

Filter om berichten aan te pakken die DMARC-verificatie overgeslagen hebben

Inhoud

[Inleiding](#)

[Vereisten](#)

[Voorwaarden](#)

[Achtergrondinformatie](#)

[Omzetfilter](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe een filter wordt gemaakt naar actie-mails die DMARC-verificatie (Domain Based Berichtverificatie) en Cloud Email Security (CES) hebben overgeslagen in de e-mail security applicatie (ESA) en Cloud Email Security (CES).

Vereisten

Voorwaarden

- AsyncOS 11.1.2 en verder.
- Begrip van DMARC. (<https://tools.ietf.org/html/rfc7489#page-56>)
- ESA/CES met DMARC-verificatie ingeschakeld.

Achtergrondinformatie

ESA/CES met DMARC-verificatie ingesteld op het poststroombeleid, waarbij bericht tracking/mail_logs de loglijn opleveren: **DMARC: Verificatie overgeslagen (het verzendende domein kan niet worden bepaald)**".

Deze loglijn betekent dat ESA/CES meer dan één domein-identiteit heeft gedetecteerd in de header en als er meer dan één e-mailadres in de header is deze header overgeslagen bij de meeste DMARC-implementaties. Kop verwerken met meer dan één domein-identiteit wordt blootgesteld als buiten bereik in de DMARC-specificatie.

Omzetfilter

De versie van Cisco AsyncOS 11.1.2 en de daaropvolgende releases voegen een nieuwe functie toe waar het apparaat een nieuwe x-header bevat die verschillende versies bevat DMARC-controleresultaten met een unieke waarde gebaseerd op de DMARC-controleresultaten.

Er zijn vier veldnamenwaarden beschikbaar om geldig overslaan te filteren, overslaan ongeldig te

maken, de temperatuur en de druk te temperen.

Opmerking: In de gevallen waarin DMARC-verificatie niet kon worden uitgevoerd omdat er speciale tekens waren of de kop van de kop verkeerd was vormd of er een DMARC-controle was mislukt vanwege een ander ongeldig overslaan of ongeldig overslaan, wordt de toegevoegde x-kop toegevoegd: **X-Ironport-Dmarc-Check-Resultaat:** ongeldig overslaan of geldig overslaan.

Opmerking: Dit filter kan zowel op de Berichtfilters (CLI-beperkingen) als op de contentfilters worden ingezet.

Kop-waarden:

- **Valid skip** beschrijft de gevallen waarin de DMARC-verificatie niet kon worden uitgevoerd wanneer er een bestand van kop of geen DMARC-record is.
- **Ongeldig skip** behandelt de gevallen waar er ongeldige tekens in de kop staan, veelvoudig van kopregels, meerdere domeinentiteiten in de kop van kop, het afzender adres heeft niet-US-ASCII tekens en als er een fout is in het parsen van waarden in het veld van de kop.
- **Permerror** omvat gevallen waarin er een permanente fout is opgetreden tijdens de DMARC-evaluatie, zoals het tegenkomen van een syntactisch onjuist DMARC-record. Het is onwaarschijnlijk dat een latere poging uiteindelijk resultaat zal opleveren.
- **De temperatuur** bestrijkt gevallen waarin een tijdelijke fout tijdens de DMARC-evaluatie heeft plaatsgevonden. Een latere poging kan een eindresultaat opleveren.

Het volgende is het DMARC-filter dat de "**X-Ironport-Dmarc-Check-Resultaat**" controleert op een **ongeldig overslaan** en vervolgens in quarantaine wordt geplaatst.

De actie kan waar nodig aan andere eisen worden aangepast.

Berichtfilter

```
Quarantine_messages_DMARC_skip:
if header("X-Ironport-Dmarc-Check-Result") == "^invalidskip$"
{
quarantine("Policy");
}
```

Content Filter

Add Incoming Content Filter

Content Filter Settings			
Name:	<input type="text" value="DMARC_Invalidskip_Check"/>		
Currently Used by Policies:	No policies currently use this rule.		
Description:	<input type="text"/>		
Order:	<input type="text" value="1"/> ▼	(of 12)	

Conditions			
<input type="button" value="Add Condition..."/>			
Order	Condition	Rule	Delete
1	Other Header	header("X-Ironport-Dmarc-Check-Result") == "^invalidskip\$"	

Actions			
<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Quarantine	quarantine("Policy")	

Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)
- [Wat is DMARC?](#)