DMARC-controle op e-mail security applicatie omzeilen

Inhoud

Inleiding

In dit document wordt beschreven hoe de op Domain Based Berichtverificatie, Rapportage en Conformiteit (DMARC) gebaseerde controle van e-mail security applicatie (ESA) moet worden omzeild. Raadpleeg Inleiding over e-mailverificatie.

Controleer DMARC

DMARC is een technische specificatie die is opgesteld om het potentieel voor misbruik per e-mail te verminderen. DMARC gestandaardiseert hoe e-mailontvangers e-mailverificatie uitvoeren met behulp van Sender Policy Framework (SPF) en DomainKeys Identified Mail (DKIM) - mechanismen. Om de DMARC-verificatie te kunnen doorgeven, moet een e-mail ten minste één van deze verificatiemechanismen doorgeven en moeten de verificatienummers voldoen aan RFC 5322.

Met het apparaat kunt u:

- Controleer de inkomende e-mails met gebruik van DMARC.
- Definieer profielen om het beleid van eigenaren van domeinen te omzeilen (accepteren, in quarantaine plaatsen of afwijzen).
- Verzend feedback-rapporten naar domeineigenaren, die helpen hun authenticatie-implementaties te versterken.
- Verzend leveringsfoutmeldingen naar de eigenaars van het terrein als het DMARC-aggregaat groter is dan 10 MB of de grootte die is gespecificeerd in de rapportage-tag (RUA) van het DMARC-record.

AsyncOS kan e-mails verwerken die compatibel zijn met de DMARC-specificatie zoals voorgelegd aan de Internet Engineering Task Force (IETF) op 31 maart 2013. Zie http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02 voor meer informatie.

> **Opmerking:** Het apparaat voert geen DMARC-verificatie uit van berichten uit domeinen met slecht gevormde DMARC-records. Dit soort berichten kan het apparaat echter ontvangen en verwerken.

DMARC-omzeilen configureren

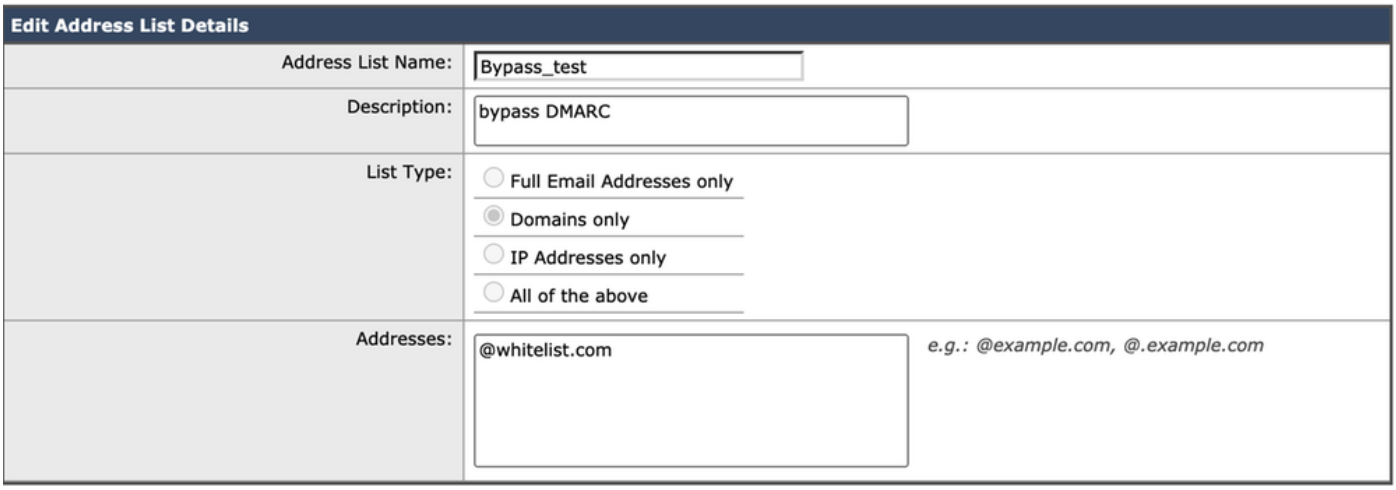
Als als beheerder uw vereiste is om DMARC verificatie van berichten van specifieke zenders over te slaan, zult u weinig stappen moeten volgen om de bypass succesvol te bereiken. Hieronder volgt een overzicht van de maatregelen:

> **Opmerking:** Adreelijsten die met het gebruik van volledige e-mailadressen of domeinen worden gemaakt, kunnen alleen worden gebruikt om DMARC-verificatie te omzeilen. U kunt een **adreslijst** met de optie **Alle bovenstaande opties** gebruiken. Indelingen met alleen een domeinadres/volledig e-mailadres of een gedeeltelijk domeinadres werken echter voor een uitzondering. U moet het **domein/volledig e-mailadres** gebruiken dat in de **Van** header wordt genoemd.

