ESA FAQ: Hoe moet ik de verificatie op de ESA configureren?

Inhoud

Inleiding

Dit document beschrijft hoe u de verificatie op de Cisco e-mail security applicatie (ESA) kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ESA
- AsyncOS

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- Cisco ESA, alle versies van AsyncOS

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

In dit deel wordt een overzicht gegeven van het taggen en controleren van de ESE.

Overzicht van de controle in de vorm van bv

Wanneer een e-mail wordt verstuurd met de mogelijkheid van een verificatie, herschrijft uw ESA het adres van de Envelope Sender in het bericht. Bijvoorbeeld, **MAIL VAN: joe@example.com** wordt **MAIL VANUIT: prvs=joe=123ABCDEFG@example.com**. De **123...** string in het voorbeeld is de *aankomende verificatietag* die aan de Envelope Sender wordt toegevoegd zoals deze door uw apparaat wordt verstuurd. Als het bericht begint, bevat het adres van de ontvanger in de bounce doorgaans de waarschuwingstag.

> Opmerking: Raadpleeg het gedeelte **Tagingtoetsen** van **het OPRI-adres configureren** in de **geavanceerde gebruikersgids** voor meer informatie.

U kunt verificatie-tagging systeem in- of uitschakelen als standaard. U kunt ook controle-tagging voor specifieke domeinen in- of uitschakelen. In de meeste situaties, kunt u het standaard inschakelen en vervolgens specifieke domeinen voor uitsluiting opnoemen in de tabel Bestandscontrole.

Wanneer een Content Security Appliance een melding levert met een aanraakbericht dat al een gelabeld adres naar een ander Content Security apparaat in de Geautomatiseerde zone (DMZ) bevat, voegt AsyncOS geen andere tag toe.

> **Voorzichtig:** Als u verificatie bij een aanval toestaat, kan dit ervoor zorgen dat uw apparatuur de legitieme e-mail afwijst die met een lege Envelope Sender wordt verstuurd.

Hoe moet ik de verificatie op de ESA configureren?

Voltooi deze stappen om verificatie aan de voorkant van de ESA te configureren:

1. Navigeer naar **Mail Policies > Bounce Verification** en voer handmatig een tagging key in met een willekeurige selectie van getallen en letters, zoals **4r5t6y7u**.

2. Bewerk de verificatie-instellingen van de voorsprong:

   Navigeer naar **postbeleid > Bestemmingscontroles** en laat controle toe.

   Kies **Default** uit het veld Domain (of uw aangepaste bestemming).

   Klik op **Ja** zodra het venster Default wordt geopend en het gedeelte Bounce Verification verschijnt.

3. Zorg ervoor dat niet-gelabelde (verkeerd georiënteerde) bedragen zijn geblokkeerd:

   Navigeer naar **Mail-beleid > Mail Flow**.

Selecteer het gewenste beleid en vul het gedeelte Beveiligingskenmerken in.

Verzeker u ervan dat de waarde voor Niet-gelabeld geld **Nee** is ingesteld. Bij eerdere versies van AsyncOS moet de waarde voor ongebagatchte obligaties op **Nee** zijn ingesteld.