Quelles sont les pratiques recommandées pour l'usage de SenderBase ?

Contenu

Introduction

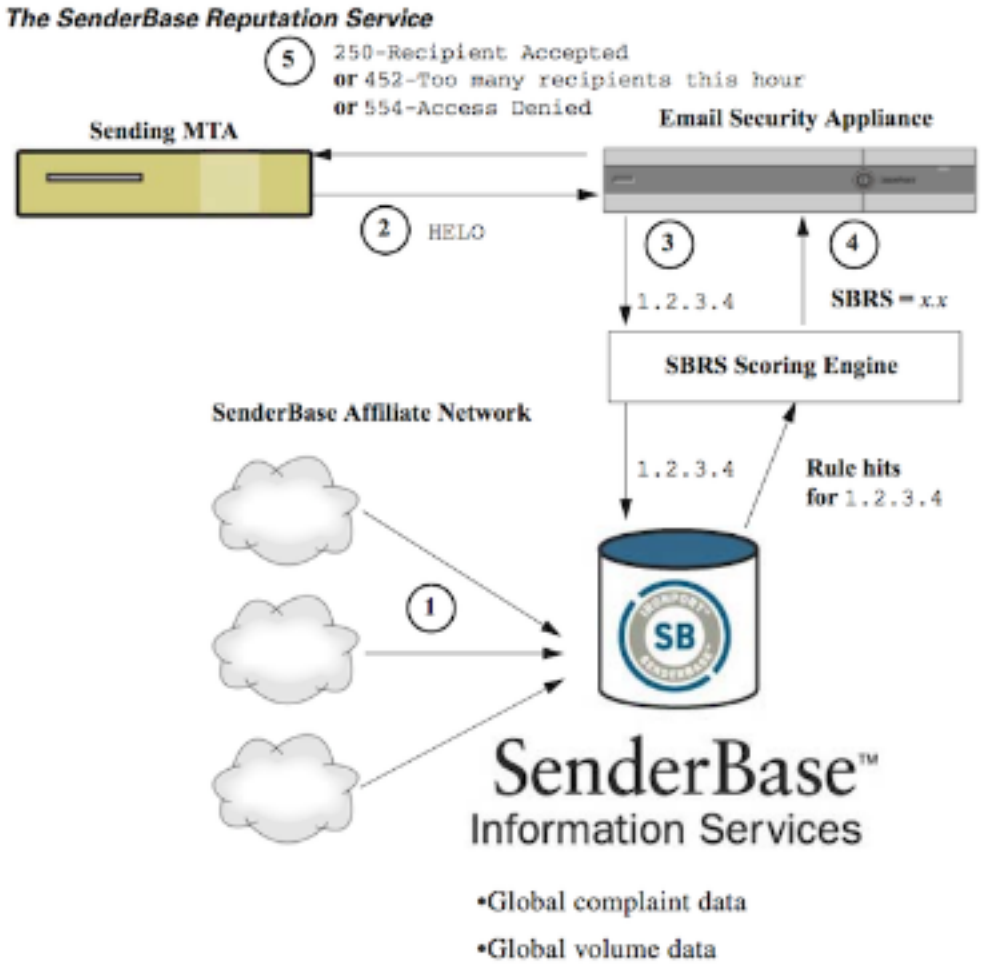
Ce document décrit les pratiques recommandées pour l'usage de SenderBase.

Quelles sont les pratiques recommandées pour l'usage de SenderBase ?

Le service de réputation de SenderBase (SBRS) fournit un précis, la façon flexible pour que vous rejetiez ou pour étranglez des systèmes suspectés transmettre le Spam basé sur l'adresse IP se connectante du serveur distant. Le SBRS renvoie un score basé sur la probabilité qu'un message d'une source donnée est Spam, s'étendant de -10 (sûr d'être Spam) par 0 à +10 (sûr de ne pas être Spam). Bien que SBRS puisse être utilisé comme solution autonome d'anti-Spam, il est le plus efficace une fois combiné avec un scanner basé sur contenu d'anti-Spam.