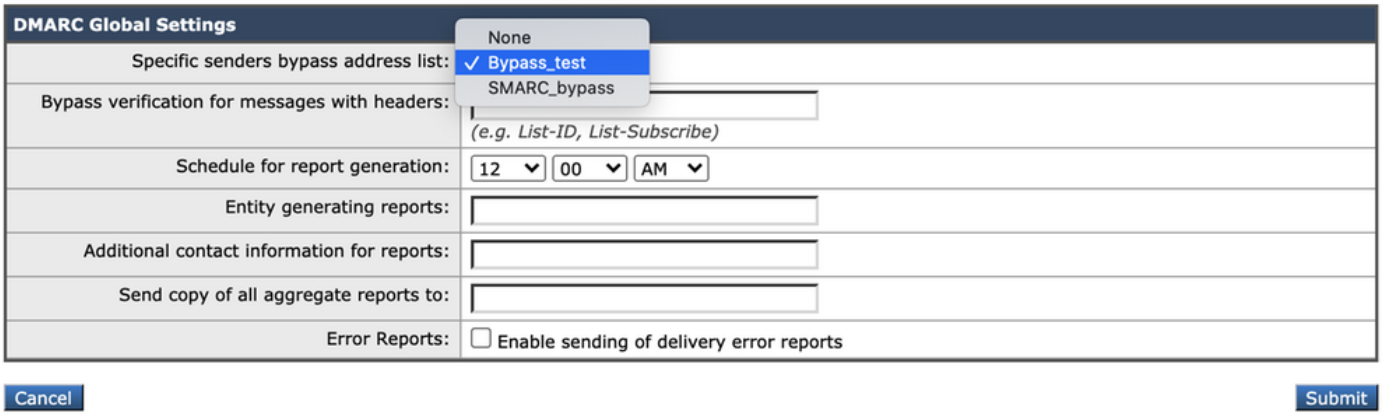
1. Zorg ervoor dat **DICOM-verificatie** is ingeschakeld voor het gekoppelde Mail Flow-beleid.
2. Navigeer naar **postbeleid > adreslijst**.
3. Klik op **adreslijst toevoegen**.
4. Maak een **adreslijst** door de details in te vullen.
5. Klik op **Inzenden**.
6. Zodra de **adreslijst** is gemaakt, moet u de lijst naar **DMARC Specific Senders Bypass List** bellen.

Hier is een voorbeeld van hoe de omzeilingconfiguratie kan worden geconfigureerd en hoe houtkap zal worden gedaan:

De adreslijst wordt aangemaakt met "**Alleen** domein" als voorbeeld en toegevoegd aan de gegevens **van** de header.



Zodra uw adreslijst met alle gewenste items is gemaakt, moet u de **adreslijst** bellen onder de **DMARC Specific Senders Bypass Address List**. U moet **in** het **postbeleid > DMARC > Global Settings** bewerken en uw nieuwe **adreslijst** bellen door op de vervolgkeuzelijst te klikken, zoals hieronder wordt getoond:



Verschil in Mail_Logs

Hier wordt een weergave van de mail_logs gepresenteerd die helpen het verschil tussen houtkap te begrijpen, wanneer de DMARC van een domein gevalideerd wordt en wanneer het zo is ingesteld dat het overslaat.

Mail Logs wanneer DMARC is ingeschakeld:

```
Sat Mar 20 21:14:22 2021 Info: ICID 57 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable

Sat Mar 20 21:14:22 2021 Info: Start MID 76571 ICID 57

Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 From:

Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 RID 0 To:

Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC: Verification skipped (No record found for the
sending domain)

Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC:

Sat Mar 20 21:14:23 2021 Info: MID 76571 Message-ID '<613a1e1b-998a-6375-8887-
ab2c6d430256@whitelist.com>'

Sat Mar 20 21:14:23 2021 Info: MID 76571 Subject 'Test 4'
```

> **Opmerking:** Er is geen record gepubliceerd op het domein @whitelist.com, wat de reden is dat we "No record found for the send domein" zien.

Mail Logs for Bypass DMARC Controleer

```
Sat Mar 20 21:15:36 2021 Info: ICID 58 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable

Sat Mar 20 21:15:37 2021 Info: Start MID 76572 ICID 58

Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 From:

Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 RID 0 To:
```

```
Sat Mar 20 21:15:37 2021 Info: MID 76572 DMARC: Verification skipped (Local bypass
configuration)

Sat Mar 20 21:15:37 2021 Info: MID 76572 Message-ID '<2ba742a2-f8ba-9ff0-7dc9-
362421f5177e@whitelist.com>'

Sat Mar 20 21:15:37 2021 Info: MID 76572 Subject 'Test Bypass DMARC'
```

Gerelateerde informatie

- Inzicht in DMARC-werkingen
- Inkomende berichten controleren met DMARC
- Filter om berichten aan te pakken die DMARC-verificatie overgeslagen hebben
- Technische ondersteuning en documentatie – Cisco Systems