Dépannage des erreurs courantes du dispositif de sécurité du courrier électronique

Table des matières

[Introduction](#)

[Quelles sont les erreurs de configuration courantes sur l'ESA ?](#)

[CHAPEAU](#)

[Policy (politique)](#)

[Relais entrants](#)

[DNS](#)

Introduction

Ce document décrit les erreurs de configuration courantes sur le dispositif de sécurité de la messagerie électronique Cisco (ESA).

Environnement

- Produit :Appareil de sécurité de la messagerie électronique Cisco (ESA)
- Logiciel:AsyncOS pour ESA (version variable selon le déploiement)
- Étendue : Appliquer ces directives aux politiques de courrier entrant et sortant, le cas échéant ; passez en revue chaque section avant d'apporter des modifications.

Conditions préalables

- Accès administratif au ESA (GUI ou CLI)
- Possibilité de consulter les journaux de messagerie et le suivi des messages pour validation
- Services de réputation SenderBase Reputation Score SBRS activé si vous utilisez des groupes d'expéditeurs basés sur SBRS
- Reconnaissance du fait que la table d'accès aux hôtes (HAT) classe les hôtes connectés avant l'évaluation de la politique de messagerie, ce qui affecte la façon dont les contrôles ultérieurs s'appliquent

Vérification générale

- Utilisez Monitor > Overview et le suivi des messages pour confirmer la classification du groupe d'expéditeurs attendue, les correspondances de stratégie et les résultats de remise après les modifications. La réussite signifie que le groupe d'expéditeurs, la stratégie et le résultat de remise attendus apparaissent après la modification.
- Surveillez les quarantaines et les faux positifs pendant 7 à 14 jours après avoir resserré les paramètres de réputation ou de filtrage, et ajustez-les en fonction des partenaires commerciaux connus, si nécessaire.

Erreurs de configuration courantes sur l'appliance de sécurité de la messagerie (ESA)

Utilisez ces vérifications pour identifier et corriger les erreurs de configuration courantes sur l'appliance de sécurité de la messagerie (ESA). Chaque sous-section utilise un problème, une cause, une résolution et un modèle de vérification cohérents afin que le problème puisse être diagnostiqué et corrigé rapidement.

Table d’accès aux hôtes (HAT)

Symptômes

- Le spam est accepté en raison de groupes d'expéditeurs basés sur la réputation trop permissifs.
- Le courrier légitime est limité ou bloqué en raison de contrôles de connexion trop stricts.

Motif

- Les groupes d'expéditeurs sont configurés avec des plages SBRS (SenderBase Reputation Score) ou des paramètres de vérification DNS (Domain Name System) inappropriés.

Résolution

1. N'ajoutez pas de valeurs SBRS positives (par exemple, +5 ou +7) à la liste verte. Pour les listes d'autorisation basées sur SBRS, utilisez uniquement les scores de 9.0 à 10.0 et validez avec le suivi des messages.
2. Configurez la liste des expéditeurs inconnus et les fonctions de vérification DNS uniquement lorsque cela est nécessaire. Si cela n'est pas requis, désactivez UNKNOWNLIST, Envelope SenderDNS Verification et Connecting HostDNS Verification.

Remarque : L'interface utilisateur ESA utilise le terme hérité UNKNOWNLIST pour la liste des expéditeurs inconnus.

3. Pour éviter des paramètres par stratégie incohérents, configurez les paramètres par défaut globaux : choisissez Mail Policies > Mail Flow Policies > Default Policy Parameters et définissez la taille du message et d'autres paramètres par défaut à cet endroit.
4. Définissez une valeur de connexion maximale par défaut raisonnable pour la plupart des expéditeurs (par exemple, 3) et appliquez-la comme valeur par défaut pour les nouvelles stratégies de flux de messagerie ; ajustez les paramètres pour les expéditeurs connus à grand volume, si nécessaire.
5. Configurez la plage SBRS de la liste de blocage en fonction de votre tolérance au risque. Dans de nombreux déploiements, le blocage de SBRS -10.0 à -2.0 peut entraîner de faibles taux de faux positifs. Validation avec suivi des messages et ajustement pour les partenaires commerciaux.

Policy (politique)

Symptôme/impact

- Les messages sont analysés ou mis en quarantaine de manière inattendue, car les stratégies de messagerie non par défaut remplacent les paramètres par défaut globaux.
- Les messages sortants déclenchent des actions antispam/filtre d'attaque inutiles, ce qui augmente le temps de traitement et les faux positifs.
- Les messages apparaissent vides car les pièces jointes infectées sont supprimées et le corps du message ne contient que le contenu supprimé.

Motif

- Les stratégies autres que les stratégies par défaut dupliquent ou remplacent les paramètres par défaut de l'antispam, de l'antivirus, du filtre de contenu ou du filtre contre les attaques sans exigence spécifique.
- Les stratégies sortantes appliquent les fonctions d'analyse axées sur les entrées.

