SenderBase fonctionne-t-il correctement derrière NAT ?

Contenu

Introduction

Ce document décrit SenderBase et sa fonctionnalité derrière le Traduction d'adresses de réseau (NAT) pour l'appliance de sécurité du courrier électronique de Cisco (ESA).

SenderBase fonctionne-t-il correctement derrière NAT ?

SenderBase est un service basé sur IP de réputation qui assigne des scores du service de réputation de SenderBase (SBRS) aux adresses IP. Les scores de SenderBase s'étendent de -10 à +10, qui reflète la probabilité qu'une adresse IP de envoi essaye d'envoyer à Spam. Les scores fortement négatifs indiquent les expéditeurs qui sont très envoyer le Spam ; les scores fortement positifs indiquent les expéditeurs qui sont peu susceptibles d'envoyer le Spam.

L'auditeur de SMTP sur un ESA fait des requêtes de score SBRS utilisant des requêtes DNS basées sur l'adresse IP de la connexion TCP entrante. Si l'adresse IP que l'appliance d'email voit est la « vraie » adresse de l'expéditeur, alors SBRS fonctionne comme prévu.

> Remarque: Si un Pare-feu utilise NAT pour l'adresse IP source, il n'insérera pas une nouvelle en-tête de message qui contient l'adresse IP source d'origine. Sans en-tête de message qui contient l'adresse IP d'origine, la caractéristique entrante de relais ne fonctionnera pas. Sans informations d'en-tête pour l'adresse IP source, l'ESA ne peut pas déterminer l'adresse IP source d'origine.

La plupart des entreprises qui utilisent NAT ainsi masquent des adresses internes de l'Internet (ou parce qu'elles n'ont pas les adresses IP suffisantes à fonctionner sans fonction NAT ou NAPT). Dans des ces cas, SenderBase fonctionne avec succès parce que l'adresse IP de l'expéditeur externe n'est pas modifiée de quelque façon.

Quelques entreprises avec des topologies du réseau plus complexes font des connexions de traduction d'adresses réseau ou de proxy vers l'intérieur de leurs réseaux. Dans des ces cas, les requêtes de SenderBase ne fonctionneront pas correctement et devraient être désactivées sur l'auditeur entrant. (du CLI, le **listenerconfig > éditent > installé**.)

Si vous avez n'importe quel doute, que les adresses soient converties ou pas ou si des

connexions proxied, examinez simplement le fichier de mail_logs (utilisez une commande CLI telle que des **mail_logs de queue**). Ceci affiche te chaque connexion entrante à chaque auditeur, et te pourra rapidement voir si les adresses IP que l'ESA voit sont de l'Internet général ou pas.

> Remarque: Faites attention à regarder seulement des connexions aux auditeurs publics ou d'arrivée sur les logs de messagerie ESA.

Informations connexes

- Guides utilisateurs d'appareils de sécurité du courrier électronique de Cisco
- Support et documentation techniques - Cisco Systems