SDR-wijzigingen in Sender Domain Exception List voor Async OS15.0 voor Cisco Secure Email Gateway

Inhoud

Inleiding

Dit document presenteert en verklaart een zeer belangrijke verbetering van de functieoptie **Domain Exception List** (SDR) binnen de Sender Domain Reputation (SDR), voor Cisco Secure Email Gateway. (SEG).

Bijgedragen door Chris Arellano Cisco TAC Engineer.

Voorwaarden

AsyncOS 15.0 en nieuwer voor Cisco Secure Email Gateway (SEG).

Algemeen begrip van de SDR - functie.

Vereisten

Schakel de Service voor domeinreputatie van afzender in en maak een adreslijst met de optie Alleen domein.

Gebruikte componenten

Domeinnaam van afzender.

Alleen domeinadreslijst.

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 live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Sender Domain Reputation for SEG is een cloudservice die meerdere afzenderwaarden verzamelt en vonnissen en opties afleidt om actie te ondernemen tegen deze vonnissen. SDR staat instellingen toe om

vertrouwde domeinen te omzeilen door het gebruik van een adreslijst die wordt toegepast op Domain Exception List.

De SDR Domain Exception List voor SEG 15.0 had 2 opties:

- Ingeschakeld = Pas de Envelop van domein aan omzeilen SDR actie.
- Uitgeschakeld = alleen matchen als alle volgende elementen aanwezig zijn: Envelope-from + Friendly From + Reply-To + SPF + DKIM + DMARC .

De nieuwe 15.0 wijziging: De Domain Exception List voor SEG 15.0 en nieuwere opties:

- Ingeschakeld = Pas de Envelop van domein aan omzeilen SDR actie.
- Uitgeschakeld = overeenkomst als het domein aanwezig is in een van de volgende waarden:
  - HELO
  - RDNS
  - Omhulling van
  - Van
  - Antwoord op

Configureren

De focus ligt alleen op de nieuwe opties in de Domain Exception List. De volledige SDR-instellingen en -configuratie worden in de Gebruikersgids meegeleverd.

Navigeer binnen WebUI naar **Beveiligingsservices** > **Domain Reputation**.

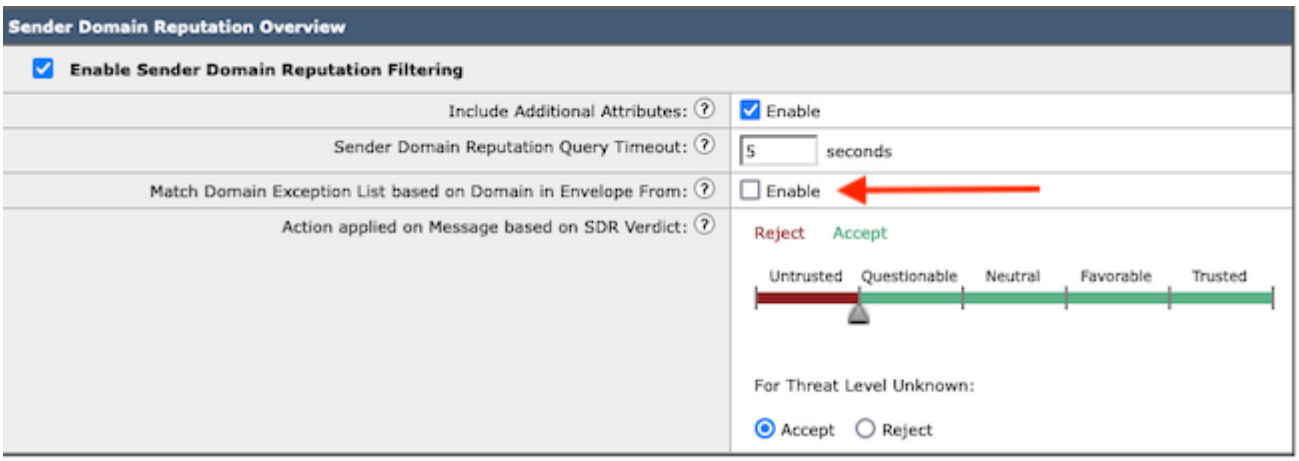
De optie **Match Domain Exception List op basis van het gedeelte Domain Name van de Envelope From**, is standaard ingeschakeld.

