Contenu

Introduction

Ce document décrit différents scénarios avec Sender Policy Framework (SPF) sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Prerequiste

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ESA
- Toutes les versions d'AsyncOS

Quelle est SPF ?

Sender Policy Framework (SPF) est un système simple de validation d'email conçu pour détecter la mystification d'email en fournissant un mécanisme pour permettre recevoir des messagers pour vérifier que la messagerie entrante d'un domaine est envoyée d'un hôte autorisé par les administrateurs de ce domaine. La liste d'hôtes expéditeur autorisés pour un domaine est éditée dans les enregistrements de Système de noms de domaine (DNS) pour ce domaine sous forme d'enregistrement particulièrement formaté TXT. Des adresses d'expéditeur modifiées par utilisation de Spam et de phishing d'email souvent, ainsi l'édition et vérifier des enregistrements SPF peuvent être considérés des techniques d'anti-Spam.

Y aura-t-il beaucoup d'incidence des performances sur l'ESAs ?

De la prospect CPU, il n'y aura pas incidence des performances énorme. Cependant, l'activation de la vérification SPF augmentera les requêtes DNS et le trafic DNS de nombre. Pour chaque message, l'ESA pourrait devoir initier 1-3 requêtes DNS SPF et ceci aura comme conséquence le cache DNS de expiration plus tôt puis avant. Par conséquent, l'ESA génèrera plus de requêtes pour les autres processus aussi bien.

En plus des informations précédentes, l'enregistrement SPF sera un enregistrement .TXT qui peut être plus grand puis les enregistrements DNS normaux et pourrait entraîner du trafic DNS supplémentaire.

Comment activez-vous la SPF ?

Ces instructions sont du guide utilisateur anticipé sur installer la vérification SPF :

Pour activer le format des données indépendant SPF/System (SIDF) sur la stratégie par défaut de mailflow :

1. **Stratégies de messagerie de** clic **> stratégie de flux de courrier**.
2. **Paramètres de stratégie par défaut de** clic.
3. Dans les paramètres de stratégie par défaut, visualisez la section de **fonctionnalités de sécurité**.
4. Dans la section de vérification SPF/SIDF, cliquez sur **oui**.
5. Placez le niveau de la conformité (le par défaut est SIDF-compatible). Cette option te permet pour déterminer quel niveau de la vérification SPF ou SIDF à l'utiliser. En plus de la conformité SIDF, vous pouvez choisir SIDF-compatible, qui combine la SPF et le SIDF.
6. Si vous choisissez un niveau de conformité de SIDF-compatible, configurez si la vérification déclassifie un résultat de **passage de l'**identité PRA à **aucun** s'il y a Renvoyer-expéditeur : ou Renvoyer-de : en-têtes actuelles dans le message. Vous pourriez choisir cette option pour des raisons de sécurité.
7. Si vous choisissez un niveau de conformité de SPF, configurez si réaliser un essai contre l'identité d'HÉLICOPTÈRE. Vous pourriez utiliser cette option d'améliorer la représentation en désactivant le contrôle d'HÉLICOPTÈRE. Ceci peut être utile, parce que la règle de filtrage SPF-passée vérifie le PRA ou la MESSAGERIE des identités d'abord. L'appliance exécute seulement l'HÉLICOPTÈRE vérifient le niveau de conformité SPF.

Pour agir sur des résultats de vérification SPF, ajoutez s'il vous plaît les filtres satisfaits :

1. Créez un filtre de contenu de SPF-état pour chaque type de vérification SPF/SIDF. Utilisez

une convention nommante pour indiquer le type de vérification. Par exemple, l'utilisation SPF-**a passé** pour les messages qui passent la vérification SPF/SIDF, ou la **SPF-TempErr** pour les messages qui n'ont pas été passés à en raison d'une erreur passagère pendant la vérification. Pour des informations sur créer un filtre de contenu de SPF-état, voir la règle de filtrage satisfaite de SPF-état dans le GUI.

2. Après que vous traitiez un certain nombre de messages SPF/SIDF-verified, to cliquer sur Monitor **> des filtres de contenu** pour voir combien de messages ont déclenché chacun des filtres de contenu SPF/SIDF-verified.

Que le « test d'hélicoptère » marche-arrêt signifie-t-il ? Que se produira si le test d'hélicoptère échoue d'un certain domaine ?

Si vous choisissez un niveau de conformité de SPF, configurez si réaliser un essai contre l'identité d'HÉLICOPTÈRE. Vous pourriez utiliser cette option d'améliorer la représentation en désactivant le contrôle d'HÉLICOPTÈRE. Ceci peut être utile parce que la règle de filtrage SPF-passée vérifie le PRA ou la MESSAGERIE des identités d'abord. L'appliance exécute seulement l'HÉLICOPTÈRE vérifient le niveau de conformité SPF.

Enregistrements valides SPF

Pour passer le contrôle d'HÉLICOPTÈRE SPF, assurez-vous que vous incluez un enregistrement SPF pour chaque MTA de envoi (séparé du domaine). Si vous n'incluez pas cet enregistrement, le contrôle d'HÉLICOPTÈRE aura vraisemblablement comme conséquence un **aucun** verdict pour l'identité d'HÉLICOPTÈRE. Si vous notez que les expéditeurs SPF à votre domaine renvoient un nombre élevé d'**aucun des** verdicts, ces expéditeurs ont pu ne pas avoir inclus un enregistrement SPF pour chaque MTA de envoi.

Le message sera fourni s'il n'y a aucun filtre de message/contenu configuré. De nouveau, vous pouvez prendre certaines mesures utilisant des filtres de message/contenu pour chaque verdict SPF/SIDF.

Quelle est la meilleure manière de l'activer pour seulement un domaine externe ?

Pour activer la SPF pour certain domaine, vous pourriez devoir définir un nouveau sendergroup avec une stratégie de flux de courrier qui a la SPF activée ; créez alors les filtres comme mentionné précédemment.

Pouvez-vous activer une SPF vérifiez-vous le Spam suspecté ?

L'anti-Spam de Cisco considère énormément de facteurs tout en calculant des scores de Spam. Avoir l'enregistrement vérifiable SPF peut réduire le score de Spam mais il reste possibilité d'obtenir ces messages attrapés en tant que Spam suspecté.

La meilleure solution serait au whitelist l'adresse IP d'expéditeur OU créerait un filtre de message pour ignorer le spamcheck dans de plusieurs conditions (en-tête distant-IP, messagerie-de, de X-skipspamcheck, etc.). L'en-tête peut être ajoutée par le serveur de envoi pour identifier un type de messages d'autres.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems