Configurer l'analyse par stratégie Threat Scanner pour SEG

Table des matières

Introduction

Conditions préalables

- Composants utilisés

Aperçu

Configurer

- Configuration de l'interface Web
- Configuration de l'interface de ligne de commande

Vérifier

Informations connexes

Introduction

Ce document décrit le service et la configuration de Threat Scanner (TS) Per Policy Integration pour Cisco Secure Email Gateway (SEG).

Conditions préalables

La connaissance des paramètres généraux et de la configuration du SEG est souhaitée.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 et versions ultérieures.
- Service Graymail.
- Service antispam.
- Stratégies de messages entrants.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Threat Scanner (TS), un sous-composant récemment activé du service Graymail, a été intégré à Antispam CASE pour offrir une meilleure protection contre le spam.

Une fois que le service Graymail a été activé, les options permettant d'activer Threat Scanner

deviennent actives dans chaque paramètre Antispam pour la politique de messages entrants. Une fois activé, TS améliore la détection antispam globale en mettant l'accent sur la détection de la contrebande HTML :

- Analyse HTML et détection de scripts malveillants
- Analyse URL et détection de redirection

Le moteur Antispam CASE gère les deux services, en gérant les mises à jour et les condamnations pour spam.

TS dispose de paramètres d'activation/de désactivation visibles dans chaque paramètre Antispam de stratégie de messages entrants.

TS influence les verdicts, ce qui augmente le poids du verdict final de l'Antispam CASE.

Configurer

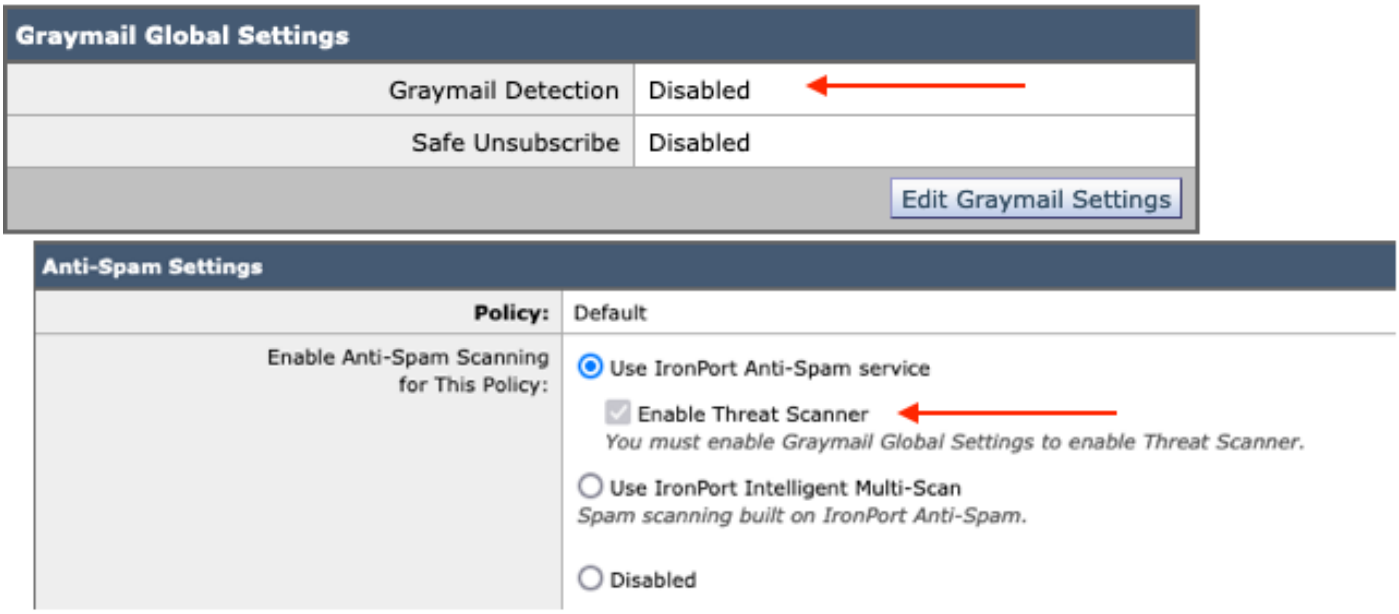
La configuration se compose de deux actions : Activer la détection Graymail et Activer TS dans les stratégies de messages entrants.

