Inkomend filter configureren op basis van DKIM-verificatie in de ESA

Inleiding

In dit document wordt beschreven hoe u de e-mail security applicatie (ESA) kunt configureren om actie te ondernemen met betrekking tot Domain Keys Identified Email (DKIM)-verificatie via een inkomend contentfilter of configuratie van het berichtenfilter.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ESA
- Basiskennis van de configuratie van het filter van de inhoud
- Basiskennis van de configuratie van berichtfilters
- Configuratiekennis voor Centraliseringsbeleid, virus en uiteinde

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Stap 1. Controleer DKIM

Zorg ervoor dat DKIM-verificatie is ingeschakeld. Navigeer naar **Mail-beleid > Mail Flow**.

Om de DKIM-verificatie op de ESA te configureren is gelijk aan de SPF-verificatie. In de **standaardbeleidsparameters** van het beleid van de Mail Flow, schakelt u de DKIM Verificatie eenvoudigweg **in**.

Stap 2: Controleer de definitieve actie

Geef eerst aan welke maatregelen moeten worden genomen overeenkomstig de DKIM-verificatie. Ex: Laat vallen, voeg een tag of quarantaine toe. Als de laatste actie in quarantaine is gezet, bekijkt u de ingestelde Quarantines.

- Als u geen gecentraliseerd beheer gebruikt:

Navigeer naar **ESR > Monitor> Beleids-, virussen- en uitbraakwachttijden**.

- Als u gecentraliseerd beheer (SMA) hebt ingesteld:

Navigatie naar **SMA > E-mail > Berichtlijnen quarantaine > Policy, Virus en Outbreak Quarantines**, zoals in de afbeelding getoond wordt:

Policy, Virus and Outbreak Quarantines

Quarantines

Add Policy Quarantine... | Search Across Quarantines

Quarantine Name	Type	Messages	Default Action	Las
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	
Policy	Centralized Policy	0	Retain 10 days then Delete	
Unclassified	Unclassified	0	Retain 30 days then Release	
Virus	Antivirus	0	Retain 30 days then Delete	