Des scores de SenderBase peuvent être utilisés dans le Tableau d'accès au hôte (CHAPEAU) sur un auditeur de SMTP pour tracer les connexions entrantes de SMTP à différents groupes d'expéditeur. Chaque groupe d'expéditeur a associé avec lui une stratégie qui affecte comment l'email entrant est manipulé. Les choses les plus communes à faire avec des scores de SenderBase sont à l'un ou l'autre de messagerie d'anomalie entièrement, ou pour étrangler l'expéditeur suspecté de Spam.

Vous pouvez employer des scores SBRS dans le CHAPEAU pour rejeter ou étrangler l'email. Vous pouvez également créer des filtres de message pour spécifier des « seuils » pour que les scores SBRS agissent plus loin sur des messages traités par le système. Le diagramme ci-dessous fournit un contour approximatif de la façon dont des scores SBRS peuvent être utilisés pour bloquer ou étrangler les expéditeurs suspectés :



1. Les filiales de SenderBase envoient le temps réel, des données globales.
2. L'envoi du MTA ouvre la connexion avec l'appliance.
3. L'appliance vérifie des données globales pour l'adresse IP se connectante.
4. Le service de réputation de SenderBase calcule la probabilité que ce message est Spam et assigne un score de réputations de SenderBase.
5. L'appliance renvoie la réponse (l'un ou l'autre rejetant l'email ou étranglant l'expéditeur) basée sur le score de réputation de SenderBase.

Comment vous utilisez les scores SBRS dépendront de la façon dont agressif vous voulez être dans l'email de pré-filtrage. L'appliance de sécurité du courrier électronique (ESA) offre trois stratégies différentes pour mettre en application SenderBase :

- **Conservateur** : Une approche prudente est de bloquer des messages avec un score de réputation de SenderBase inférieur que -7.0, d'étrangler entre -7.0 et -2.0, appliquer la stratégie par défaut entre -2.0 et +6.0, et d'appliquer la stratégie de confiance pour des messages avec un score plus grand que +6.0. Utilisant cette approche assure un débit zéro proche de faux positif tout en réalisant une meilleure performance du système.
- **Modéré :** Une approche modérée est de bloquer des messages avec un score de réputation de SenderBase inférieur que -4.0, d'étrangler entre -4.0 et 0, appliquer la stratégie par défaut entre 0 et +6.0, et d'appliquer la stratégie de confiance pour des messages avec un score plus grand que +6.0. Utilisant cette approche assure un débit très petit de faux positif tout en réalisant une meilleure performance du système (parce que plus de messagerie est manoeuvrée à partir de l'anti-Spam traitant).
- **Agressif :** Une approche agressive est de bloquer des messages avec un score de réputation de SenderBase inférieur que -1.0, d'étrangler entre -1.0 et 0, appliquer la stratégie par défaut

entre 0 et +4.0, et d'appliquer la stratégie de confiance pour des messages avec un score plus grand que +4.0. Utilisant cette approche, vous pourriez encourir quelques faux positifs ; cependant, cette approche maximise la performance du système en manoeuvrant la plupart de messagerie à partir du traitement d'anti-Spam.

Le graphique et la table ci-dessous récapitule ces trois stratégies :

Approach	Characteristics	Whitelist	Blacklist	Suspectlist	Unknownlist
		Sender Base Reputation Score range:			
Conservative	Near zero false positives, better performance	7 to 10	-10 to -4	-4 to -2	-2 to 7
Moderate (Installation default)	Very few false positives, high performance	Sender Base Reputation Scores are not used.	-10 to -3	-3 to -1	-1 to +10
Aggressive	Some false positives, maximum performance. This option shunts the most mail away from Anti-Spam processing.	4 to 10	-10 to -2	-2 to -1	-1 to 4
		Mail Flow Policy:			
All approaches		Trusted	Blocked	Throttled	Accepted

