Quelles sont les meilleures pratiques pour utiliser SenderBase ?

Contenu

Introduction

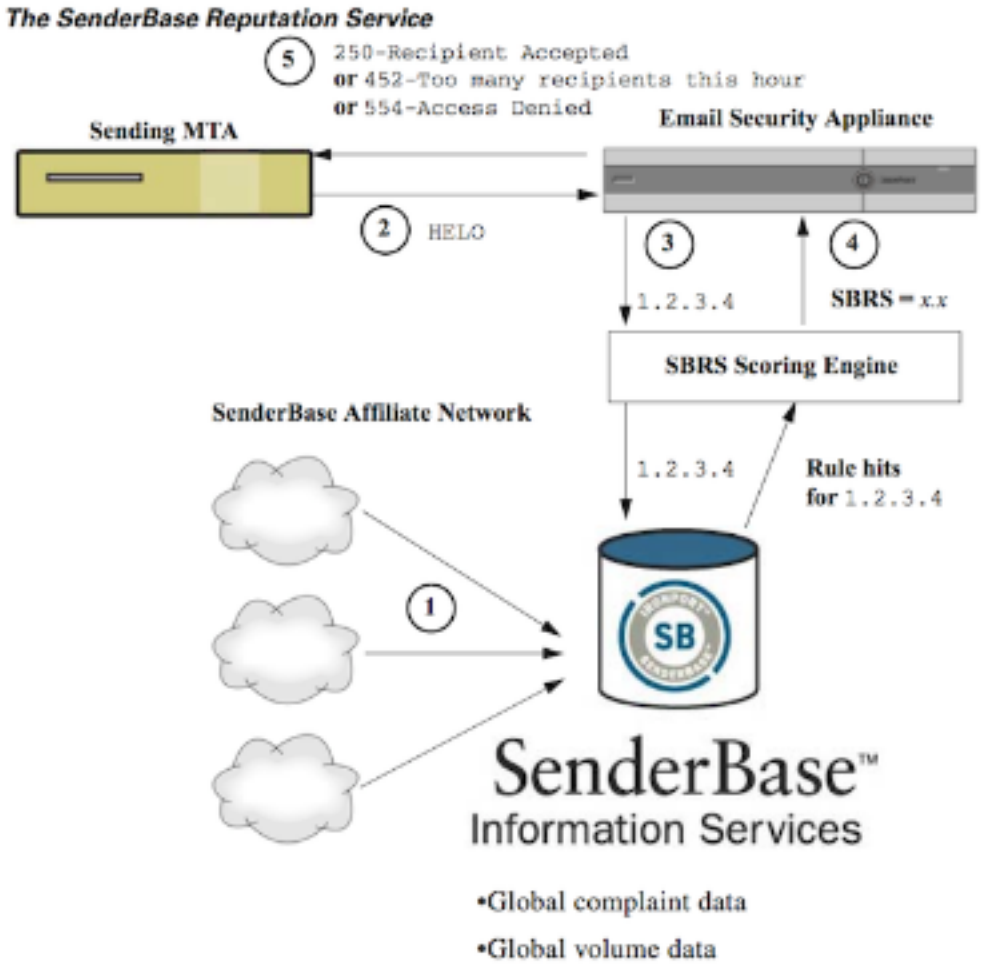
Ce document décrit les meilleures pratiques d'utilisation de SenderBase.

Quelles sont les meilleures pratiques pour utiliser SenderBase ?

Le service de réputation SenderBase (SBRS) offre une méthode précise et flexible pour rejeter ou limiter les systèmes soupçonnés de transmettre du courrier indésirable en fonction de l'adresse IP de connexion de l'hôte distant. Le SBRS renvoie un score basé sur la probabilité qu'un message d'une source donnée soit du spam, allant de -10 (certain comme spam) à +10 (certain comme non spam). Bien que SBRS puisse être utilisé comme solution antispam autonome, il est plus efficace lorsqu'il est combiné à un analyseur antispam basé sur le contenu.

Les scores SenderBase peuvent être utilisés dans la table d'accès hôte (HAT) sur un écouteur SMTP pour mapper les connexions SMTP entrantes à différents groupes d'expéditeurs. Chaque groupe d'expéditeurs lui a associé une stratégie qui affecte la manière dont les e-mails entrants sont traités. Les choses les plus courantes à faire avec les scores SenderBase sont soit de rejeter entièrement le courrier, soit de limiter l'expéditeur suspecté de spam.

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 présente un aperçu de la façon dont les scores SBRS peuvent être utilisés pour bloquer ou limiter les expéditeurs suspects :



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. SenderBase Reputation Service calcule la probabilité que ce message soit un 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 de l'agressivité que vous souhaitez avoir dans le pré-filtrage des e-mails. L'appliance de sécurité de la messagerie (ESA) propose trois stratégies différentes pour mettre en oeuvre SenderBase :

- **Conservateur** : Une approche prudente consiste à bloquer les messages dont le score de réputation SenderBase est inférieur à -7.0, régit entre -7.0 et -2.0, applique la stratégie par défaut entre -2.0 et +6.0 et applique la stratégie de confiance pour les messages dont le score est supérieur à +6.0. Cette approche garantit un taux faux positif 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, régit entre -4.0 et 0, applique la stratégie par défaut entre 0 et +6.0 et applique la stratégie de confiance pour les messages dont le score est supérieur à +6.0. L'utilisation de cette approche garantit un taux de faux positifs très faible tout en améliorant les performances du système (car plus de courrier est exclu du traitement antispam).
- **Agressif :** Une approche agressive consiste à bloquer les messages dont le score de réputation SenderBase est inférieur à -1,0, régit entre -1,0 et 0, applique la stratégie par

défaut entre 0 et +4,0 et applique la stratégie de confiance pour les messages dont le score est supérieur à +4,0. En utilisant cette approche, vous pourriez avoir des faux positifs ; toutefois, cette approche optimise les performances du système en éliminant le plus grand nombre de courriers du traitement antispam.

Le tableau ci-dessous résume ces trois politiques :

Approche	Caractéristiques	Liste des autorisations	Liste de blocage	Liste de suspicions	Inconnu
		Plage de scores de réputation de base de l'expéditeur :			
conservateur	Des faux positifs proches de zéro, de 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 de l'expéditeur ne sont pas utilisés.	-10 à -3	-3 à -1	-1 à +10
	Quelques faux positifs, performances maximales				
Agressif	Cette option permet de supprimer le plus grand nombre de courriers du traitement antispam.	4 à 10	-10 à -2	-2 à -1	-1 à 4
Toutes les approches		Stratégie de flux de messages : Fiable	Bloqué	Bouleversé	Accepté

Implémentation du blocage ou de la limitation SenderBase

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

Pour implémenter la limitation SenderBase en fonction de la stratégie par défaut, vous allez modifier les quatre groupes d'expéditeurs (Allowlist, Blocklist, Suspectlist et Unknown-list) à l'aide de Politiques de messagerie > Vue d'ensemble de la table d'accès hôte (HAT). Commencez par cliquer sur « Autoriser » le groupe d'expéditeurs. Ensuite, à l'aide du menu déroulant de l'onglet Expéditeurs, cliquez sur « Ajouter un expéditeur » avec « Score de réputation SenderBase (SBRS)" sélectionné. Cette opération ajoute une ligne SBRS à la liste des expéditeurs. Complétez la plage de scores SBRS (dans ce cas, de 6.0 à 10.0) et cliquez sur le bouton **Soumettre**.

La stratégie du groupe d'expéditeurs Allowlist est « Approuvée ». Par défaut, cette stratégie ignorera le traitement antispam, ce qui augmentera les performances du système. Comme les

expéditeurs ayant des scores SBRS très élevés sont très peu susceptibles d'envoyer du spam, cette seule étape augmentera le débit. Modifiez les trois autres groupes d'expéditeurs pour ajouter des scores SBRS, conformément au tableau ci-dessous :

Groupe d'expéditeurs	Plage de scores	Résultat
Liste des autorisations	6 à 10	Les bons expéditeurs connus ne seront pas analysés
Inconnu	-2 à +6	Les expéditeurs disposant de peu d'informations sont analysés normalement
Liste de suspicions	-7 à -2	Les expéditeurs dont la réputation est médiocre seront fortement limités pour réd le nombre de courriers indésirables qu'ils peuvent envoyer
Liste de blocage	-10 à -7	Les messages envoyés par des spammeurs connus seront rejetés au moment S 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 aux 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 des groupes d'expéditeurs dans le 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 un TAH, la première règle correspondant à un expéditeur est utilisée pour sélectionner une stratégie. Si une connexion entrante à partir d'un domaine émetteur a un score SBRS défini et correspond à la plage dans une règle du TAH du processus d'écoute, la politique de flux de courrier 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 exige que toutes les règles non SBRS soient évaluées avant que les scores SBRS ne 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 des stratégies SBRS avec leurs stratégies pertinentes.

Informations connexes

- SenderBase - Forum aux questions
- Support et documentation techniques - Cisco Systems