Quelles sont les meilleures pratiques d'utilisation de SenderBase ?

Table des matières

Introduction

Quelles sont les meilleures pratiques d'utilisation de SenderBase ?

Implémentation de la limitation ou du blocage SenderBase

Informations connexes

Introduction

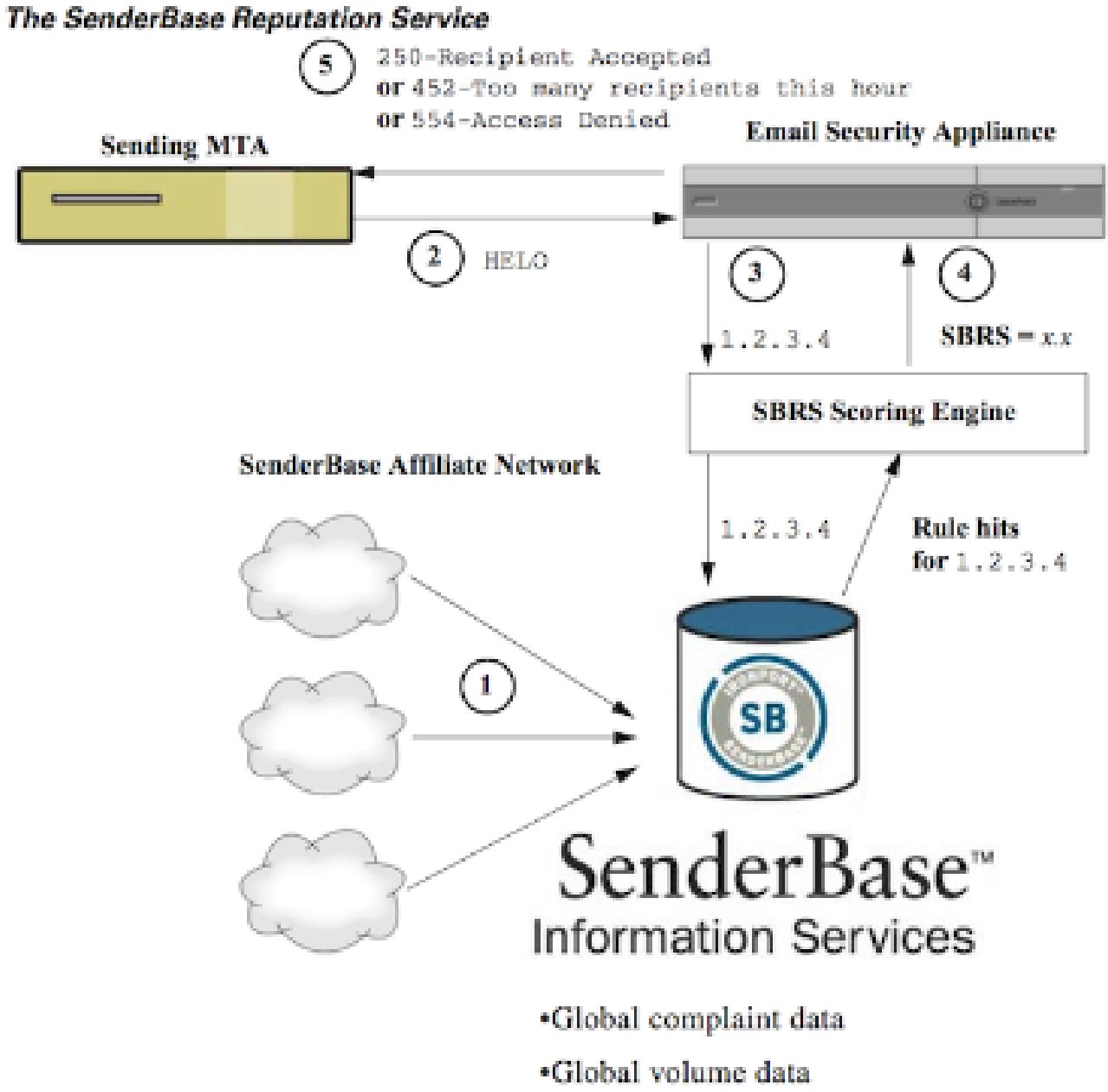
Ce document décrit les meilleures pratiques d'utilisation de SenderBase.