Mise en oeuvre de SenderBase étranglant ou blocage

La meilleure manière d'utiliser des scores de SenderBase signifie suivre une méthodologie simple et en deux parties. D'abord, vous décidez de votre stratégie (par exemple, vous pourriez commencer par la stratégie « conservatrice » ci-dessus) et tracez cette stratégie aux groupes d'expéditeur. Puis, vous tracez ces groupes d'expéditeur à la stratégie que vous voulez. L'ESA a déjà créé une matrice des groupes d'expéditeur et des stratégies de flux de courrier qui peuvent servir de modèle à votre implémentation de SBRS.

Pour implémenter l'étranglement de SenderBase basé sur la stratégie par défaut, vous éditerez les quatre groupes d'expéditeur (Whitelist, liste noire, Suspectlist, et Unknownlist) aux stratégies de messagerie > à l'aperçu de Tableau d'accès au hôte (CHAPEAU). Début en cliquant sur sur le groupe d'expéditeur de « Whitelist ». Puis, utilisant le menu déroulant dans l'onglet d'expéditeurs, cliquez sur en fonction « ajoutent l'expéditeur » avec « le score de réputation de SenderBase (SBRS) » sélectionné. Ceci ajoutera une ligne SBRS à la liste d'expéditeurs. Complétez votre plage de score SBRS (dans ce cas 6.0 10.0) et cliquez sur le bouton de **soumission**.

La stratégie pour le groupe d'expéditeur de Whitelist « est faite confiance. » Par défaut, cette stratégie ignorera l'anti-Spam traitant, qui augmentera la performance du système. Puisque les expéditeurs avec les scores très élevés SBRS sont fortement peu susceptibles d'envoyer le Spam, cette seule étape augmentera le débit. Éditez les trois groupes demeurants d'expéditeur pour ajouter des scores SBRS, selon la table ci-dessous :

Groupe d'expéditeur	Chaîne de score	Résultat
Whitelist	6 à 10	De bons expéditeurs connus ne seront pas balayés
Unknownlist	-2 à +6	Des expéditeurs avec peu d'informations seront balayés normalement
Suspectlist	-7 à -2	Des expéditeurs avec la réputation pauvre seront fortement étranglés pour rédu quantité de Spam qu'ils peuvent envoyer
Liste noire	-10 à -7	La messagerie des spammers connus sera rejetée au temps de SMTP avec un réponse 5xx

Quand vous êtes fait ajoutant des plages de score, n'oubliez pas de cliquer sur des « **modifications de validation**. » Quand vous ajoutez des règles de marquage SBRS aux groupes existants d'expéditeur, placez-les au bas de la liste d'expéditeurs dans n'importe quel groupe. Commandez les sujets en définissant des groupes d'expéditeur dans le CHAPEAU d'un auditeur, en tant que groupes sont évalués de haut en bas, et dans chaque groupe, chaque règle est évaluée individuellement, de haut en bas. Dans un CHAPEAU, la première règle appariant un expéditeur sera utilisée pour sélectionner une stratégie. Si une connexion entrante d'un domaine de envoi a un score défini SBRS et apparie la plage dans une règle dans le CHAPEAU de l'auditeur, la stratégie de flux de courrier sera appliquée, même si l'autre bas de règles autre dans la liste de groupes d'expéditeur pourrait également s'assortir.

Si votre stratégie pour mettre des expéditeurs dans des groupes d'expéditeur exige que toutes les règles de non-SBRS soient évaluées avant que des scores SBRS soient considérés, alors vous pouvez simplement ajouter quatre nouveaux groupes d'expéditeur à la fin de la liste de groupes existants d'expéditeur spécifiquement pour la stratégie SBRS s'assortissant avec leurs stratégies appropriées.

Informations connexes

- Forums aux questions de SenderBase
- Support et documentation techniques - Cisco Systems