Erreurs communes de configuration sur l'ESA

Contenu

Introduction
Quelles sont les erreurs communes de configuration sur l'ESA ?
1. CHAPEAU
2. Stratégie
3. Relais entrants
4. DN
5. Filtres de message et de contenu
7. Prévention de relais ouvert
Informations connexes

Introduction

Ce document décrit des erreurs communes de configuration sur l'appliance de sécurité du courrier électronique (ESA).

Quelles sont les erreurs communes de configuration sur l'ESA ?

Si vous installez une nouvelle évaluation ou regardez au-dessus d'une configuration existante, vous pouvez se référer à cette liste de contrôle des erreurs communes de configuration.

1. CHAPEAU

- Ne mettez pas les scores positifs SBRS comme +5 ou +7 dans le WHITELIST. Une plage de 9.0-10.0 serait CORRECTE, mais l'inclusion des scores inférieurs la fera seulement plus vraisemblablement que le Spam obtiendra.

- Désactivez l'UNKNOWNLIST, les DN vérification d'expéditeur d'enveloppe et connecter la vérification de DN d'hôte à moins que vous vraiment ayez besoin et comprenniez de ces derniers.

- Au lieu de changer la taille de message et d'autres paramètres de la stratégie dans chaque stratégie de flux de courrier, allez aux stratégies de flux de courrier le menu et choisissez la dernière option, des « paramètres de stratégie par défaut ».

- Limitez les nombres maximaux de connexions à trois pour la plupart des expéditeurs, et faites

à ceci le par défaut pour de nouvelles stratégies de flux de courrier.

- Vérifiez que des scores de SenderBase de -10.0 à -2.0 sont inclus dans la LISTE NOIRE. La documentation et les assistants de configuration sont terminés conservateurs ; nous n'avons actuellement aucun faux positif dans cette plage.

2. Stratégie

- Nommez les stratégies après qui les obtient, pas ce qu'elles font. Nommez tous les filtres satisfaits après ce qu'elles font, et utilisez les abréviations comme Q_basic_attachments, D_spoofers, Strip_Multi-Media, où Q signifie que la quarantaine et le D signifie la baisse.

- stratégies de Non-par défaut si « utilisez les valeurs par défaut » pour l'anti-Spam, l'Anit-virus, les filtres satisfaits et les filtres d'épidémie sauf là où vous avez besoin vraiment de configurations spéciales. Ne recréez pas ces configurations dans chaque stratégie s'il n'est pas nécessaire.

- Untick « baisse a infecté des connexions » ou bien vous passerez en fonction beaucoup de courriers électroniques vides où le virus a été éliminé.

- Les configurations d'antivirus pour sortant devraient informer l'expéditeur, pas le destinataire

- Des filtres et l'anti-Spam d'épidémie devraient être désactivés sur sortant

3. Relais entrants

Si le « moniteur > l'aperçu » affiche des connexions de vos propres serveurs et domaines, vous devez les ajouter à l'installation entrante de relais. Une erreur très commune, à l'aide du GUI, est de penser que vous avez activé la caractéristique entrante de relais quand tout que vous avez fait est ajoute les entrées à la table. En outre :

- Ajoutez un groupe spécial d'expéditeur de CHAPEAU pour eux, au-dessus de WHITELIST, pour signaler des buts. Ne choisissez aucune limitation de débit ou DHAP, mais le Spam et la détection des virus sont CORRECTS.

- Ajoutez un filtre de message pour apparier votre action de stratégie de LISTE NOIRE. Exemple :

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

Dans de rares cas où vous réinjectez le courrier électronique (par exemple, retraitant la messagerie d'inter-abonné par la stratégie d'arrivée de messagerie), votre filtre devra également exempter l'interface de reinjection. Normalement ce n'est pas nécessaire.

4. DN

Beaucoup de clients forcent l'ESA pour questionner leurs serveurs DNS internes hors de l'habitude. À la plupart des installations, 100% des enregistrements DNS que nous avons besoin sont sur l'Internet, pas dans les DN internes. Il semble plus de raisonnable de questionner les serveurs racine d'Internet, réduisant le chargement d'expédition sur les DN internes.

5. Filtres de message et de contenu

L'erreur la plus commune est de mettre des conditions assorties dans des filtres satisfaits où elles ne sont pas exigées. La plupart des filtres devraient répertorier quelques actions, mais la condition devrait être blanc de gauche. Le filtre sera *vrai* toujours, et fonctionnera toujours. Vous contrôlez que les utilisateurs/stratégies reçoivent ces actions en créant de nouvelles stratégies entrantes ou de mail sortant comme nécessaires, et appliquant ce filtre à la stratégie. Voici les exemples incorrects et corrects :

- C'est presque toujours une erreur pour utiliser rcpt-à la condition dans un filtre de message. La procédure correcte est d'écrire un filtre satisfait entrant, et le rend spécifique pour un utilisateur particulier en ajoutant une stratégie basée sur destinataire de messagerie entrante.

- C'est presque toujours une erreur pour avoir un test satisfait de filtre pour la présence d'une connexion, puis relâche la connexion. La méthode correcte est de relâcher toujours cette connexion, sans déterminer sa présence.

- C'est presque toujours une erreur pour utiliser le deliver(). Livrez signifie le saut tous filtres restants, puis le livre. Si vous voulez juste livrer sans ignorer le reste des filtres, aucune action explicite n'est exigée (implicite livrez).

7. Prévention de relais ouvert

Quelques services vérifieront pour voir si votre message transfer agent (MTA) reçoit les adresses qui potentiellement pourraient avoir comme conséquence des états de relais ouvert. Puisque laisser votre MTA comme relais ouvert de fonctionnement est mauvais, ces sites peuvent vous ajouter aux listes noires à moins que vous rejetiez ces adresses dangereuses dans la conversation de SMTP.

Ajoutez un groupe spécial d'expéditeur de CHAPEAU pour eux, au-dessus de WHITELIST, pour signaler des buts. Ne choisissez aucune limitation de débit ou DHAP, mais permettez le Spam et la détection des virus.

- Modification à analyser strict d'adresse (est lâchement le par défaut). C'est nécessaire pour empêcher le double @ se connecte des adresses.

- Caractères incorrects d'anomalie (pas bande). C'est également nécessaire pour empêcher le double @ se connecte des adresses.

- Rejetez (ne pas recevoir) les coquilles, et écrivez les caractères suivants : *% ! \ \/?

Informations connexes

- Support et documentation techniques - Cisco Systems