Quelles sont les meilleures pratiques d'utilisation de SenderBase ?

Le service de réputation SenderBase (SBRS) offre un moyen précis et flexible de rejeter ou d'étrangler les systèmes suspectés de transmettre du spam en fonction de l'adresse IP de connexion de l'hôte distant. SBRS renvoie un score basé sur la probabilité qu'un message provenant d'une source donnée soit du spam, allant de -10 (spam avéré) à +10 (spam avéré). Bien que SBRS puisse être utilisé comme solution anti-spam autonome, il est plus efficace lorsqu'il est associé à un analyseur anti-spam basé sur le contenu.

Les scores SenderBase peuvent être utilisés dans la table d'accès aux hôtes (HAT) d'un écouteur SMTP pour mapper les connexions SMTP entrantes à différents groupes d'expéditeurs. Chaque groupe d'expéditeurs est associé à une stratégie qui affecte la manière dont le courrier électronique entrant est traité. La chose la plus courante à faire avec les scores SenderBase est soit de rejeter entièrement le courrier électronique, soit de limiter l'expéditeur suspecté de courrier indésirable.

Vous pouvez utiliser les scores SBRS dans le TAH pour rejeter ou limiter les e-mails. Vous pouvez également créer des filtres de messages pour spécifier des « seuils » pour les scores SBRS afin d'agir sur les messages traités par le système. Le schéma ci-dessous décrit brièvement comment les scores SBRS peuvent être utilisés pour bloquer ou étrangler les expéditeurs suspectés :



1. Les filiales SenderBase envoient des données globales en temps réel.
2. L'envoi de MTA ouvre la connexion avec l'appliance.
3. L'appliance vérifie les données globales pour l'adresse IP de connexion.
4. Le service de réputation SenderBase calcule la probabilité que ce message soit du spam et attribue un score de réputation SenderBase.
5. L'appliance renvoie la réponse (rejet de l'e-mail ou limitation de l'expéditeur) en fonction du score de réputation SenderBase.

La façon dont vous utilisez les scores SBRS dépend du niveau d'agressivité que vous souhaitez avoir lors du pré-filtrage des e-mails. L'appliance de sécurisation de la messagerie (ESA) propose trois stratégies différentes pour la mise en oeuvre de SenderBase :

- Conservateur : Une approche prudente consiste à bloquer les messages dont le score de réputation SenderBase est inférieur à -7,0, à réguler entre -7,0 et -2,0, à appliquer la stratégie par défaut entre -2,0 et +6,0 et à appliquer la stratégie approuvée pour les

messages dont le score est supérieur à +6,0. Cette approche garantit un taux de faux positifs proche de zéro tout en améliorant les performances du système.

- Modéré : Une approche modérée consiste à bloquer les messages dont le score de réputation SenderBase est inférieur à -4,0, à réguler entre -4,0 et 0, à appliquer la stratégie par défaut entre 0 et +6,0 et à appliquer la stratégie approuvée pour les messages dont le score est supérieur à +6,0. L'utilisation de cette approche garantit un très faible taux de faux positifs tout en améliorant les performances du système (car un plus grand nombre de messages est détourné du traitement antispam).
- Agressif : Une approche agressive consiste à bloquer les messages dont le score de réputation SenderBase est inférieur à -1,0, à réguler entre -1,0 et 0, à appliquer la stratégie par défaut entre 0 et +4,0 et à appliquer la stratégie approuvée pour les messages dont le score est supérieur à +4,0. Cette approche peut entraîner des faux positifs ; toutefois, cette approche optimise les performances du système en éloignant le plus grand nombre de messages du traitement antispam.

