Configuration des paramètres antispam ESA pour améliorer la détection du spam

Table des matières

[Introduction](#)

[Configuration de base](#)

[Activer SBNP](#)

[Raison d'être SBRS](#)

Introduction

Ce document décrit comment améliorer l'efficacité de l'anti-spam du dispositif de sécurité de la messagerie Cisco (ESA) et réduire le spam qui contourne le filtrage.

Problème

Les messages indésirables contournent le filtrage ESA ou ne sont pas traités comme prévu par les politiques de messages entrants.

Environnement

- Appliance de sécurisation de la messagerie Cisco (ESA) avec fonction antispam activée et clé de fonction antispam valide.
- Flux de messages entrants et sortants configurés sur des écouteurs distincts (recommandé pour les paramètres SenderBase).
- SenderBase Reputation Score (SBRS) et SenderBase Network Participation (SBNP) disponibles dans le déploiement.

Résolution

Suivez les procédures décrites dans ces sections pour vérifier le fonctionnement de l'antispam, confirmer l'analyse, régler les seuils et optimiser SBRS et les stratégies de flux de messages.

Motif

- Antispam désactivé, clé de fonction manquante ou mises à jour de règle non actualisées.
- Les messages contournent l'analyse en raison des listes d'autorisation, des filtres de messages ou des limites de taille d'analyse.
- Stratégies HAT (Permissive Host Access Table) ou seuils SBRS.
- Augmentation du volume de spam au fil du temps.

Configuration

Procédure 1 : Vérifier que l'antispam est activé

1.- Assurez-vous que tous les enregistrements MX (Mail Exchange) (y compris les enregistrements MX de priorité inférieure) relaient le courrier via l'ESA.

2.- Vérifiez que l'appliance dispose d'une clé de fonction antispam valide.

3.- Assurez-vous que l'antispam est activé pour toutes les stratégies de messages entrants appropriées.

Procédure 2 : Vérifier les mises à jour des règles antispam

Accédez à Security Services > Anti-Spam et vérifiez que les horodatages de mise à jour de règle les plus récents se situent dans les 2 dernières heures.

Procédure 3 : Vérifier que les messages sont analysés par l'antispam

1.- Recherchez l'en-tête X-IronPort-Anti-Spam-Result dans un échantillon de messages de spam en absence :

2.- Si l'en-tête est manquant, procédez comme suit :

- Vérifiez qu'aucune entrée de liste autorisée ni aucun filtre ne contourne l'analyse du spam.
- Vérifiez que les messages ne contournent pas l'analyse en raison de la taille maximale d'analyse des messages (262144 octets par défaut).
- Vérifiez chaque entrée de la table d'accès aux hôtes (HAT) et confirmez que spam_check=on est défini pour les stratégies de flux de messages entrants.

- Vérifiez les filtres de messages et assurez-vous qu'aucun filtre n'utilise skip-spamcheck sauf si nécessaire.
- Utilisez un exemple de spam récent (heure, date, destinataire) et consultez mail_logs pour confirmer qu'Anti-Spam a renvoyé un verdict négatif.

Procédure 4 : Vérifier les actions pour les messages positifs pour le spam

Passez en revue les stratégies de messages entrants et vérifiez que les messages de spam avéré et suspecté sont abandonnés ou mis en quarantaine dans la stratégie par défaut, et que les autres stratégies héritent du comportement par défaut ou le remplacent intentionnellement.

Procédure 5 : Régler les seuils de spam (facultatif)

1.- Réduisez le seuil de spam positif à 80 (90 par défaut) lorsque les faux positifs sont acceptables à un certain seuil.

2.- Réduisez le seuil de spam suspecté à 40 (50 par défaut) lorsque les faux positifs sont acceptables au seuil suspect.

3.- Lorsque les plaintes sont limitées à un sous-ensemble de destinataires, créer une politique de messagerie distincte pour les destinataires ayant des seuils inférieurs.

Procédure 6 : Optimiser les paramètres SBRS et les stratégies HAT

1.- Ajuster les plages SBRS pour les groupes d'expéditeurs bloqués et suspects en fonction de la tolérance organisationnelle pour les faux positifs.

2.- Lorsque la stratégie nécessite une validation plus stricte, ajoutez SBRS none à un groupe d'expéditeurs suspects qui utilise une stratégie limitée.

