DMARC-fouten oplossen door SPF- en DKIM-uitlijning te corrigeren

Inhoud

uitgifte

E-mails van specifieke domeinen worden geblokkeerd door de Cisco Secure Email Gateway (CES/ESA) vanwege fouten in de DMARC-verificatie. Analyse van het volgen van berichten geeft aan dat deze e-mails in de werkvoorraad worden bewaard en in quarantaine worden geplaatst of worden afgewezen, waardoor ze de beoogde ontvangers niet kunnen bereiken.

milieu

- Cisco Secure Email Gateway (CES/ESA)-apparaten
- SPF-, DKIM- en DMARC-beleid worden geconfigureerd en afgedwongen

resolutie

Samenvattende tabel SPF/DKIM-uitlijning (voorbeelden)

mechanisme	uitlijningsstatus	Envelop/handtekeningdomein	Van domein koptekst	logica
SPF	in uitlijning	sender@example.com	sender@example.com	Directe overeenkomst
SPF	in uitlijning	sender@child.example.com	sender@example.com	Bovenliggende

				domeinovereenko
SPF	Niet in alignment	sender@test.com	sender@example.com	Domeinmismatch
DKIM	in uitlijning	example.com	sender@example.com	Directe overeenkomst
DKIM	in uitlijning	example.com	sender@child.example.com	Relaxed mode ma
DKIM	Niet in alignment	example.com	sender@test.com	Domeinmismatch

Coördineren met afzender (aanbevolen)

- Werk samen met de beheerders van het afzenderdomein om DMARC-storingen te verhelpen door te zorgen voor een goede SPF- en DKIM-uitlijning op het niveau van de koptekst.
- De afzender moet:
    - Zorg ervoor dat het domein dat wordt gebruikt in de SPF-gevalideerde MAIL FROM- of HELO/EHLO-identiteit overeenkomt met het domein in de From-header van de e-mail.
    - Implementeer DKIM-ondertekening waarbij het domein dat is opgegeven in de d= -tag van de DKIM-handtekening, wordt uitgelijnd met het domein Van header.
    - Controleer of het DMARC-beleid correct is geconfigureerd om de gewenste uitlijningsmodus (strikt of ontspannen) en rapportageopties af te dwingen.
- Deze aanpak pakt de hoofdoorzaak van DMARC-storingen aan door zich te richten op de uitlijning van geverifieerde domeinen met het zichtbare From header-domein, dat van cruciaal belang is voor de levering van e-mail op lange termijn.

DMARC-uitzondering maken (alternatief)

- Als herstel door de afzender niet haalbaar is, maakt u een uitzondering op het ESR-apparaat

voor het specifieke afzenderadres om DMARC-controles te omzeilen.

- Dit is een tijdelijke oplossing en moet gepaard gaan met monitoring.

Controleren en valideren

- Nadat u wijzigingen hebt doorgevoerd, controleert u de levering van waarschuwingsmails aan de beoogde ontvangers.
- Controleer de logboeken voor het bijhouden van berichten om te bevestigen dat DMARC-storingen zijn verholpen.
- Blijf bijgewerkte gegevens voor het volgen van berichten analyseren als er problemen met de levering blijven bestaan.

Oorzaak

De belangrijkste oorzaak van quarantaine of afwijzing van e-mail is DMARC-verificatie mislukt als gevolg van SPF en DKIM uitlijning problemen. Deze fouten geven aan dat, hoewel SPF- en DKIM-records correct kunnen worden gepubliceerd, de domeinen die tijdens de e-mailuitwisseling zijn geverifieerd, niet overeenkomen met het Van-header-domein, wat resulteert in quarantaine van e-mails.

Inzicht in DMARC, SPF en DKIM-uitlijning:

- SPF verifieert het domein in de opdrachten MAIL FROM of HELO/EHLO SMTP en vereist dat dit domein wordt uitgelijnd met het domein in de koptekst Van voor DMARC-naleving.
- DKIM maakt gebruik van cryptografische handtekeningen met een ondertekeningsdomein dat is opgegeven in de tag d=, die moet worden uitgelijnd met het domein Van header.
- DMARC bouwt voort op SPF en DKIM door te eisen dat ten minste een van deze geverifieerde domeinen zich aanpast aan het Van header-domein, hetzij precies (strikte modus) of als een subdomein (ontspannen modus).

Het falen van deze domeinuitlijning leidt tot DMARC-fouten en daaropvolgende afwijzing of quarantaine van e-mail, zelfs als de SPF- en DKIM-records zelf correct zijn gepubliceerd en geldig zijn.

Deze uitlijningsfocus zorgt ervoor dat de geverifieerde identiteit overeenkomt met de zichtbare identiteit van de afzender, waardoor spoofing wordt voorkomen en de betrouwbaarheid van e-mail wordt verbeterd.

Gerelateerde inhoud

- SPF-uitlijningsinformatie
- DKIM-uitlijningsgegevens
- Beste praktijken voor e-mailverificatie - Optimale manieren om SPF, DKIM en DMARC te implementeren - Cisco
- Inkomend filter configureren op basis van DKIM-verificatie in ESA - Cisco

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.