Résolution

1. Nommez les stratégies de messagerie des destinataires auxquels elles s'appliquent (par exemple, Inbound_Executives) et nommez les filtres de contenu pour l'action qu'elles effectuent (par exemple, Q_basic_attachments et Dspoofers).

2. Pour les stratégies autres que les stratégies par défaut, sélectionnez Utiliser les paramètres par défaut pour l'antispam, l'antivirus, les filtres de contenu et les filtres contre les attaques, sauf si une exception documentée est requise.
3. Désactivez la case à cocher Abandonner les pièces jointes infectées pour éviter de remettre des messages dont le contenu est retiré et qui peuvent apparaître vides.
4. Pour les actions antivirus sortantes, avertissez l'expéditeur et non le destinataire.
5. Désactivez les filtres contre les attaques et l'antispam sur les stratégies de messages sortants, sauf en cas d'utilisation explicite de messages sortants.

Vérifier

- Utilisez le suivi des messages pour confirmer que la stratégie de messagerie souhaitée correspond et que les paramètres d'analyse par défaut sont hérités comme prévu.
- Envoyez un message de test sortant contrôlé et confirmez que les filtres antispam/contre les attaques ne sont pas appliqués, sauf s'ils sont configurés par exception.

Relais entrants

Symptômes

- Les serveurs de messagerie internes sont traités comme des expéditeurs externes, ce qui peut entraîner des actions inattendues de limitation, de filtrage ou de réputation.

Motif

- Les adresses IP ou les réseaux du serveur de messagerie interne ne sont pas configurés comme relais entrants ou la fonctionnalité de relais entrant est désactivée.
- Les hôtes de relais internes ne sont pas classés dans un groupe d'expéditeurs HAT dédié, ce qui peut entraîner des limites de connexion non souhaitées ou un comportement DHAP (Directory Harvest Attack Prevention).

Résolution

1. Dans l'interface graphique utilisateur, choisissez Politiques de messagerie > Relais entrants, et ajoutez vos adresses IP ou réseaux de serveur de messagerie interne.
2. Assurez-vous que la fonction de relais entrant est activée (n'ajoutez pas uniquement des entrées à la table).
3. Créez un groupe d’expéditeurs HAT (Host Access Table) dédié pour les relais internes répertoriés dans la liste verte de la liste précédente à des fins de création de rapports. Si

nécessaire, configurez no rate limit et no Directory Harvest Attack Prevention (DHAP), tout en maintenant l'analyse antispam et antivirus activée.DHAP limite les tentatives d'énumération de destinataires non valides pendant la conversation SMTP (Simple Mail Transfer Protocol).

4. Si vous supprimez des messages en fonction de leur réputation pour le trafic non relayé, ajoutez un filtre de messages qui applique un traitement équivalent aux messages relayés, le cas échéant. Exemple :

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

Vérifier

- Dans Monitor > Overview, vérifiez que les serveurs internes n'apparaissent plus en tant qu'expéditeurs externes non approuvés.
- Dans les journaux de suivi des messages/messages, vérifiez que le groupe d'expéditeurs attendu est appliqué (par exemple, un groupe d'expéditeurs de relais interne).



Remarque : Si le courrier est réinjecté (par exemple, le courrier entre abonnés est retraité via la stratégie de trafic entrant), exemptez l'interface de réinjection dans le filtre si nécessaire.La réinjection renvoie un message via l'évaluation de la stratégie, afin que les filtres puissent à nouveau faire correspondre le même message, sauf si l'interface est exclue.

DNS

Symptômes

- Sélection ou fractionnement du résolveur DNS : la configuration DNS entraîne des échecs de remise, des transactions SMTP lentes ou des échecs de réputationContrôles DNS.

Environnement

- S'applique aux déploiements qui nécessitent une résolution DNS publique, une résolution DNS interne uniquement ou un DNS « split-horizon » pour les domaines et services internes.

Symptômes

- Le suivi des messages affiche les échecs/délais d'attente de la recherche DNS pour les requêtes MX, AAA, PTRR ou liées à la réputation.
- La remise des messages est retardée en raison de tentatives DNS répétées.

Motif

- ESA est configuré pour utiliser des résolveurs qui ne peuvent pas résoudre les enregistrements publics requis, les enregistrements internes requis, ou les deux.
- Split-horizonDNS, qui renvoie des réponses différentes pour le même domaine en fonction du réseau source, est requis mais pas mis en oeuvre pour les domaines ou services internes.

Résolution

Configurez la résolution DNS (Domain Name System) en fonction de l'emplacement où l'ESA résout les enregistrements : l'Internet public, les domaines internes uniquement ou les deux :

1. Utilisez des résolveurs récursifs publics lorsque l’ESA a principalement besoin d’enregistrements DNS publics et que la politique le permet.

2. Utilisez internalDNS ou split-horizon DNS lorsque l'ESA doit résoudre des zones internes uniquement, des enregistrements MXX (Mail Exchange interne), des enregistrements LDAPP (Lightweight Directory Access Protocol) ou d'autres services privés.

