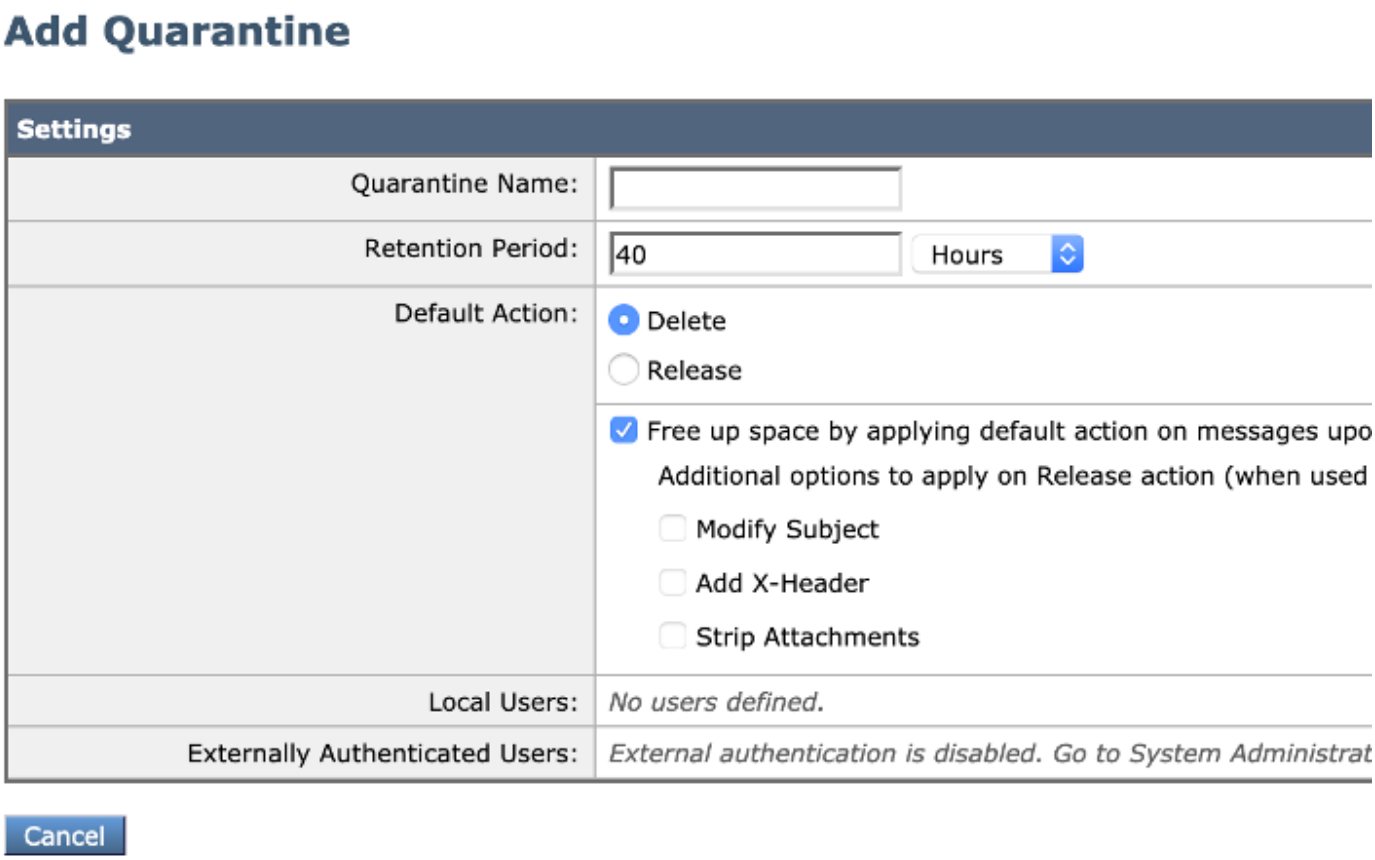


Wenn keine spezifische Quarantäne für **DKIM**/Domain-basierte Nachrichtenauthentifizierung, Reporting & Conformance (DMARC)/Sender Policy Framework (SPF)-Dienste vorliegt. Es wird empfohlen, eine zu erstellen.

