Configuration SPF et meilleures pratiques

Contenu

Introduction

Ce document décrit différents scénarios avec le cadre de stratégie de l'expéditeur (SPF) sur l'appliance de sécurité de la messagerie Cisco (ESA).

Conditions préalables

Cisco vous recommande de connaître les sujets suivants :

- Cisco ESA
- Toutes les versions d'AsyncOS

Qu'est-ce que SPF ?

Sender Policy Framework (SPF) est un système simple de validation des e-mails conçu pour détecter l'usurpation d'e-mails en fournissant un mécanisme permettant aux échangeurs de messages de réception de vérifier que le courrier entrant d'un domaine est envoyé par un hôte autorisé par les administrateurs de ce domaine. La liste des hôtes d'envoi autorisés pour un domaine est publiée dans les enregistrements DNS (Domain Name System) de ce domaine sous la forme d'un enregistrement TXT spécialement formaté. Le courrier indésirable et l'hameçonnage utilisent souvent des adresses d'expéditeur falsifiées, de sorte que la publication et la vérification des enregistrements SPF peuvent être considérées comme des techniques antispam.

Y aura-t-il un impact considérable sur les performances des AES ?

Du point de vue du processeur, il n'y aura pas d'impact énorme sur les performances. Cependant, l'activation de la vérification SPF augmentera le nombre de requêtes DNS et le trafic DNS. Pour chaque message, l'ESA peut devoir initier 1 à 3 requêtes DNS SPF, ce qui entraînera l'expiration

du cache DNS plus tôt qu'auparavant. Par conséquent, l'ESA va générer plus de requêtes pour les autres processus également.

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

Comment activez-vous le SPF ?

Ces instructions proviennent du Guide de l'utilisateur avancé sur la configuration de la vérification SPF :

Pour activer le format SIDF (System Independent Data Format) SPF/System sur la stratégie de flux de messagerie par défaut :

1. Cliquez sur **Politiques de messagerie > Politique de flux de messagerie**.
2. Cliquez sur **Paramètres de stratégie par défaut**.
3. Dans les paramètres de stratégie par défaut, affichez la section **Fonctions de sécurité**.
4. Dans la section Vérification SPF/SIDF, cliquez sur **Oui**.
5. Définissez le niveau de conformité (la valeur par défaut est compatible SIDF). Cette option vous permet de déterminer la norme de vérification SPF ou SIDF à utiliser. Outre la conformité SIDF, vous pouvez choisir SIDF-compatible, qui combine SPF et SIDF. Les détails des niveaux de conformité sont disponibles dans le *Guide de l'utilisateur final.*
6. Si vous choisissez un niveau de conformité compatible SIDF, configurez si la vérification dégrade un résultat **Pass** de l'identité PRA à **None** s'il existe Resent-Sender : ou Rent-De : en-têtes présents dans le message. Vous pouvez choisir cette option à des fins de sécurité.
7. Si vous choisissez un niveau de conformité SPF, configurez si vous devez effectuer un test sur l'identité HELO. Vous pouvez utiliser cette option pour améliorer les performances en désactivant le contrôle HELO. Cela peut être utile car la règle de filtre spf-passée vérifie d'abord les identités PRA ou MAIL FROM. L'appliance effectue uniquement la vérification HELO pour le niveau de conformité SPF.

Pour prendre des mesures sur les résultats de la vérification SPF, ajoutez des filtres de contenu :

1. Créez un filtre de contenu d'état spf pour chaque type de vérification SPF/SIDF. Utilisez une convention d'attribution de noms pour indiquer le type de vérification. Par exemple, utilisez **SPF-Passed** pour les messages qui réussissent la vérification SPF/SIDF ou **SPF-TempErr** pour les messages qui n'ont pas été transmis en raison d'une erreur transitoire pendant la vérification. Pour plus d'informations sur la création d'un filtre de contenu d'état spf, consultez la règle de filtre de contenu d'état spf dans l'interface utilisateur graphique.
2. Après avoir traité certains messages vérifiés SPF/SIDF, cliquez sur **Monitor > Content Filters** pour voir combien de messages ont déclenché chacun des filtres de contenu vérifiés SPF/SIDF.

Qu'est-ce que « Helo Test » on and off signifie ? Que se passe-t-il si le test Helo échoue à partir d'un domaine donné ?

Si vous choisissez un niveau de conformité SPF, configurez si vous devez effectuer un test sur l'identité HELO. Vous pouvez utiliser cette option pour améliorer les performances en désactivant le contrôle HELO. Cela peut être utile car la règle de filtre spf-passée vérifie d'abord les identités PRA ou MAIL FROM. L'appliance effectue uniquement la vérification HELO pour le niveau de conformité SPF.

Enregistrements SPF valides

Pour réussir la vérification HELO SPF, assurez-vous d'inclure un enregistrement SPF pour chaque MTA d'envoi (distinct du domaine). Si vous n'incluez pas cet enregistrement, la vérification HELO entraînera probablement un verdict **Aucun** pour l'identité HELO. Si vous remarquez que les expéditeurs SPF de votre domaine retournent un nombre élevé de verdicts **Aucun**, ces expéditeurs peuvent ne pas avoir inclus d'enregistrement SPF pour chaque MTA d'envoi.

Le message sera remis s'il n'y a aucun filtre de message/contenu configuré. De nouveau, vous pouvez effectuer certaines actions à l'aide de filtres de message/contenu pour chaque verdict SPF/SIDF.

Quel est le meilleur moyen de l'activer pour un seul domaine externe ?

Pour activer le SPF pour un domaine donné, vous devrez peut-être définir un nouveau groupe d'expéditeurs avec une stratégie de flux de courrier dont le SPF est activé ; puis créez des filtres comme indiqué précédemment.

Pouvez-vous activer une vérification SPF pour détecter les spams suspectés ?

Cisco Anti-Spam prend en compte de nombreux facteurs lors du calcul des scores de spam. Le fait d'avoir un enregistrement SPF vérifiable peut réduire le score de spam, mais il est toujours possible de faire passer ces messages comme spam suspecté.

La meilleure solution serait d'autoriser l'adresse IP de l'expéditeur OU de créer un filtre de messages pour ignorer le spam avec plusieurs conditions (ip distante, courrier électronique, en-tête X-skipspamcheck, etc.). L'en-tête peut être ajouté par le serveur émetteur pour identifier un type de messages provenant d'autres.

Informations connexes

- Cisco Email Security Appliance - Guides de l'utilisateur final
- Meilleures pratiques d'authentification de la messagerie - Déploiement de SPF/DKIM/DMARC
- Support et documentation techniques - Cisco Systems