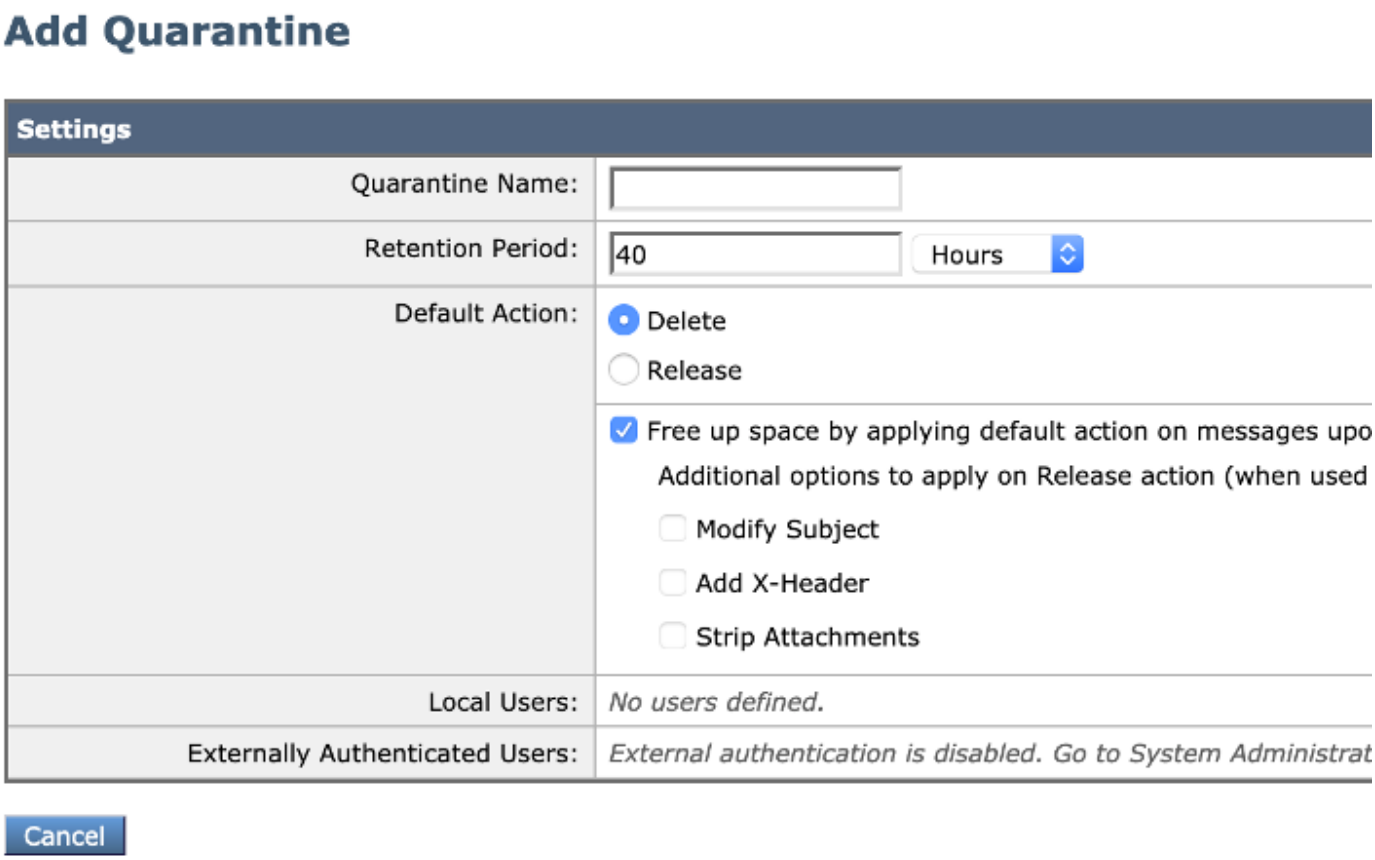
Available space for

Als er geen specifieke quarantaine is voor **DKIM**/Domain-Based Berichtverificatie, Reporting & Conformance (DMARC)/Sender Policy Framework (SPF)-services. Aanbevolen wordt om er een te maken.

Terwijl u Quarantines voor beleid, virussen en uitbraken selecteert, selecteert u **Policy Quarantine toevoegen**:

Hier kunt u instellen:

- Quarantine name: Voor bijv. **DKimQuarantine**
- Bewaarperiode: Het is aan u en is afhankelijk van de behoeften van uw organisatie en de actie Default. Nadat de bewaartijd in de e-mail is verstreken of weer wordt vrijgegeven en bezorgd, wat wordt bepaald door uw selectie, zoals in de afbeelding wordt weergegeven:



Stap 3: Inkomend filter voor het ESR

a. Een inkomend inhoudsfilter voor ESA maken:

Navigeer naar **ESA > Mail Policies > Inkomend contentfilters > Add filter**.

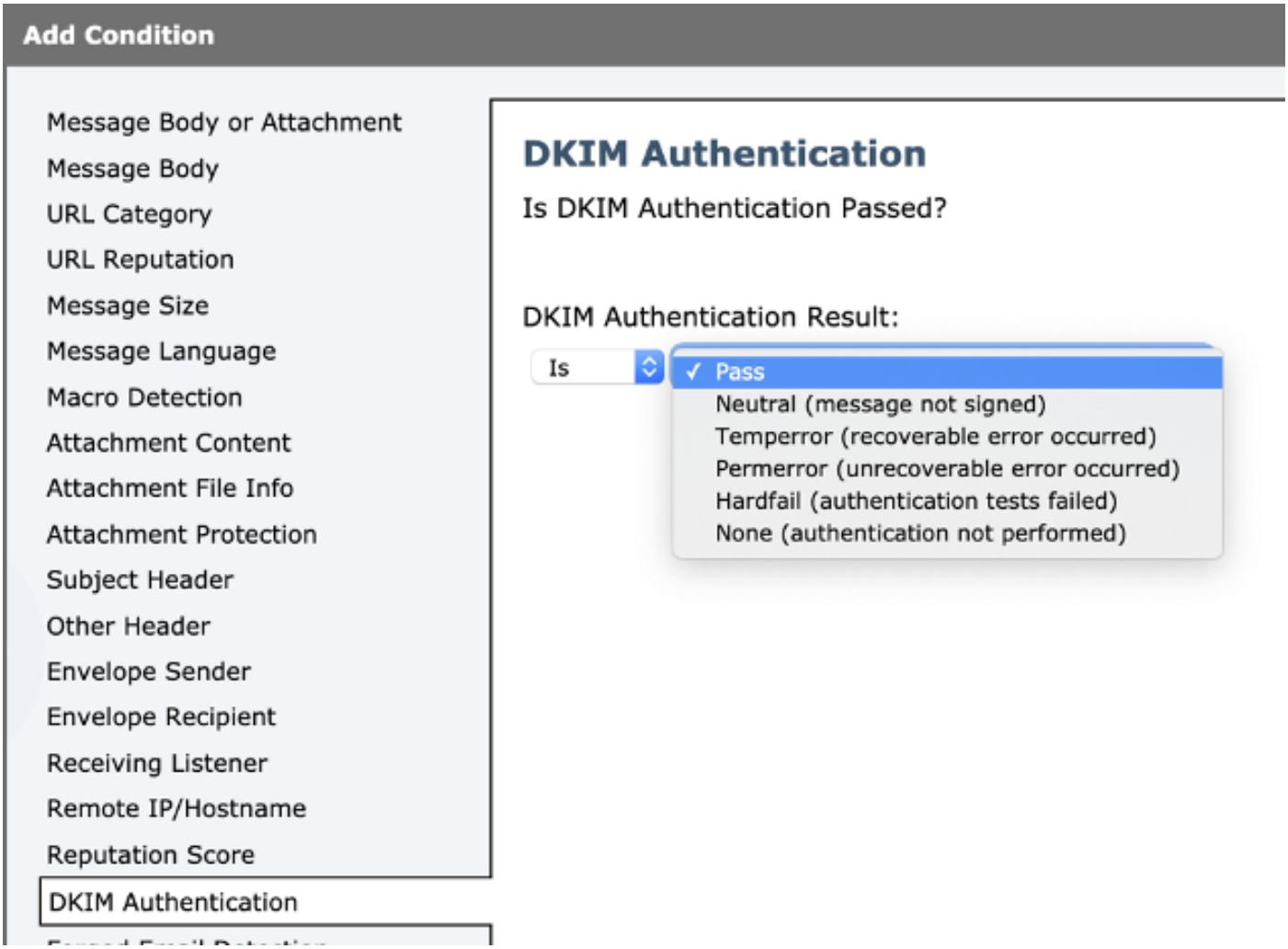
- Eerste afdeling: U kunt de **naam**, **beschrijving** en **volgorde** van het filter configureren:

- Tweede deel: Voeg conditionering toe. U kunt meer dan één voorwaarde toevoegen en u kunt meer contentfilters configureren om actie te ondernemen met een DKIM-verificatie:

Verwachte verificatie-resultaten en betekenis:

