Dépannage des erreurs HAT/RAT courantes sur ESA

Table des matières

Introduction

Aperçu

- CHAPEAU
- Groupe d'expéditeurs
- Score de réputation SenderBase
- Sources ETF (External Threat Feed) appliquées
- Politique de flux de messages
- RAT

Scénarios de mise en oeuvre communs

- Blocage manuel d'un expéditeur
- Ajout de groupes/plages d'adresses IP dans le TAH

Dépannage

- Groupe d'expéditeurs incorrect
- Configuration d'hôte de groupe d'expéditeurs incorrecte
- Les refus HAT/RAT sont-ils pris en compte dans le filtrage par réputation ?
- Vérification des rejets par table RAT
- Comment consigner des informations supplémentaires sur l'expéditeur/le destinataire pour les connexions rejetées ?

Informations connexes

Introduction

Ce document décrit une présentation générale, des conseils de configuration et des techniques de dépannage permettant de diagnostiquer les problèmes courants de la table d'accès aux hôtes (HAT) et de la table d'accès aux destinataires (RAT) sur l'appliance de sécurité de la messagerie (ESA).

Aperçu

CHAPEAU

Pour chaque écouteur configuré, vous devez définir un ensemble de règles qui contrôlent les connexions entrantes des hôtes distants. Par exemple, vous pouvez définir des hôtes distants et

indiquer s'ils peuvent ou non se connecter au processus d'écoute. AsyncOS vous permet de définir les hôtes autorisés à se connecter à l'écouteur à l'aide du TAH.

Le TAH gère un ensemble de règles qui contrôlent les connexions entrantes des hôtes distants pour un écouteur. Chaque écouteur configuré possède son propre TAH indépendant. Vous pouvez configurer des TAH pour les écouteurs publics et privés.

Par défaut, le TAH est défini pour effectuer différentes actions en fonction du type d'écouteur :

- Auditeur public : Le TAH est configuré pour accepter les e-mails de tous les hôtes.
- Écouteur privé : Le TAH est configuré pour relayer les e-mails provenant des hôtes que vous spécifiez et rejeter tous les autres hôtes.

Une règle HAT se compose d'un groupe d'expéditeurs, d'un score de réputation SenderBase (SBRS), de sources de flux de menaces externes appliquées et d'une stratégie de flux de messagerie.

Groupe d'expéditeurs

Un groupe d'expéditeurs est une liste d'expéditeurs identifiés par un ou plusieurs des éléments suivants :

- Adresse IP (IPv4 ou IPv6)
- Plage IP
- Nom d'hôte ou de domaine spécifique
- Classification d''organisation' IP Reputation Service
- Plage du score de réputation IP (IPRS) (ou absence de score)
- Réponse à une requête de liste DNS

Score de réputation SenderBase

L'appliance peut interroger le service de réputation IP pour déterminer un score de réputation IP. Le score de réputation IP est une valeur numérique attribuée à une adresse IP, un domaine ou une organisation en fonction des informations du service de réputation IP.

Sources ETF (External Threat Feed) appliquées

Le cadre des ETF permet à l'ESA d'utiliser des informations sur les menaces externes au format STIX communiquées via le protocole TAXII.

La possibilité d'utiliser des informations sur les menaces externes aide une entreprise à :

- Répondez de manière proactive aux cybermenaces telles que les programmes malveillants, les ransomwares, les attaques par phishing et les attaques ciblées.
- Abonnez-vous aux sources de renseignements sur les menaces locales et tierces.
- Améliorer l'efficacité.

Vous avez besoin d'une clé de fonction valide pour utiliser ETF sur votre ESA. Pour plus d'informations sur l'obtention d'une clé de fonction, contactez votre représentant commercial Cisco et/ou Cisco Global Licensing Operations.

Politique de flux de messages

Les stratégies de flux de messages vous permettent de contrôler ou de limiter le flux des messages électroniques d'un expéditeur à l'écouteur pendant la conversation SMTP. Vous contrôlez les conversations SMTP en définissant ces types de paramètres dans la stratégie de flux de messagerie :

- Paramètres de connexion (par exemple, nombre maximal de messages par connexion)
- Paramètres de limitation de débit (par exemple, nombre maximal de destinataires par heure)
- Les codes et les réponses SMTP personnalisés sont communiqués pendant la conversation SMTP
- Activer/désactiver la détection antispam
- Activer/désactiver la protection antivirus
- Chiffrement (par exemple, TLS)
- Authentification et vérification (par exemple, DMARC, DKIM et SPF)

RAT

AsyncOS utilise la TAD pour chaque écouteur public afin de gérer l'acceptation ou le rejet des adresses des destinataires. Les adresses des destinataires sont les suivantes :

- Domaines
- Adresses e-mail
- Groupes d'adresses électroniques

Par défaut, le TAD rejette tous les destinataires pour empêcher la création d'un relais ouvert.

