

Configurer la liste des exceptions du domaine de l'expéditeur pour la passerelle de messagerie sécurisée

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Configurer](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les « Nouvelles modifications » apportées à l'option de paramètre SDR (Sender Domain Reputation) Domain Exception List pour Cisco Secure Email Gateway (SEG).

Contribution de Chris Arellano Ingénieur du centre d'assistance technique Cisco

Conditions préalables

Une connaissance générale des paramètres et de la configuration du SEG est souhaitée.

AsyncOS 15.0 et versions ultérieures pour Cisco Secure Email Gateway (SEG).

Compréhension générale de la fonctionnalité SDR.

Exigences

Activez le service Sender Domain Reputation et créez une liste d'adresses avec l'option Domain Only.

Composants utilisés

- Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :
 - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 et versions ultérieures.
- Réputation du domaine de l'expéditeur SEG.

- Liste d'adresses.

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

La réputation de domaine de l'expéditeur est un service cloud qui collecte plusieurs valeurs d'expéditeur, dérive des verdicts et fournit des options permettant d'agir sur ces verdicts. SDR permet aux paramètres de contourner les domaines approuvés par le biais de l'utilisation d'une liste d'adresses appliquée à la liste d'exceptions de domaine.

La liste d'exceptions de domaine SDR dans les versions d'AsynOS antérieures à SEG 15.0 avait 2 options :

- Activé = Faire correspondre l'enveloppe de, domaine pour contourner l'action SDR.
- Désactivé = Correspondance uniquement si toutes les réponses sont présentes : Enveloppe de + Convivial de + Répondre à + SPF + DKIM + DMARC .

Liste des exceptions de domaine pour SEG 15.0 et les options plus récentes :

- Activé = Faire correspondre l'enveloppe de, domaine pour contourner l'action SDR.
- Disabled = Match si le domaine est présent dans l'une des valeurs :
 - BONJOUR
 - RDNS
 - Enveloppe - De
 - Expéditeur
 - Réponse

Configurer

Le point central de cet article est la nouvelle configuration de la liste d'exceptions de domaine uniquement. La configuration complète du SDR est fournie dans le Guide de l'utilisateur.

Naviguez dans l'interface WebUI vers Security Services > Domain Reputation.


- L'option Match Domain Exception List basée sur la partie Domain Name de l'enveloppe de est activée par défaut.
 - Si la case à cocher est activée, seule la valeur « Envelope From, header » correspondra et contournera le message s'il est reconnu coupable.
 - Si la case à cocher est vide, la liste d'exceptions de domaine SDR correspondra à l'un des en-têtes « HELO: », « RDNS: », « Envelope From: », « From: » et « Reply-To: », correspondra et contournera le message s'il est reconnu coupable.

Si l'icône d'information ? associée est sélectionnée, les détails du paramètre sont présentés.

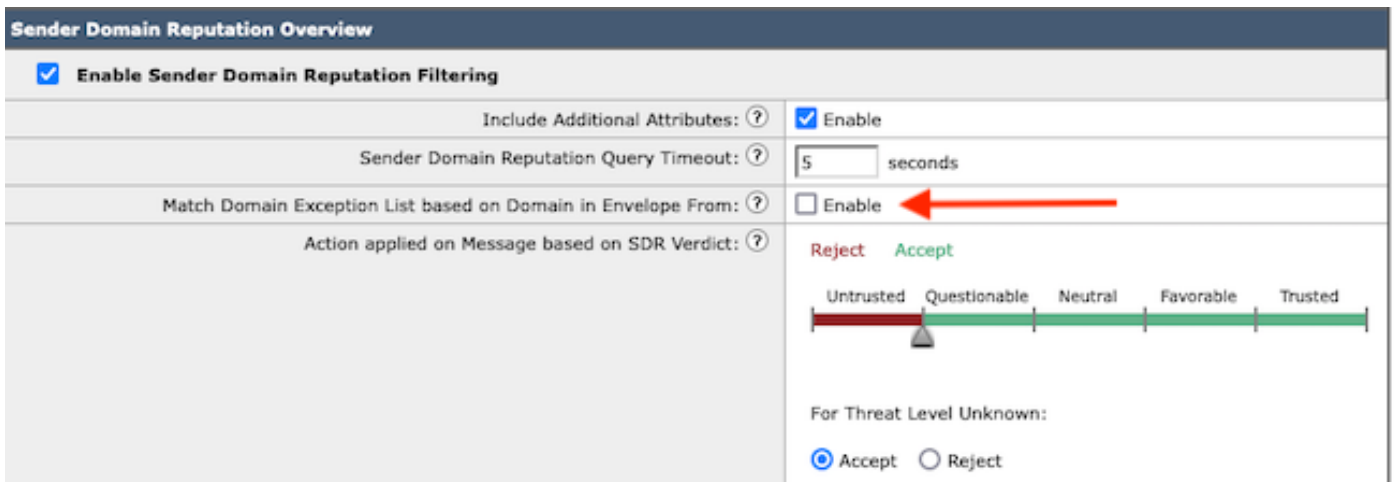
Match Domain Exception List based on Domain in Envelope From. ✕