3. Le DNS public est approprié lorsque l'appliance résout principalement les enregistrements de messagerie Internet et qu'aucune zone interne ou restriction de stratégie ne s'applique.

Utilisez InternalDNS ou splitDNS lorsque cela est nécessaire

- Domaines internes uniquement
- Enregistrements InternalMXX
- Split-horizonDNS (réponses différentes pour le même domaine en fonction du réseau source)
- La conformité ou la stratégie de sécurité nécessite des résolveurs récursifs internes
- Zones DNS privées requises pour le routage
- Zones PrivateDNS requises pour le protocole LDAPP (Lightweight Directory Access Protocol)

- Zones DNS privées requises pour les services internes utilisés par l'ESA

Vérifier

- Vérifiez que l'ESA peut résoudre les noms d'hôtes publics et internes requis (le cas échéant) et que la remise des messages et la réputationLes vérifications DNS réussissent le suivi des messages.

Filtres de messages et de contenu

L'erreur la plus courante consiste à ajouter des conditions correspondantes dans les filtres lorsqu'elles ne sont pas requises.

- Conditions vides : Laissez la condition vide lorsque le filtre doit être exécuté pour chaque message d'une stratégie de messagerie donnée.
- Comportement d'évaluation : Dans les filtres de messages asyncOS, une condition vide est évaluée à true, de sorte que le filtre s'exécute sur chaque message qui l'atteint.
- Portée : Contrôlez l'étendue en attachant le filtre à la stratégie de messages entrants ou sortants appropriée.
- Commande : Les filtres de message évaluent les attributs de message et les actions dans l'ordre. Les filtres de contenu sont généralement définis par la stratégie de messagerie qui les appelle.

Exemples:

- L'utilisation de la condition rcpt-to dans un filtre de message est généralement inutile lorsque l'objectif est de cibler un utilisateur ou un groupe spécifique. Préférez une stratégie de messages entrants basée sur les destinataires et appliquez le filtre de contenu à cette stratégie lorsque les exigences sont correctement associées aux destinataires ou aux groupes de destinataires. Réservez les conditions rcpt-to aux exceptions pour lesquelles la correspondance de stratégie ne peut pas exprimer le besoin.
- Le test de la présence d'une pièce jointe avant sa suppression est généralement redondant lorsque l'intention est de bloquer un type de pièce jointe spécifique. Configurez le filtre pour supprimer directement le type de pièce jointe ciblé ; utilisez un test de présence de pièce jointe uniquement lorsque différentes actions sont requises selon qu'une pièce jointe existe ou non.
- Utilisez delivery() seulement quand le message doit contourner les filtres restants. L'action delivery() arrête le traitement du filtre, puis transmet le message ; pour remettre des messages sans ignorer les filtres restants, ne configurez pas d'action delivery() explicite (la remise implicite s'applique).

Prévention Relais Ouvert

Symptôme/impact

- Les tests de relais tiers indiquent que l'appliance accepte les adresses de destinataires malformées ou dangereuses.
- Les listes de blocage publiques répertorient le protocole IPP expéditeur, car l'analyse des adresses SMTP autorise les modèles couramment utilisés pour valider les relais ouverts.

Motif

- Protocole SMTP (Simple Mail Transfer Protocol) L'analyse d'adresse SMTP et la gestion des caractères autorisent des formats d'adresse non valides (par exemple, double @ signes) ou des littéraux d'adresse, qui sont des adresses IP écrites directement dans l'adresse au lieu d'un nom de domaine.

Résolution

Certains services vérifient si l'agent de transfert de messages (MTA) accepte les adresses mal formées qui peuvent indiquer une condition de relais ouvert. Configurez le comportement strict d'analyse et de rejet afin que l'ESA rejette ces adresses pendant la conversation SMTP.

- Ajoutez un groupe d'expéditeurs HAT dédié pour les sources de test de relais précédant ALLOWLIST pour la création de rapports. Si nécessaire, configurez no rate limit et no Directory Harvest Attack Prevention (DHAP), tout en maintenant les fonctions antispam et antivirus activées, le cas échéant.
- Activez l'analyse d'adresse stricte (la valeur par défaut est Loose) pour empêcher les doubles @ dans les adresses.
- Rejeter (ne pas supprimer) les caractères non valides pour empêcher l'acceptation d'adresses mal formées.
- Rejetez (n'acceptez pas) les littéraux d'adresse et entrez les caractères suivants : *% !\\/ ?

Vérifier

- Exécutez un test de relais externe et confirmez que l'ESA rejette les adresses de destinataires mal formées pendant la conversation SMTP.
- Utilisez le suivi des messages pour confirmer que le groupe d'expéditeurs test-relais est mis en correspondance et que le courrier est traité avec les paramètres d'analyse prévus.

Informations connexes

- Obtenir une assistance technique et de la documentation
- Consulter les guides d'utilisation AsyncOSS pour ESA
- Guides d'installation et de configuration de l'appliance de sécurisation de la messagerie (ESA) (TAH, stratégies de messagerie et filtres de messages)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.