

SPM wordt ontvangen door Cisco e-mail security applicatie (ESA) in uw organisatie

Inhoud

[Inleiding](#)

[Methoden](#)

[1. Legitiem bericht / marketing e-mail](#)

[2. Het antisempas wordt niet correct bijgewerkt](#)

[3. Mail-beleid of berichtfilter](#)

[4. Beleid inzake Mail Flow](#)

[5. Bericht is spam](#)

Inleiding

In dit document worden vijf methoden beschreven waarmee e-mails van spam uw organisatie kunnen bereiken.

Methoden

1. Legitiem bericht / marketing e-mail

Het legitieme bericht is ingeslagen door de gebruiker of hun naam is verkocht aan een andere organisatie. In het eerste geval moet de gebruiker stappen ondernemen om het abonnement in de lijst op te heffen. Als het de laatste is, stuur het bericht dan opnieuw naar spam@access.ironport.com zodat de definities van spam wereldwijd kunnen worden bijgewerkt, waardoor de totale spamopnamesnelheid van uw ESA wordt verbeterd. Het in staat stellen van marketing mail bij het inkomende e-mailbeleid kan helpen de perceptie van dit bericht "marketing" over "Spam" veranderen.

2. Het antisempas wordt niet correct bijgewerkt

Anti-spam is uitgeschakeld of de functiesets is verlopen. Om te controleren of Anti-Spam een update geeft, ga naar **GUI > Security Services > IronPort Anti-Spam**. Binnen dit paneel dient u binnen de laatste 6 uur updates van de regels of de motor te zien. Ook vanuit dit tabblad aan de bovenkant kunt u ervoor zorgen dat de Anti-Spam-service is ingeschakeld. Voor het bekijken van de status Functie Belangrijkste status kunt u naar het tabblad Systeembeheer > Functiesleutel gaan om de status van de Anti-Spam-toets te controleren.

3. Mail-beleid of berichtfilter

Spam kan in uw organisatie komen als de anti-Spam veiligheidsmotor voor een specifieke zender of ontvanger per een klant Mail Policy is uitgeschakeld. Een andere manier om spamfiltering te overslaan is via berichtfilters (CLI: **filters** opdracht).

4. Beleid inzake Mail Flow

Een bericht wordt geclassificeerd met behulp van de ICID van het bericht. In deze situatie is het waarschijnlijk dat de optie Anti-Spam Security is uitgeschakeld, aangezien deze het Mail Policy overtreft. U kunt dit bepalen door te kijken naar de e-maillogs, in de logbestanden moet u eerst de ICID bekijken om te begrijpen in welke SenderGroup het bericht is geclassificeerd. Van daaruit onderzoek van het geassocieerde beleid van de Mail Flow. Als u een grote hoeveelheid ingangen in uw AllowList hebt, moet u misschien een aantal van de berichten bekijken die binnenkomen om te zien of zij gescand zijn door de AntiSpam motor. Open de kopregels van een bericht en zoek de kop X-IronPort-Spam, omdat deze kop is ingedrukt, betekent dit dat het bericht naar de machine is gegaan.

5. Bericht is spam

Het bericht is feitelijk spam. U hebt bevestigd dat het bericht is gescand door de anti-spammotor met behulp van de Berichttraceringsfunctie (zoek in het bericht dat u volgt "CASE"). Als de caseuitspraak negatief is en u meent dat het bericht spam is, stuurt u het oorspronkelijke bericht naar spam@access.ironport.com. Dit zou een geval kunnen zijn van een nieuwe Spam-dreiging die net werd uitgebracht of een oudere dreiging die opnieuw werd gemanipuleerd.

De verwerking van de Spam-inzendingen is zowel automatisch als handmatig proces en er is geen feedback voor uw specifieke inzending. Op elk punt kunt u contact opnemen met Cisco TAC en een evaluatie en respons aanvragen.