Disable this option if you want to skip the SDR checks if any domains in the 'HELO:', 'RDNS:', 'Envelope From:', 'From:' and 'Reply-To:' headers of the message match the domains configured in the domain exception list.

Note: By default, SDR checks are skipped based on the domain in the 'Envelope From:' header only.

 Remarque : par défaut, les vérifications SDR sont ignorées en fonction du domaine dans l'en-tête « Envelope From: » uniquement.

Sélectionnez Edit Global Settings pour supprimer l'option de case à cocher, comme illustré dans l'image :



The screenshot shows the 'Sender Domain Reputation Overview' settings page. It includes several configuration options:

- Enable Sender Domain Reputation Filtering:** Enable
- Include Additional Attributes:** Enable
- Sender Domain Reputation Query Timeout:** 5 seconds
- Match Domain Exception List based on Domain in Envelope From:** Enable (highlighted with a red arrow)
- Action applied on Message based on SDR Verdict:** A scale from 'Untrusted' (red) to 'Trusted' (green) with a slider positioned at 'Questionable'. Below the scale, 'For Threat Level Unknown:' is set to Accept and Reject.

La liste d'exceptions de domaine elle-même est une liste d'adresses contenant des noms de domaine.

Vérifier

Pour vérifier le bon fonctionnement à l'aide de la nouvelle fonctionnalité de désactivation, vous devez envoyer un message de test au SEG avec une valeur de domaine correspondante dans l'une des 5 valeurs d'en-tête.

Un exemple de journal indiquant une exception dans la liste d'exceptions globale et correspondant dans une stratégie de flux de courrier se présenterait au début des journaux de courrier :

```
Info: MID 14 SDR: MID 14 containing domain name'test1.example.com' matched the global domain exception
```

Un exemple de journal indiquant une exception contient à la fois le domaine et le nom de la liste d'exceptions.

```
Info: MID 16 containing domain name 'test3.example.com' matched the domain exception list 'SDR-TEST-3'
```

Dépannage

Si des questions se posent quant à l'exactitude d'un verdict de message sélectionné, les valeurs sont documentées et comparées au suivi de message.

- Documentez les paramètres globaux de réputation de domaine > Paramètres de sécurité > Réputation de domaine.
- Vérifiez la liste d'adresses associée configurée dans les paramètres globaux de réputation de domaine.
- Vérifiez la stratégie de flux de messages correspondante en fonction du suivi des messages.
- Vérifiez et notez les détails des filtres de messages ou de contenu avec des listes d'exceptions de domaine configurées.

Collecter le suivi des messages, les journaux de messagerie et les en-têtes d'e-mail originaux.

- Si l'exception globale correspond sur un message, il n'y a pas d'entrées de journal pour la réputation de domaine, simplement une ligne indiquant le domaine correspondant.
- Si la liste d'exceptions globale ne correspond pas sur un message, il existe des entrées de journal pour la réputation de domaine à partir desquelles comparer les valeurs.
 - Info : MID 16 SDR : Domaines pour lesquels SDR est demandé : reverse DNS host : Not Present, helo : mail1.example.com, env-from : test2.example.com, header-from : te destination.example.com, réponse à : test2.example.com
- Les en-têtes d'e-mail incluent l'une des 5 valeurs présentes dans un e-mail individuel à comparer aux paramètres.

Une fois toutes les données collectées, vérifiez les correspondances ou les absences de correspondances pour déterminer le bon fonctionnement.

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.