- Le service global Graymail doit être activé pour activer TS.
- L'option « Antispam » de la stratégie de courrier entrant « Activer l'analyseur de menaces » devient disponible une fois que Graymail a été activé globalement.

Configuration de l'interface Web

Pour activer Graymail dans WebUII :

- Accédez à Services de sécurité
    - IMS et Graymail
        - Paramètres généraux de Graymail
            - Modifiez les paramètres Graymail.
                - Sélectionnez l'option permettant d'activer la détection Graymail.
- Soumettre et valider les modifications pour finaliser l'action.

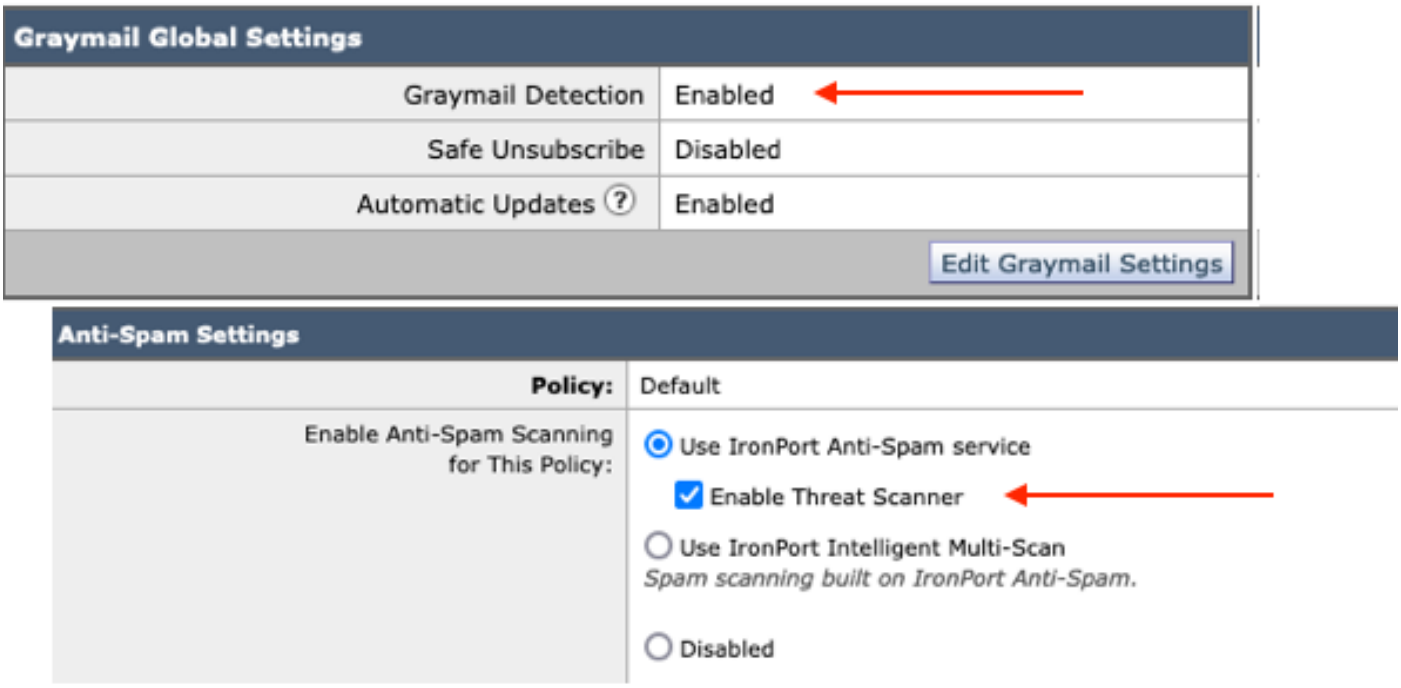


La vue avant la configuration

Une fois Graymail activé, la zone de sélection du Threat Scanner devient disponible pour chaque stratégie de messages entrants.

Pour activer Threat Scanner dans l'interface Web :

- Naviguer jusqu'aux stratégies de messagerie
  - Stratégies de messages entrants
    - Sélectionnez la stratégie de messagerie souhaitée
      - Sélectionnez Antispam.
        - Le haut de la page de configuration présente l'option de case à cocher Activer Threat Scanner.
- Soumettre et valider les modifications pour finaliser la configuration



Option Threat Scanner dans l'antispam

Configuration de l'interface de ligne de commande

Activez le service Graymail à l'aide des commandes CLI.