Scénarios de mise en oeuvre communs

Blocage manuel d'un expéditeur

Afin de bloquer un expéditeur spécifique par adresse IP d'expéditeur, ajoutez une entrée manuelle pour l'adresse IP sous le groupe d'expéditeurs de la liste de blocage et assurez-vous que l'action est définie sur 'Rejeter' ou 'Refuser TCP'. Pour les instructions de configuration, référez-vous à : Block a Sender IP Manually on ESA.

Ajout de groupes/plages d'adresses IP dans le TAH

Les adresses IP adjacentes peuvent être regroupées en sous-réseaux tels que 192.0.2.0/24, en plages d'adresses IP telles que 192.0.2.10-20 ou en adresses IP partielles telles que 192.0.2. et ajoutées à la table. Afin d'ajouter plusieurs adresses IP non adjacentes, observez ces étapes :

À partir de l'interface utilisateur :

1. Naviguez jusqu'à Politiques de messagerie **>** Vue d'ensemble HAT (si nécessaire, choisissez le niveau de cluster approprié).
2. Choisissez le Groupe d'expéditeurs à modifier et choisissez Ajouter un expéditeur.
3. Dans le champ Sender, saisissez les plages d'adresses IP applicables (par exemple, 192.0.2.0/24), un commentaire facultatif et choisissez Submit.
4. Cliquez sur Commit Changes pour enregistrer.

À partir de la CLI :

1. Exécutez la séquence de commandes :

   <#root>

   ```
   listenerconfig >> EDIT
   ```

2. Entrez le nom ou le numéro du processus d'écoute à modifier.
3. Exécutez la séquence de commandes, puis entrez le numéro ou le nom du groupe d'expéditeurs à modifier :

   ```
   HOSTACCESS >> EDIT >> 1
   ```

4. Choisissez new et entrez une liste d'expéditeurs à ajouter séparés par des virgules.
5. Une fois terminé, exécutez commit pour enregistrer les modifications.

Dépannage

Groupe d'expéditeurs incorrect

Vérifiez les journaux de messagerie sur l'ESA ou le suivi des messages sur le dispositif de gestion de la sécurité (SMA), et vérifiez ces entrées dans l'ID de connexion entrante (ICID) :

```
ICID 476946 ACCEPT SG WhiteList match nx.example SBRS None country United States
```

Motif : La vérification DNS de l'hôte de connexion est activée sur le groupe d'expéditeurs et l'enregistrement PTR de l'hôte de connexion n'existe pas dans DNS est sélectionné.

```
ICID 476946 ACCEPT SG WhiteList match not.double.verified.example SBRS None country United States
```

Motif : Connexion La vérification DNS de l'hôte est activée sur le groupe d'expéditeurs et la connexion de la recherche DNS inverse de l'hôte (PTR) ne correspond pas à la recherche DNS directe (A) est choisie.

```
ICID 476946 ACCEPT SG WhiteList match serv.fail.example SBRS None country United States
```

Motif : La vérification DNS de l'hôte de connexion est activée sur le groupe d'expéditeurs et la recherche d'enregistrements PTR de l'hôte de connexion échoue en raison d'une défaillance DNS temporaire est sélectionnée.

Configuration d'hôte de groupe d'expéditeurs incorrecte

Un groupe d'expéditeurs est une liste d'expéditeurs identifiés par :

- Adresse IP (IPv4 ou IPv6)
- Plage IP
- Nom d'hôte ou de domaine spécifique
- Classification d''organisation' IP Reputation Service
- Plage du score de réputation IP (IPRS) (ou absence de score)
- Réponse à la requête Liste DNS

Exemple d'adresses mal configurées sous Sender Group : ESA Sender Group Matching Partial Hostnames.

Les refus HAT/RAT sont-ils pris en compte dans le filtrage par réputation ?

Oui, les messages rejetés par un groupe d'expéditeurs avec l'action de rejet dans la stratégie de flux de messagerie sont comptés dans le compteur de rapports « Arrêté par filtrage par réputation ».



Remarque : Ce compteur peut inclure les rejets de stratégie HAT et les rejets basés sur SBRS. Vérifiez la raison du rejet dans les journaux de messagerie pour distinguer la source.

Vérification des rejets par table RAT

Voici un exemple de sortie de journal à partir des journaux de messagerie sur un ESA :

```
Thu Sep 18 09:10:14 2014 Info: MID 48445 ICID 15970 To: <user@example.com> "Rejected by RAT"
```

Motif : Le domaine spécifique n'est pas autorisé sous le RAT dans la configuration ESA.

Comment consigner des informations supplémentaires sur l'expéditeur/le destinataire pour les connexions rejetées ?

Par défaut, une connexion rejetée enregistre uniquement l'adresse IP MTA de l'expéditeur dans les journaux de messagerie et n'enregistre pas l'expéditeur ou le destinataire de l'enveloppe. Si une journalisation supplémentaire est requise pour le dépannage, le rejet HAT retardé peut être activé sur AsyncOS.



Mise en garde : Cisco vous recommande de ne pas activer cette fonctionnalité de manière permanente, car elle nécessite des ressources supplémentaires.

Plus de détails peuvent être trouvés ici : FAQ sur le rejet retardé du TAH.

Informations connexes

- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final
- Assistance technique de Cisco et téléchargements

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.