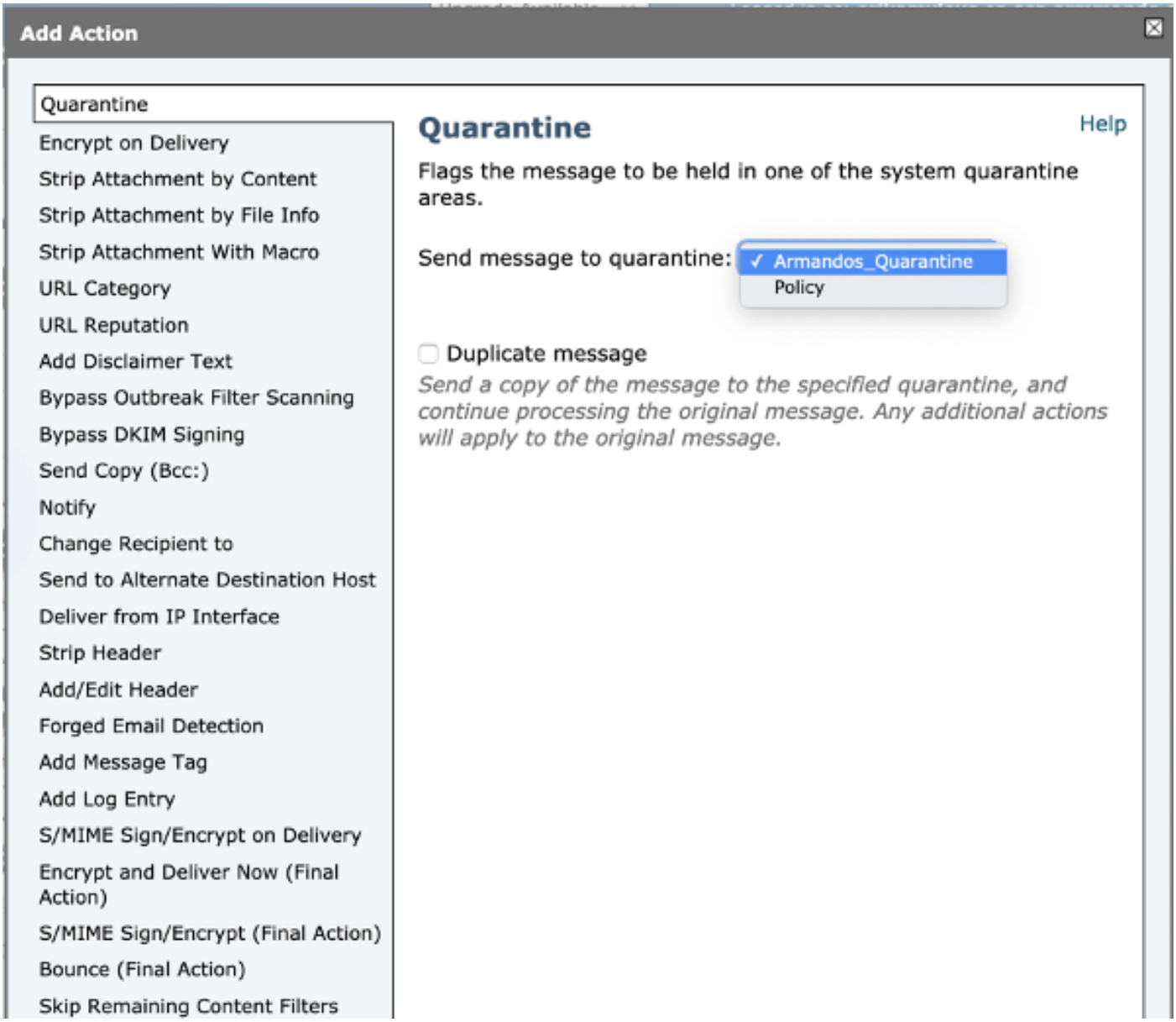
- Pass: Het bericht werd goedgekeurd door de verificatietests.

- Neutraal: Verificatie is niet uitgevoerd.
- Temperatuur Er is een herstelbare fout opgetreden.
- Permerror: Er is een niet-herstelbare fout opgetreden.
- Hardfabel: De verificatietests zijn mislukt.
- None. Het bericht is niet ondertekend.



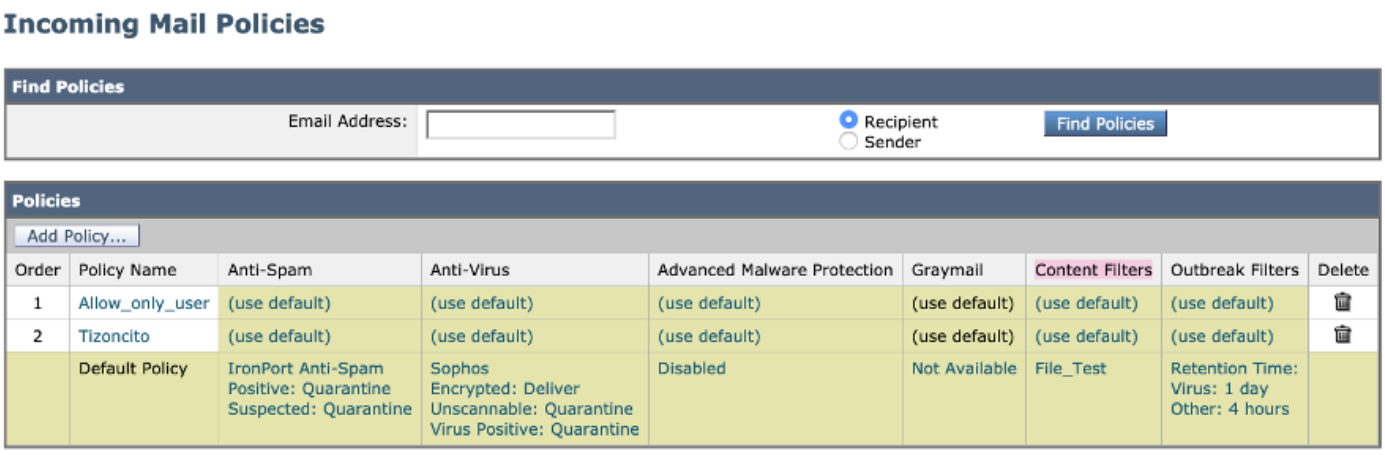
Opmerking: Eisen voor DKIM-verificatie: De afzender moet het bericht ondertekenen voordat het kan worden geverifieerd. Het verzendende domein moet een openbare sleutel hebben die in DNS beschikbaar is voor verificatie.