3.- Définissez le nombre maximal de destinataires par heure sur 5 pour la stratégie limitée.

4.- Créez éventuellement plusieurs stratégies limitées avec différentes limites de destinataire par heure pour différentes plages SBRS.

Procédure 7 : Activer la vérification de l'expéditeur pour le flux de courrier limité

1.- Lorsque la stratégie nécessite une validation plus stricte, ajoutez des expéditeurs dont le

système de noms de domaine (DNS) est inexistant ou mal configuré à un groupe d'expéditeurs suspects.

2.- Considérez une stratégie de flux de messagerie distincte qui renvoie une réponse 4xx personnalisée indiquant pourquoi les messages sont rejetés.

Procédure 8 : Activer l'acceptation LDAP et Directory Harvest Attack Protection

1.- Activer l'acceptation LDAP (Lightweight Directory Access Protocol) pour réduire le courrier indésirable envoyé à des destinataires non valides.

2.- Si l'acceptation LDAP est activée, configurez la protection contre les attaques par collecte d'annuaire (DHAP) pour chaque écouteur entrant avec un maximum de tentatives non valides entre 5 et 10 par IP.

Procédure 9 : Activer les dictionnaires de contenu (facultatif)

L'ESA comprend deux dictionnaires de contenu : profanity.txt et sex_content.txt. Appliquez ces dictionnaires uniquement lorsque cela est nécessaire, car ils peuvent augmenter le nombre de faux positifs.

Procédure 10 : Signaler les messages mal classés

Soumettez les faux positifs et les faux négatifs au TAC Cisco pour analyse.

Procédure 11 : Désactiver SBRS pour l'analyse sortante

Activer SBNP

1.- Assurez-vous que les messages entrants et sortants se trouvent sur des écouteurs distincts.

2.- Désactiver les recherches SenderBase pour les e-mails sortants. Accédez à Réseau > Écouteurs. Sélectionnez l'écouteur sortant. Cliquez sur Avancé. Désactivez la case à cocher Utiliser le profilage IP SenderBase.

SenderBase Network Participation (SBNP) peut améliorer l'efficacité des filtres de réputation, des

filtres antispam et des filtres contre les attaques de virus. SBNP n'a pas d'impact notable sur les performances lorsque l'antispam est activé et sécurisé.

Remarque : Le volume de spam que votre entreprise reçoit change avec le temps. Il est possible qu'un plus grand nombre de courriers indésirables transitent par les ESA simplement parce que l'entreprise reçoit plus de courriers indésirables que par le passé. Suivez ce comportement dans le temps en consultant la page Présentation des messages entrants et en ajoutant les éléments de ligne arrêtés par filtrage par réputation et messages indésirables détectés.

Raison d'être SBRS

La principale préoccupation concernant les faux positifs est que les e-mails importants peuvent être perdus. Dans ce contexte, la mise en quarantaine ou l'abandon d'e-mails positifs pour le spam peut être problématique. Si un e-mail légitime est envoyé dans un dossier de quarantaine ou de spam, une recherche proactive est nécessaire pour identifier que le courrier légitime a été classé comme spam.

En revanche, les listes de blocage et les e-mails à débit limité sont bloqués de telle sorte que l'expéditeur en est immédiatement averti. Si cet expéditeur n'est pas un spammeur, il trouvera probablement un autre moyen d'établir un contact. En fait, en tant que stratégie globale, le blocage par défaut, puis l'acceptation de partenaires de confiance sur demande, est une meilleure position pour certaines entreprises.

La limitation, si elle est correctement définie, affecte rarement, voire jamais, les partenaires, mais fournit une protection contre les domaines infectés par des virus. La limitation est également rebutante pour les spammeurs. Une technique de spam connue consiste à acheter un grand nombre d'adresses IP, à générer suffisamment d'e-mails corrects pour obtenir un score SBRS correct, puis à commencer à envoyer du spam. Une plage de listes suspectes plus large intercepte le spam, limite les dommages qu'il cause et peut éventuellement les amener à cesser d'envoyer du spam à votre domaine.

Autres informations utiles

- Comment les Scores de réputation SenderBase (SBRS) sont-ils déterminés et que signifient-ils ?

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.