Wählen Sie unter "Policy, Virus and Outbreak Quarantines" die Option **Policy Quarantine hinzufügen aus**:

Hier können Sie Folgendes einrichten:

- Quarantänename: Für ex, **DkimQuarantine**
- Aufbewahrungszeitraum: Es liegt an Ihnen und hängt von den Anforderungen Ihres Unternehmens und der Standardaktion ab. Nach Ablauf der Aufbewahrungsfrist für die E-Mail wird gelöscht, veröffentlicht und zugestellt, bestimmt durch Ihre Auswahl, wie im Bild gezeigt:

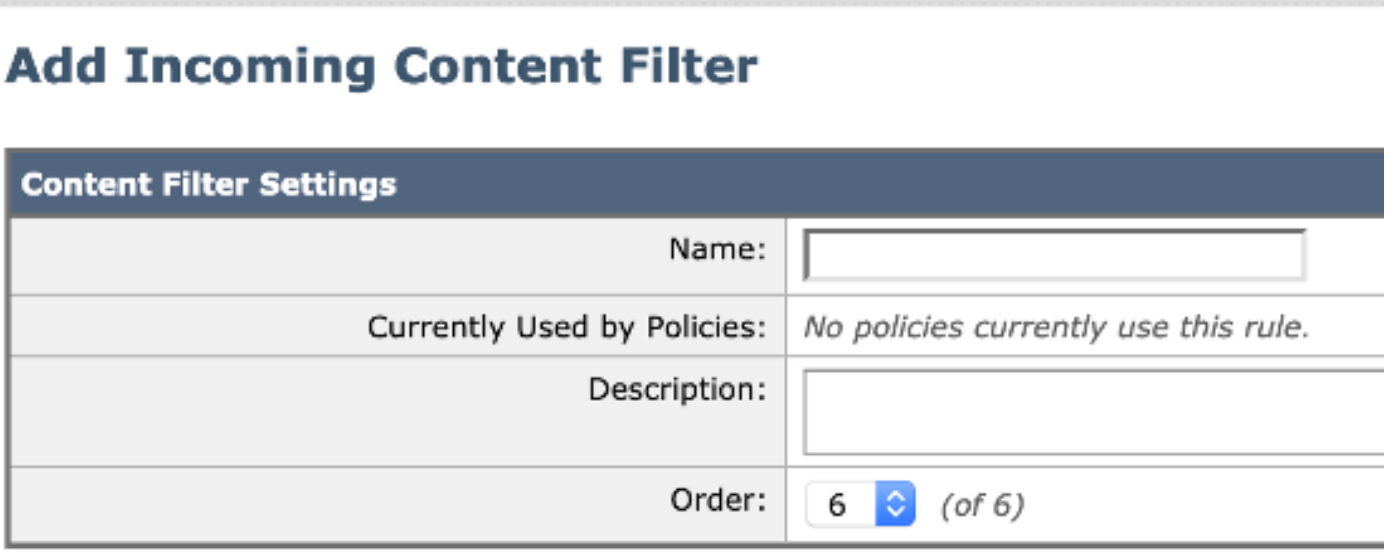


Schritt 3: Eingehender Filter für ESA

a) Erstellen Sie einen Filter für eingehende Inhalte für die ESA:

Navigieren Sie zu **ESA > Mail Policies > Incoming Content Filters > Add Filter (E-Mail-Policys > Filter hinzufügen)**.

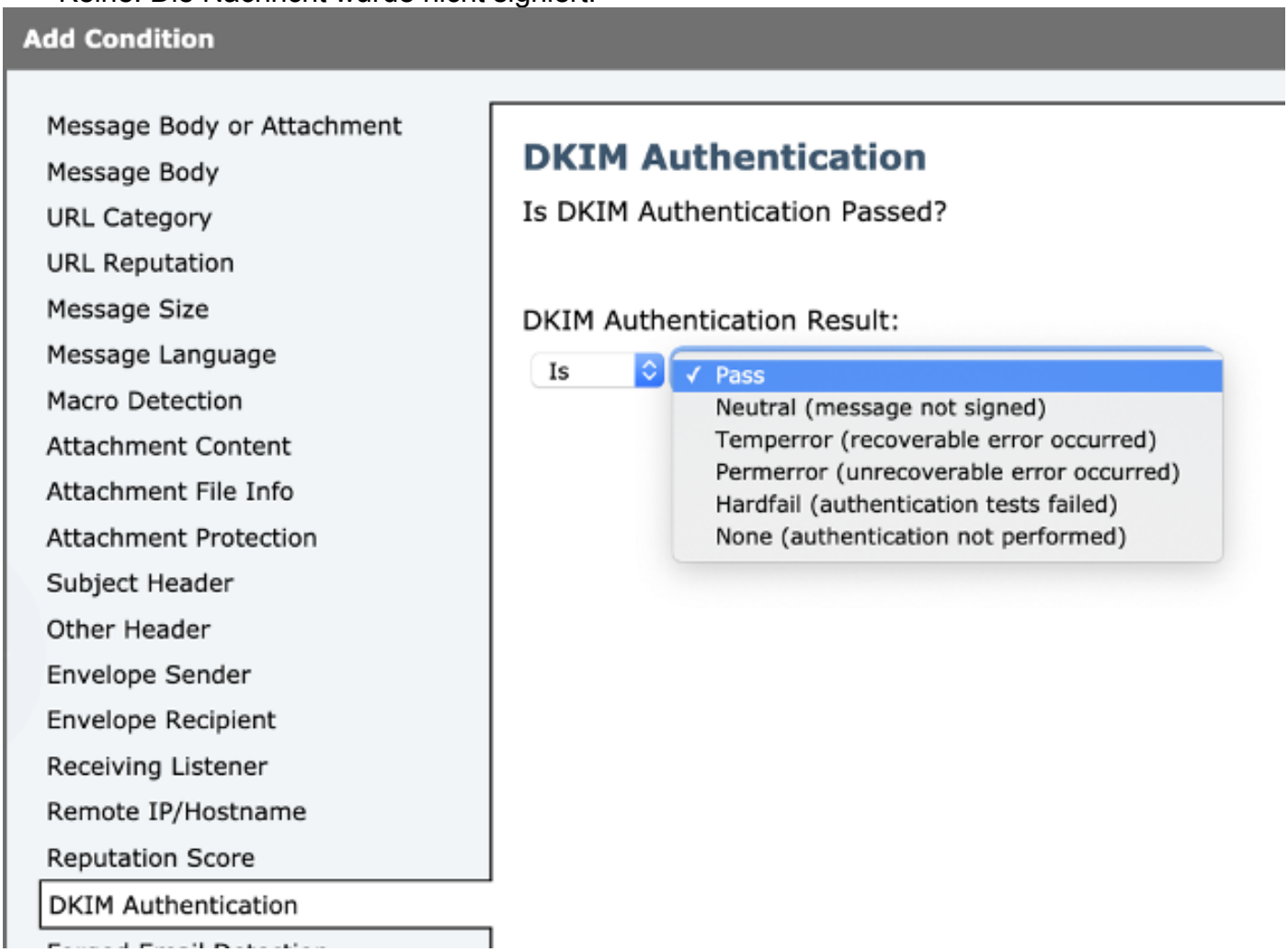
- Erster Abschnitt: Sie können den **Namen**, die **Beschreibung** und die **Reihenfolge** des Filters konfigurieren:



- Abschnitt 2: Bedingung hinzufügen. Sie können mehrere Bedingungen hinzufügen und weitere Content-Filter konfigurieren, um die DKIM-Verifizierung zu aktivieren:

