# SPF-configuratie en best-praktijken

## Inhoud



## Inleiding

Dit document beschrijft verschillende scenario's met Sender Policy Framework (SPF) op Cisco e-mail security applicatie (ESA).

## Voorwaarden

Cisco raadt u aan deze onderwerpen te kennen:

- Cisco ESA
- Alle versies van AsyncOS

## Wat is SPF?

Sender Policy Framework (SPF) is een eenvoudig e-mailvalideringssysteem dat bedoeld is om e-mailspoofing te detecteren door middel van een mechanisme dat ontvangende mail-uitwisselaars toestaat om te controleren of inkomende e-mail vanuit een domein wordt verzonden vanuit een host die door de beheerders van dat domein is geautoriseerd. De lijst van geautoriseerde verzendhosts voor een domein wordt gepubliceerd in de DNS-records van het Domain Name System (DNS) voor dat domein in de vorm van een speciaal geformatteerde TXT-record. E-mail spam en phishing gebruiken vaak vervalste adressen van zenders, zodat het publiceren en controleren van SPF records kan worden beschouwd als anti-spamtechnieken.

## Zal er veel impact zijn op de prestaties van de ESA's?

Vanuit het CPU-vooruitzicht zal er geen grote impact zijn op de prestaties. Door SPF-verificatie mogelijk te maken, worden echter meer DNS-vragen en DNS-verkeer gepubliceerd. Voor elk bericht kan het ESA 1-3 SPF DNS vragen moeten initiëren en dit zal leiden tot het eindigen van DNS cache eerder dan daarvoor. Daarom zal de ESA ook meer vragen voor de andere processen

opleveren.

Naast de vorige informatie zal de SPF-record een TXT-record zijn die groter kan zijn dan de normale DNS-records en extra DNS-verkeer kan veroorzaken.

## Hoe schakelt u de SPF in?

Deze instructies zijn afkomstig van de Advanced User Guide bij het instellen van een SFP-verificatie:

Zo schakelt SPF/System Independent Data Format (SIDF) in het standaardbeleid voor e-mailstromen:

1. Klik op **Mail Policies > Mail Flow Policy**.
2. Klik op **Standaardbeleidsparameters**.
3. In de standaardbeleidsparameters, bekijk de sectie **Beveiligingskenmerken**.
4. Klik in het gedeelte SPF/SIDF Verificatie op **Ja**.
5. Stel het conformiteitsniveau in (de standaardinstelling is SIDF-compatibel). Met deze optie kunt u bepalen welke standaard van de SPF- of SIDF-verificatie moet worden gebruikt. Naast de conformiteit met SIDF kunt u voor SIDF-compatibel kiezen, waarbij SPF en SIDF worden gecombineerd. Er zijn in de *eindgebruikershandleiding* meer informatie over de *conformiteitsniveaus* beschikbaar.
6. Als u een conformiteitsniveau van SIDF-compatibel kiest, moet u configureren of de verificatie een **passerresultaat** van de PRA-identiteit naar **geen** reduceert als er een Sender is: of beantwoord: kopregels in het bericht. U kunt deze optie voor beveiligingsdoeleinden kiezen.
7. Als u een conformiteitsniveau van SPF kiest, moet u configureren of een test uitvoeren tegen de HELO-identiteit. U kunt deze optie gebruiken om de prestaties te verbeteren door de HELO-toets uit te schakelen. Dit kan nuttig zijn omdat de spf-passeerde filterregel eerst de PRA of de MAIL VAN Identificaties controleert. Het apparaat voert alleen de HELO-controle uit op het niveau van overeenstemming van het SFP.

Om actie te ondernemen met betrekking tot de resultaten van de verificatie van het SFP kunt u een of meer inhoudfilter(s) toevoegen:

1. Maak een filter van de inhoud van de spf-status voor elk type van de SPF/SIDF-verificatie. Gebruik een naamgevingsconventie om het type verificatie aan te geven. Gebruik bijvoorbeeld **SPF-Passed** voor berichten die de SPF/SIDF-verificatie doorgeven, of **SPF-TempErr** voor berichten die niet werden doorgegeven vanwege een tijdelijke fout tijdens de verificatie. Zie de SF-status contentfilterregel in de GUI voor meer informatie over het maken van een filter voor de spf-status.
2. Nadat u een aantal door SPF/SIDF gecontroleerde berichten hebt verwerkt, klikt u op **Monitor > Contentfilters** om te zien hoeveel berichten elk van de door SPF/SIDF gecontroleerde contentfilters hebben geactiveerd.

## Wat betekent "Helo Test" op en uit? Wat zal er gebeuren als de Helo-test op een bepaald gebied faalt?

Als u een conformiteitsniveau van SPF kiest, moet u configureren of een test uitvoeren tegen de HELO-identiteit. U kunt deze optie gebruiken om de prestaties te verbeteren door de HELO-toets uit te schakelen. Dit kan nuttig zijn omdat de spf-passeerde filterregel eerst de PRA of de MAIL VAN Identificaties controleert. Het apparaat voert alleen de HELO-controle uit op het niveau van overeenstemming van het SFP.

### Valid SPF records

Om de SPF HELO-controle over te gaan, zorg ervoor dat u een SPF-record voor elke verzendende MTA (gescheiden van het domein) opneemt. Als u deze record niet opneemt, zal de HELO-controle waarschijnlijk resulteren in een **Geen** oordeel over de HELO-identiteit. Als u opmerkt dat SPF-zenders naar uw domein een groot aantal **Geen** vonnissen teruggeven, hebben deze zenders mogelijk geen SPF-record voor elke verzendende MTA opgenomen.

Het bericht wordt afgeleverd indien er geen bericht/contentfilters zijn geconfigureerd. Opnieuw kunt u bepaalde acties uitvoeren met Berichtings-/contentfilters voor elk SPF/SIDF-vonnis.

## Wat is de beste manier om het voor slechts één extern domein mogelijk te maken?

Om SPF voor een bepaald domein in staat te stellen, zou u een nieuwe sendergroep met een poststroombeleid kunnen moeten definiëren dat SPF heeft ingeschakeld; maak vervolgens filters zoals eerder vermeld.

## Kunt u een SPF-controle voor vermoedelijk spam inschakelen?

Cisco Anti-Spam houdt rekening met een groot aantal factoren bij het berekenen van spamscores. Een controleerbare registratie van het SFP kan de spamscore verlagen, maar er is nog een kans om die berichten als vermoedelijk spam te vangen.

De best mogelijke oplossing zou zijn om het IP-adres van de afzender toe te staan of een berichtfilter te maken om de controle van de spam met meerdere voorwaarden (Remote-ip, mail-van, X-skipspamcheck header, enz.) over te slaan. De header kan door de verzendende server worden toegevoegd om één type berichten van anderen te identificeren.

## Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- E-mailverificatie Best Practices - Delivery SPF/DKIM/DMARC
- Technische ondersteuning en documentatie – Cisco Systems