Comment résoudre le problème de la non-réception d'un message par Cisco Secure Email Gateway ?

Contenu

Introduction

Ce document décrit pourquoi un message n'est pas reçu par la passerelle de messagerie sécurisée Cisco et les options permettant de résoudre le problème.

Comment résoudre le problème de la non-réception d'un message par Cisco Secure Email Gateway ?

Afin de dépanner la réception des messages, vous devez connaître les adresses IP utilisées pour envoyer le courrier par l'organisation qui a envoyé le courrier. En règle générale, le moyen le plus précis d'obtenir ces informations est de contacter l'administrateur de messagerie de l'organisation de l'expéditeur. En l'absence de cette ressource, vous pouvez utiliser l'une des options suivantes :

- **SenderBase** - Si vous entrez un domaine dans la zone de recherche à l'adresse http://www.senderbase.org, vous recevrez une liste des adresses IP d'envoi connues pour ce domaine.
- **Journaux de messagerie** - Si vous avez reçu du courrier du domaine dans le passé, vous pouvez rechercher dans les journaux de messagerie l'une de ces livraisons réussies.
- **Système de noms de domaine (DNS)** - Vous pouvez rechercher les enregistrements de l'échangeur de messages (MX) pour le domaine. La plupart des petites entreprises utilisent les mêmes serveurs entrants et sortants. Pour les organisations plus grandes ou plus segmentées, cette option ne révélera probablement pas les informations requises.

Une fois que vous connaissez les adresses IP, vous devez effectuer une recherche dans les journaux de messagerie. L'utilitaire grep est un bon outil à cet effet. Si vous exécutez Microsoft Windows, vous pouvez utiliser Rechercher dans Word Pad ou Bloc-notes ou télécharger un utilitaire grep depuis Internet. Unix et Mac OSX sont intégrés et accessibles à partir d'un interpréteur de commandes. La ligne de commande grep ressemblera à ceci, où '10.2.3.4' est l'adresse IP à rechercher :

```
host> grep '10.2.3.4' file.log
```

Si le serveur de l'expéditeur se connecte correctement à votre serveur, une ligne similaire à cet exemple s'affiche lorsque vous recherchez leur adresse IP :

```
Wed Feb  2 23:43:11 2008 Info: New SMTP ICID 6 interface Management (10.0.0.1)
address 10.2.3.4 reverse dns host test.ironport.com verified no
```

Vous pouvez ensuite rechercher toutes les lignes qui impliquent l'ID de connexion entrante (ICID). Les lignes que vous trouverez vous diront si elles ont envoyé des informations de provenance, si elles ont envoyé des informations de destination et les ID de message (MID) liés à la connexion. Une recherche sur les MID vous indiquera si le message a été accepté par le système, les résultats de l'analyse et si la remise a été tentée.

Un autre outil de dépannage disponible est les **journaux de débogage d'injection**. Vous devez d'abord connaître l'adresse IP du ou des serveurs d'envoi. Une fois que vous avez ceci, utilisez la **logconfig** et sélectionnez ce type de journal. Une fois le journal configuré et validé, vous pouvez demander à l'utilisateur d'envoyer un message de test et (en supposant que son serveur se connecte à votre passerelle de messagerie sécurisée Cisco) la passerelle de messagerie sécurisée Cisco consignera l'intégralité de la conversation SMTP. Cela vous permet de voir le point de rupture dans la communication.

S'il n'y a toujours aucune connexion et donc aucun message reçu, l'étape suivante consiste à demander à l'administrateur du serveur émetteur de vérifier ses journaux et/ou d'utiliser telnet pour tester manuellement l'envoi d'un message à partir du serveur de messagerie. Cela imitera le serveur qui tente de livrer à votre passerelle de messagerie sécurisée Cisco et votre passerelle de messagerie sécurisée Cisco réagira de la même manière que si l'application serveur émettrice l'envoyait.

Si le test passe, mais que l'application serveur échoue lorsqu'elle tente d'envoyer du courrier, cela indique des problèmes de remise sur le serveur distant. L'administrateur du serveur distant devra consulter les journaux afin de diagnostiquer les erreurs.

Une cause courante de retard ou d'échec de réception des messages est que l'adresse IP du serveur émetteur n'a pas de DNS inversé configuré correctement, ce qui entraîne un long délai (30+ secondes) pour que la passerelle de messagerie sécurisée Cisco fournisse une bannière SMTP. Certaines applications serveur atteignent leur délai d'attente configuré et ferment la session avant d'envoyer du courrier en raison de la bannière retardée. Dans ce cas, la solution consiste à prolonger le délai d'attente ou à implémenter le DNS inverse. L'action recommandée consiste à implémenter le DNS inverse pour tous les serveurs de messagerie qui livrent à d'autres serveurs de messagerie Internet. Il est considéré comme une étiquette Internet appropriée et permet aux serveurs de messagerie de confirmer l'identité du serveur à un niveau très basique.