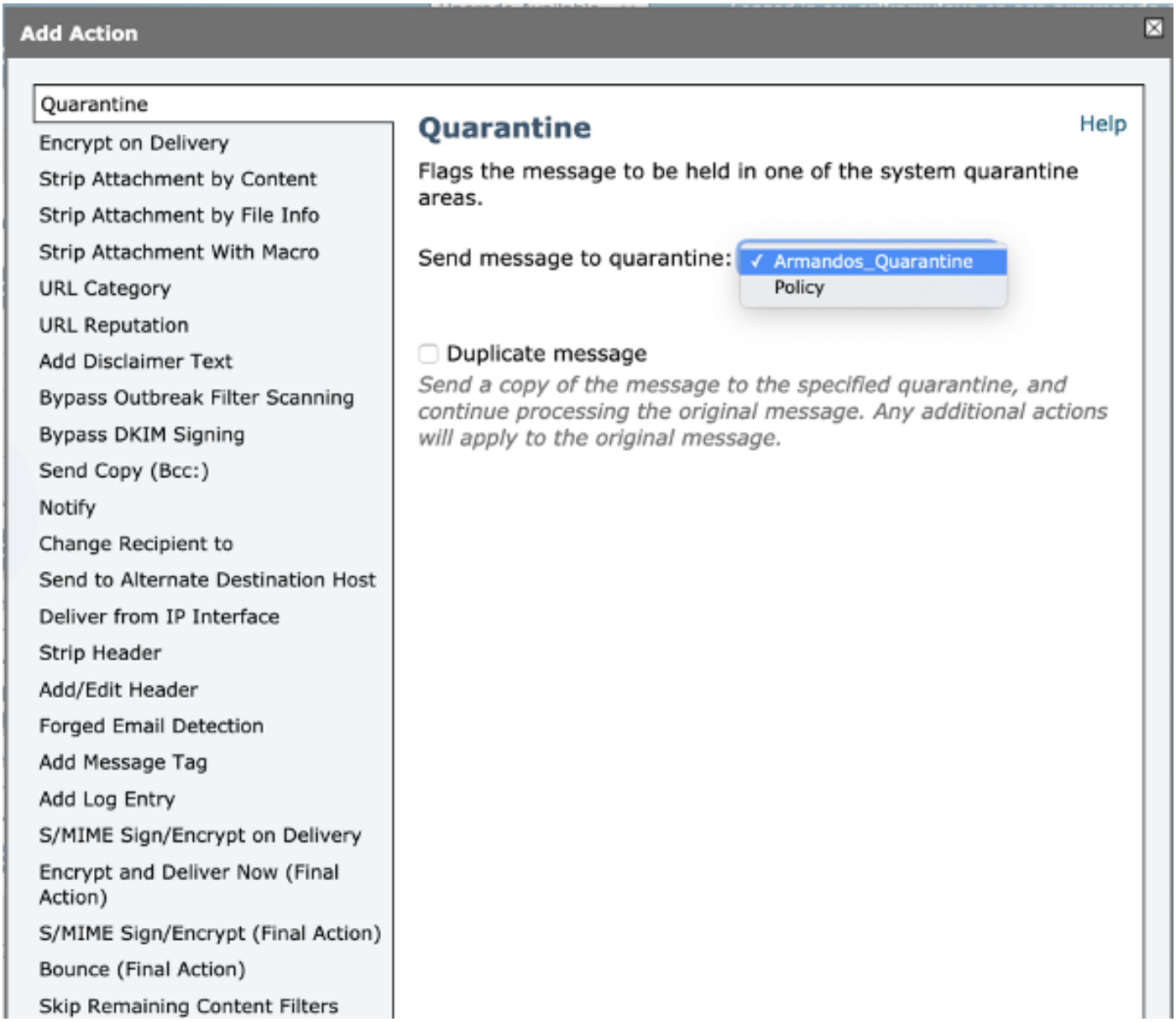
Authentifizierungsergebnisse erwartet und Bedeutung:

- Bestehen: Die Nachricht hat die Authentifizierungstests bestanden.
- Neutral: Die Authentifizierung wurde nicht durchgeführt.
- Temperror: Ein behebbarer Fehler ist aufgetreten.
- Permerror: Ein nicht behebbarer Fehler ist aufgetreten.
- Hardfail: Die Authentifizierungstests sind fehlgeschlagen.
- Keine. Die Nachricht wurde nicht signiert.



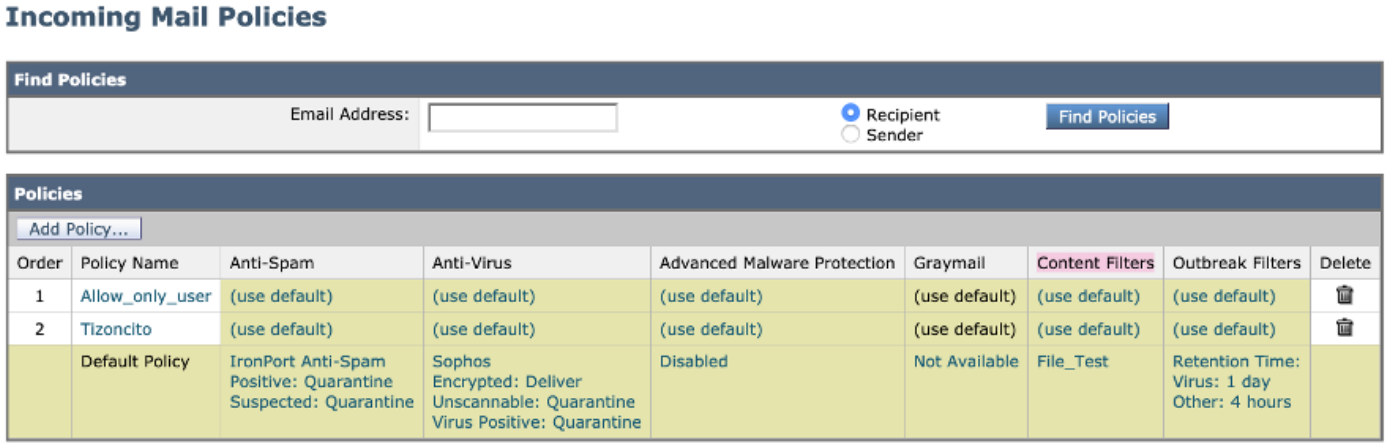
Hinweis: DKIM-Verifizierungsanforderungen: Der Absender muss die Nachricht signieren, bevor sie verifiziert werden kann. Die sendende Domäne muss über einen öffentlichen Schlüssel verfügen, der im DNS zur Überprüfung verfügbar ist.