- imsandgraymailconfig
  - chaire grise
    - coup monté
      - Voulez-vous utiliser la détection Graymail ? [Y] >
        - Voulez-vous activer les mises à jour automatiques pour le moteur Graymail ? [O]>
  - Complétez les invites restantes pour revenir à l'invite de l'ordinateur principal.

- Valider + ajouter les commentaires souhaités > Effectuez l'action en appuyant sur la touche Retour.

Activation ou désactivation de Threat Scanner dans une stratégie à partir de l'interface de ligne de commande.

- CLI> configuration de la stratégie

Voulez-vous configurer la stratégie de messages entrants ou de messages sortants ou la priorité des en-têtes de correspondance ?

1. Stratégies de messages entrants
2. Stratégies de messages sortants
3. Priorité de correspondance des en-têtes

[1]> 1

Configuration de la stratégie de messagerie entrante

1. Nord1
2. LISTE_BLOQUÉE
3. LISTE_AUTORISÉE
4. ALLOW_SPOOF
5. PAR DÉFAUT

Saisissez le nom ou le numéro de l'entrée que vous souhaitez modifier :
[]> 1

Sélectionnez l'opération que vous souhaitez effectuer :
- NOM - Modifier le nom de la stratégie
- NOUVEAU - Ajouter une nouvelle ligne de membre de stratégie
- DELETE - Supprime une ligne de membre de stratégie
- PRINT - Imprime les lignes de membre de stratégie
- ANTISPAM - Modifier la politique antispam
- ANTIVIRUS - Modifier la stratégie antivirus
- ÉPIDÉMIE - Modifier la stratégie des filtres contre les épidémies

- ADVANCEDMALWARE - Modifier la stratégie Advanced Malware Protection
- GRAYMAIL - Modifier la stratégie Graymail
- THREATDEFENSECONNECTOR - Modifier le connecteur de défense contre les menaces
- FILTRES - Modifier les filtres
[]> antispam

Sélectionnez l'opération que vous souhaitez effectuer :
- DISABLE - Désactive la politique antispam (désactive toutes les actions liées à la politique)
- ENABLE - Activer la politique anti-spam
[]> activer

Commencer la configuration de l'antispam

Voulez-vous utiliser l'analyse multiple intelligente sur cette stratégie ? [N]>

Souhaitez-vous utiliser l'antispam IronPort sur cette stratégie ? [O]>

Certains messages sont identifiés comme étant du spam. Certains messages sont identifié comme spam suspecté. Vous pouvez définir l'antispam IronPort Spam suspecté Seuil inférieur.
Les options de configuration s'appliquent aux messages POSITIVEMENT identifiés comme spam :
Voulez-vous activer un traitement spécial pour Threat Scanner verdict ? [N]> o

Continuez à parcourir les sélections de menu pour compléter les choix de stratégie de messagerie et appuyez sur la touche Retour pour accepter l'action par défaut pour chaque choix.

Effectuez l'enregistrement à l'aide des commandes.

- Valider + ajouter les commentaires souhaités > Effectuez l'action en appuyant sur la touche Retour.

Vérifier

Comment lire et interpréter les journaux.

La journalisation des e-mails de Threat Scanner ne présente qu'un verdict provisoire, alors que CASE présente le verdict final.

Les journaux d'e-mails affichent deux verbiages différents pour les verdicts de Threat Scanner sains et condamnés

- Si le verdict provisoire de Threat Scanner est clair, le journal est présenté de la même manière que ces échantillons.
    - Infos : verdict provisoire graymail - LEGIT (0) <Message propre>
    - Infos : verdict provisoire - MCE (11) <Campagne d'e-mails divers>
- Si le verdict provisoire de Threat Scanner doit être prononcé, le journal est présenté de la

même façon que ces échantillons.
- Info : verdict provisoire de ThreatScanner - HAMEÇONNAGE (101)
- Info : verdict provisoire de ThreatScanner - VIRUS (2)

Journaux de messagerie, exemple : le verdict Nettoyer Threat Scanner utilise différents verbiages : verdict graymail.