Als het bijbehorende **?** informatiepictogram wordt geselecteerd, wordt de nieuwe optie weergegeven.

Schakel deze optie uit als u de SDR-controles wilt overslaan als er domeinen in de 'HELO:', 'RDNS:', 'Envelope From:', 'From:' en 'Reply-To:' kopregels van het bericht overeenkomen met de domeinen die zijn geconfigureerd in de lijst met domeinuitzonderingen.

> **Opmerking**: Standaard worden SDR-controles overgeslagen op basis van het domein in alleen de 'Envelop van:'-header.

Selecteer **Globale instellingen bewerken** om de optie voor het selectievakje te verwijderen, zoals in de afbeelding:



De Domain Exception List zelf is een adreslijst met domeinnamen.

Verifiëren

Om de juiste functie te verifiëren met de nieuwe functionaliteit uitschakelen, hebt u een testbericht nodig dat naar de SEG wordt gestuurd met een overeenkomende domeinwaarde in een van de 5 headerwaarden.

Een voorbeeldlogbestand dat een uitzondering in de Global Exception List aangeeft en binnen een Mail Flow Policy is afgestemd, zou in een vroeg stadium aan de mail_logs presenteren:

- Info: MID 14 SDR: MID 14 bevattende domeinnaam '**test1.com**' kwam overeen met de **algemene** domeinuitzonderingslijst '**SDR-TEST-1**'.

Een voorbeeldlogboek dat een uitzondering aangeeft, zou zowel het domein als de naam van de uitzonderingslijst bevatten.

- Info: MID 16 met domeinnaam '**test3.com**' kwam overeen met de domeinuitzonderingslijst '**SDR-TEST-3**' geconfigureerd in het **filter**.

Problemen oplossen

Als er vragen rijzen over de juistheid van een gekozen berichtvonnis, worden de volgende waarden gedocumenteerd en vergeleken met het bijhouden van berichten.

- Documenteer de Global **Domain Reputation Settings** > **Security Settings** > **Domain Reputation**.
- Controleer de bijbehorende adreslijst die in de algemene domeinreputatie-instellingen is geconfigureerd.
- Verifieer het overeenstemmende Mail Flow Policy gebruikt op basis van het bericht volgen.
- Controleer en noteer details van alle Berichtfilters of contentfilters met Domain Exception Lists geconfigureerd.

Verzamel Berichttracering, e-maillogbestanden en de oorspronkelijke e-mailkopregels.

- Als de Global-uitzondering op een bericht overeenkomt, zijn er geen logitems voor Domain Reputation, gewoon een regel die het overeenkomende domein aangeeft.
- Als de Global Exception List niet overeenkomt op een bericht, zijn er logitems voor Domain Reputation van waaruit om waarden te vergelijken.
    - Info: MID 16 SDR: Domeinen waarvoor SDR is aangevraagd: **reverse DNS host**: Niet aanwezig, **helo**: testl.com, **env-from**: test2.com, **header-from**: te st3.com, **antwoord op**: test5.com
- De e-mailheaders zelf bevatten een van de 5 waarden aanwezig in een individuele e-mail om te vergelijken met de instellingen.

Nadat alle gegevens zijn verzameld, controleert u op overeenkomsten of afwezigheid van overeenkomsten om de juiste functionaliteit te bepalen.

Gerelateerde informatie

- E-mail security installatiehandleiding
- Cisco Secure Email Gateway-startpagina voor ondersteuningshandleidingen

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.