- Dritter Abschnitt: Wählen Sie eine Aktion aus. Sie können mehrere Aktionen hinzufügen, z. B. einen Protokolleintrag hinzufügen, eine E-Mail an Quarantäne senden, eine E-Mail löschen, Benachrichtigungen senden usw. Wählen Sie in diesem Fall die zuvor konfigurierte Quarantäne aus, wie im Bild gezeigt:



Neue Filter-Mail-Flow-Richtlinie hinzufügen:

Nachdem ein Filter erstellt wurde. Fügen Sie von der ESA den Filter für jede Mail-Fluss-Richtlinie hinzu, in der Sie DKIM mit einer abschließenden Aktion überprüfen möchten. Navigieren Sie zu **ESA> Mail Policies > Incoming Mail Policies (E-Mail-Policys für eingehende E-Mails)**, wie im Bild gezeigt:



Klicken Sie auf die Spalte **Content-Filter** und die Zeile **Mail Flow-Richtlinie**.

> **Hinweis**: (Standard verwenden) bedeutet nicht, dass die Aktion als Standardrichtlinieneinstellungen konfiguriert ist. Konfigurieren Sie jede Mail-Flow-Richtlinie mit den erforderlichen Filtern.

b) Erstellen Sie einen Nachrichtenfilter für die ESA:

Der gesamte Nachrichtenfilter wird über die ESA-CLI konfiguriert. Geben Sie den Befehl **Filters** ein, und befolgen Sie die Anweisungen:

```
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.
```

Überprüfen Sie nach dem Erstellen des Filters die Legende: **1 Filter hinzugefügt**.

Die zu konfigurierenden Bedingungen und Aktionen entsprechen denen, die vom Filter für eingehende Inhalte verwendet werden.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Filter für eingehende Inhalte:

- Von der ESA-Webbenutzeroberfläche (WebUI)

a) Überprüfen Sie, ob der Filter konfiguriert ist:

Navigieren Sie zu **ESA > Mail-Policys > Filter für eingehende Inhalte.** Der Filter muss entsprechend der zuvor in der angezeigten Liste ausgewählten Reihenfolge konfiguriert werden.

b) Überprüfen Sie, ob der Filter angewendet wird:

Navigieren Sie zu **ESA>Mail-Policys > Richtlinien für eingehende E-Mails**.

Der Name des Filters muss in der Spalte Content-Filter und in der Zeile Mail-Flow-Richtlinie angezeigt werden. Wenn die Liste breit ist und Sie den Namen nicht sehen können, klicken Sie auf die Filterliste, um die auf die Richtlinie angewendeten Filter zu identifizieren.

Nachrichtenfilter:

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
```

Die Liste zeigt, ob der Filter konfiguriert und aktiv ist.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Konfiguration überprüfen:

Sie müssen sicherstellen, dass

- Die Mail-Flow-Richtlinie hat dkim: bei Überprüfung
- In einem Content-Filter oder Nachrichtenfilter ist eine Aktion konfiguriert.
- Überprüfen Sie bei einem Content-Filter, ob der Filter einem Mail-Fluss zugeordnet ist.

Nachrichtenverfolgung überprüfen:

Die Nachrichtenverfolgung ermöglicht uns Folgendes zu beobachten:

- Ergebnis der DKIM-Verifizierung, z. B.: durchlassen
- Der konfigurierte Protokolleintrag (falls konfiguriert)
- Angewendeter Filter (Name und Aktion)

Nachverfolgung von der 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
```

Zugehörige Informationen

- Best Practices ESA-SPF-DKIM-DMARC
- Email Security Appliance - Benutzerhandbuch
- DKIM RFC 4871
- DKIM RFC8301
- DKIM RFC8463
- Technischer Support und Dokumentation - Cisco Systems