Le tableau ci-dessous résume ces trois politiques :

Approche	Caractéristiques	Liste D'Admissibilité	Liste De Blocage	Suspecteur	Liste Inconnue
		Plage de scores de réputation de base des expéditeurs :			
Conservateur	Faux positifs proches de zéro, meilleures performances	7 à 10	-10 à -4	-4 à -2	-2 à 7
Modéré (par défaut)	Très peu de faux positifs, hautes performances	Les scores de réputation de base des expéditeurs ne sont pas utilisés.	-10 à -3	-3 à -1	-1 à +10
Agressif	Quelques faux positifs, performances maximales Cette option éloigne le plus grand nombre de messages du traitement antispam.	4 à 10	-10 à -2	-2 à -1	-1 à 4
Toutes les approches		Stratégie de flux de messagerie :			
		Fiable	Bloqué	Limité	Accepté

Implémentation de la limitation ou du blocage SenderBase

La meilleure façon d'utiliser les scores SenderBase consiste à suivre une méthodologie simple en 2 parties. Tout d'abord, vous décidez de votre stratégie (par exemple, vous pouvez commencer par la stratégie « Conservateur » ci-dessus) et la mapper aux groupes d'expéditeurs. Ensuite, vous mappez ces groupes d'expéditeurs à la stratégie de votre choix. L'ESA a déjà créé une matrice de groupes d'expéditeurs et de stratégies de flux de messages qui peut servir de modèle pour votre implémentation de SBRS.

Pour implémenter la limitation SenderBase basée sur la stratégie par défaut, vous allez modifier les quatre groupes d'expéditeurs (liste autorisée, liste de blocage, liste suspecte et liste inconnue) dans Politiques de messagerie > Vue d'ensemble de la table d'accès aux hôtes (HAT). Commencez par cliquer sur le groupe d'expéditeurs "Liste autorisée". Ensuite, à l'aide du menu déroulant dans l'onglet Expéditeurs, cliquez sur "Ajouter un expéditeur" avec "SenderBase Reputation Score (SBRS)" sélectionné. Une ligne SBRS sera ajoutée à la liste des expéditeurs. Complétez la plage de scores SBRS (dans ce cas, 6.0 à 10.0) et cliquez sur Envoyer.

La stratégie du groupe d'expéditeurs de la liste d'autorisation est « Approuvée ». Par défaut, cette stratégie ignore le traitement antispam, ce qui augmente les performances du système. Étant donné que les expéditeurs ayant un score SBRS très élevé ont très peu de chances d'envoyer du spam, cette étape à elle seule augmente le débit. Modifiez les trois groupes d'expéditeurs restants pour ajouter les scores SBRS, conformément au tableau ci-dessous :

Groupe d'expéditeurs	Plage de scores	Résultat
Liste D'Admissibilité	6 à 10	Les expéditeurs connus ne seront pas analysés
Liste Inconnue	-2 à +6	Les expéditeurs avec peu d'informations seront analysés normalement
Suspecteur	-7 à -2	Les expéditeurs ayant une mauvaise réputation seront fortement limités pour réduire la quantité de spam qu'ils peuvent envoyer
Liste De Blocage	-10 à -7	Les messages provenant de spammeurs connus seront rejetés au moment du SMTP avec une réponse 5xx

Lorsque vous avez terminé d'ajouter des plages de scores, n'oubliez pas de cliquer sur Valider les modifications. Lorsque vous ajoutez des règles d'évaluation SBRS à des groupes d'expéditeurs existants, placez-les en bas de la liste des expéditeurs de n'importe quel groupe. L'ordre est important lors de la définition de groupes d'expéditeurs dans la TAH d'un écouteur, car les groupes sont évalués de haut en bas, et dans chaque groupe, chaque règle est évaluée individuellement, de haut en bas. Dans une TAH, la première règle correspondant à un expéditeur sera utilisée pour sélectionner une règle. Si une connexion entrante d'un domaine expéditeur a un score SBRS défini et correspond à la plage d'une règle dans le TAH de l'écouteur, la stratégie de flux de messages sera appliquée, même si d'autres règles plus bas dans la liste des groupes d'expéditeurs peuvent également correspondre.

Si votre stratégie de placement des expéditeurs dans des groupes d'expéditeurs nécessite que toutes les règles non-SBRS soient évaluées avant que les scores SBRS soient pris en compte, vous pouvez simplement ajouter quatre nouveaux groupes d'expéditeurs à la fin de la liste des groupes d'expéditeurs existants spécifiquement pour la mise en correspondance de la stratégie SBRS avec leurs stratégies pertinentes.

Informations connexes

- Foire aux questions SenderBase
- Assistance et documentation techniques - Cisco Systems

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.