- Derde deel: Selecteer een actie. U kunt meer dan één actie toevoegen zoals een logbestand toevoegen, naar quarantaine versturen, de e-mail laten vallen, melden, enzovoort. Selecteer in dit geval de eerder ingestelde quarantaine, zoals in de afbeelding:



Voeg nieuw filter toe aan beleid voor Mail flow:

Nadat een filter is gemaakt. Voeg het filter in elk poststroombeleid toe waar u de DKIM met een laatste actie wilt controleren. Navigeer naar **ESR> Mail-beleid > Income Mail-beleid**, zoals in de afbeelding getoond:



Klik op de rij **Content Filters** en **Mail Flow**.

Opmerking: (gebruik standaard) actie betekent niet dat deze is ingesteld als standaardinstellingen voor beleid. Configureer elk poststroombeleid met de benodigde filters.

b. Maak een berichtfilter voor ESA:

Alle berichtfilter is geconfigureerd vanuit ESA CLI. Voer de opdrachtfilters in en volg de instructies:

```
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.
```

Nadat het filter is gemaakt, controleert u de legende: **1 filters toegevoegd**.

De omstandigheden en acties die moeten worden geconfigureerd zijn dezelfde als die welke worden gebruikt door het inkomende contentfilter.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Inkomend inhoudsfilter:

- Van ESA Web User Interface (WebeiUI)

a. Controleer of het filter is ingesteld:

Navigeer naar **ESR > Mail - beleid > inkomende contentfilters.** Het filter moet worden ingesteld in overeenstemming met de volgorde die eerder in de opgeroepen lijst is geselecteerd.

b. Controleer of het filter is gebruikt:

Navigeer naar het **ESR>Mail-beleid > Inkomenspostbeleid**.

De naam van het filter moet in de kolom Content Filters en de rij Mail Flow worden weergegeven. Als de lijst breed is en u de naam niet kunt zien, klikt u op in de filterlijst om de filters te identificeren die op het beleid worden toegepast.

Berichtfilter:

```
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
```

De lijst toont als het filter ingesteld en actief is.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Controleer de configuratie:

U moet ervoor zorgen dat:

- Het poststroombeleid heeft kritiek: betreffende verificatie
- Er wordt een actie ingesteld in een inhoudsfilter of berichtfilter
- In het geval van een inhoudfilter, bevestig dat het filter met een poststroom wordt geassocieerd

Controleer het volgende bericht:

Berichttracering stelt ons in staat om te observeren:

- Het resultaat van de DKIM-verificatie, bijvoorbeeld: permitteren
- De geconfigureerde logingang (indien een is ingesteld)
- Het toegepaste filter (naam en gevolg)

Tracking vanuit de ESE:

```
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
```

Gerelateerde informatie

- Best Practices ESA-SPF-DKIM-DMARC
- Eindgebruikershandleiding voor e-mail security applicatie
- DKIM RFC4871
- DKIM RFC8301
- DKIM RFC8463
- Technische ondersteuning en documentatie – Cisco Systems