<#root>

```
Wed Jan 31 08:19:32 2024 Info: MID 3189755
```

interim graymail verdict - LEGIT (0) <Clean message>

```
Wed Jan 31 08:19:33 2024 Info: MID 3189755 interim verdict using engine: CASE negative
Wed Jan 31 08:19:33 2024 Info: MID 3189755 using engine: CASE spam negative
```

Le suivi des messages n'affiche pas l'entrée du journal de Threat Scanner, mais uniquement le message CASE : Final Verdict.

Ces exemples de Threat Scanner (TS) présentent les 4 scénarios de verdict.

Remarque : les catégories TS de « PHISHING » et de « VIRUS » sont les seules détections qui augmentent le poids du verdict CASE

Exemples de journaux de messagerie : la condamnation de PHISHING TS et la condamnation antispam sont toutes deux présentes

<#root>

```
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

interim

ThreatScanner verdict - PHISHING (101)

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:23 2024 Info: MID 3057397 interim verdict using engine: CASE spam positive
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

using engine: CASE spam positive

```
Thu Jan 25 09:05:23 2024 Info: Message aborted MID 3057397 Dropped by CASE
```

Exemple de suivi : la condamnation PHISHING TS est absente et la condamnation CASE est présente.

25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Final verdict: Positive

PHISHING TS condamné et traçage de l'antispam condamné

Exemples de journaux de messagerie : PHISHING TS Conviction et AntiSpam Negative sont tous deux présents.

<#root>

```
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

interim ThreatScanner verdict - PHISHING (101)

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:47 2024 Info: MID 3057413 interim verdict using engine: CASE spam negative
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

using engine: CASE spam negative

Exemple de suivi : PHISHING TS Convicted and AntiSpam Negative is present.

25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Final verdict: Negative

Exemples de journaux de messagerie : VIRUS TS Conviction et AntiSpam Conviction, exemples de journaux de messagerie.

<#root>

```
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim
```

ThreatScanner verdict - VIRUS (2)

```
 <Virus detected by ThreatScanner engine>
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim verdict using engine: CASE spam positive
Thu Jan 25 13:37:16 2024 Info: MID 3066060
```

using engine: CASE spam positive

```
Thu Jan 25 13:37:16 2024 Info: Message aborted MID 3066060 Dropped by CASE
```

Exemple de suivi : VIRUS TS Conviction absent et AntiSpam Conviction présent.

25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 scanned by Anti-Spam engine: CASE. Final verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 aborted: Dropped by CASE

Exemples de journaux de messagerie : VIRUS TS Conviction et AntiSpam Negative sont tous deux présents.

<#root>

```
Jan 23 21:38:57 2024 Info: MID 3013692
```

interim ThreatScanner verdict - VIRUS (2)

```
 <Virus detected by ThreatScanner engine>
Jan 23 21:38:58 2024 Info: MID 3013692 interim verdict using engine: CASE spam negative
Jan 23 21:38:58 2024 Info: MID 3013692
```

using engine: CASE spam negative

Exemple de suivi : VIRUS TS Conviction absent et AntiSpam Negative présent.

23 Jan 2024 19:38:57 (GMT -08:00)	Message 3013692 matched per-recipient policy DEFAULT for inbound mail policies.
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Final verdict: Negative

Les journaux Graymail contiennent le verdict de Threat Scanner et le contenu de prise en charge pour l'analyse TALOS si un faux positif est émis.

La présence des résultats bruts de Threat Scanner a entraîné le basculement plus rapide de la journalisation Graymail. Pour remédier à ce comportement, les modifications SEG ont été apportées aux journaux Graymail.

- AsyncOS 15.5 définit l'abonnement par défaut aux fichiers journaux Graymail sur 20 pour une meilleure rétention des journaux.
  - Aucun paramètre de fichier journal ne change si le paramètre est défini sur une valeur supérieure à 20 lors de la mise à niveau.
- Les messages Graymail entrants reconnus provisoirement affichent les résultats bruts de l'analyse complète, au niveau des informations.
- Les résultats de l'analyse Graymail pour tous les autres messages s'affichent au niveau de débogage.

Informations connexes

- Guide de configuration de Email Security
- Guides d'assistance de la page de lancement de Cisco Secure Email Gateway

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.

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.