Autoriser un expéditeur de confiance à contourner l'antispam

Contenu

[Introduction](#)
[Ajout du nom d'hôte/de l'adresse IP de l'expéditeur dans le groupe d'expéditeurs ALLOWED_LIST](#)
[À partir de la GUI](#)
[À partir de l'interface de ligne de commande](#)
[Examiner l'analyse antivirus et antispam dans la stratégie de flux de messages de confiance](#)
[Ajouter un expéditeur de confiance à la liste sécurisée](#)
[Expéditeurs approuvés avec stratégies de messagerie entrante](#)
[Informations connexes](#)

Introduction

Ce document décrit les détails permettant à un expéditeur de confiance de contourner l'analyse antispam, ainsi que les différentes méthodes que vous pouvez opter pour la même option sur la passerelle de messagerie sécurisée (anciennement appelée dispositif de sécurité de la messagerie).

Ajout du nom d'hôte/de l'adresse IP de l'expéditeur dans le groupe d'expéditeurs ALLOWED_LIST

Ajoutez des expéditeurs approuvés au groupe d'expéditeurs ALLOWED_LIST, car ce groupe d'expéditeurs utilise la stratégie de flux de messages $TRUSTED. Les membres du groupe d'expéditeurs ALLOWED_LIST ne sont pas soumis à la limitation de débit, et le contenu de ces expéditeurs n'est pas analysé par le moteur antispam, mais est toujours analysé par l'antivirus.

> **Note**: Avec la configuration par défaut, l'analyse antivirus est activée mais l'antispam est désactivé.

Afin de permettre à un expéditeur de contourner l'analyse antispam, ajoutez l'expéditeur au groupe d'expéditeurs ALLOWED_LIST dans la table d'accès hôte (HAT). Vous pouvez configurer le TAH via l'interface utilisateur graphique ou l'interface de ligne de commande.

Àpartir de la GUI

1. Sélectionnez l'onglet **Politiques de messagerie**.
2. Sous la section **Table d'accès aux hôtes**, sélectionnez **Vue d'ensemble de HAT**.
3. Sur la droite, assurez-vous que votre écouteur **InboundMail** est actuellement sélectionné.
4. Dans la colonne **Groupe d'expéditeurs**, sélectionnez **ALLOWED_LIST**.
5. Cliquez sur le bouton **Ajouter un expéditeur** en bas de la page.
6. Saisissez l'adresse IP ou le nom d'hôte que vous souhaitez autoriser à contourner dans le

premier champ.

Lorsque vous avez terminé d'ajouter des entrées, sélectionnez le bouton **Soumettre**. N'oubliez pas de sélectionner le bouton **Valider les modifications** afin d'enregistrer vos modifications.

Àpartir de l'interface de ligne de commande

```
example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (172.19.1.80/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess
Default Policy Parameters
==========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
```

```
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> edit
1. Edit Sender Group
2. Edit Policy
[1]> 1
Currently configured HAT sender groups:
1. ALLOWED_LIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLOCKED_LIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]> 1

Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]> new
Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed. IP
address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are
allowed. Hostnames such as crm.example.com are allowed. Partial hostnames such
as .example.com are allowed.
Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are allowed.
SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blocklist queries such as dnslist[query.blocklist.example] are allowed.
Separate multiple hosts with commas
[]>
```

N'oubliez pas d'émettre la commande **commit** afin d'enregistrer vos modifications.

Examiner l'analyse antivirus et antispam dans la stratégie de flux de messages de confiance

Pour l'expéditeur approuvé, une stratégie de flux de courrier est nommée par défaut en tant que présent approuvé. La stratégie de flux de courrier approuvé aura un comportement de connexion Accepter (similaire au comportement d'autres stratégies de flux de courrier pour les courriers entrants).

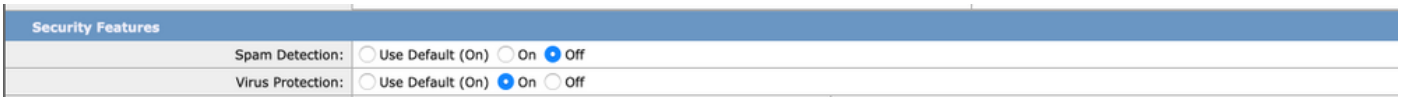
Lorsqu'un expéditeur est approuvé pour les besoins de l'entreprise, nous pouvons choisir de désactiver les contrôles antivirus et antispam pour lui. Cela permettra de réduire la charge de traitement supplémentaire sur les deux moteurs d'analyse pendant qu'ils analysent les e-mails qui ne proviennent pas de sources fiables.

> **Note**: Les moteurs anti-spam et anti-virus désactivés ignorent les analyses de spam ou de virus pour les e-mails entrants dans ESA. Cela ne doit être fait que si vous êtes totalement sûr que les analyses ignorées pour ces expéditeurs de confiance ne présentent aucun

risque.

L'option à partir de laquelle vous pouvez désactiver les moteurs est disponible dans l'onglet Fonctionnalités de sécurité des stratégies de flux de courrier. Le chemin d'accès est **GUI > Mail Policies > Mail Flow Policies**. Cliquez sur la **stratégie de flux TRUSTEDMail** et faites défiler jusqu'à **Fonctions de sécurité** sur la page suivante.

Assurez-vous de valider les modifications après avoir effectué les modifications souhaitées.



Ajouter un expéditeur de confiance à la liste sécurisée

Les listes sécurisées et les listes de blocage des utilisateurs finaux sont créées par les utilisateurs finaux et stockées dans une base de données vérifiée avant l'analyse antispam. Chaque utilisateur final peut identifier des domaines, des sous-domaines ou des adresses e-mail qu'il souhaite toujours traiter comme du spam ou jamais comme du spam. Si une adresse d'expéditeur fait partie d'une liste sécurisée des utilisateurs finaux, l'analyse antispam est ignorée

Cette configuration permettra à l'utilisateur final de mettre en sécurité un expéditeur conformément à sa condition d'exemption des analyses antispam. L'analyse antivirus et d'autres analyses du pipeline de courrier électronique ne seront pas touchées par cette configuration et se poursuivront conformément à la configuration des stratégies de courrier. Cette configuration réduira l'engagement de l'administrateur, chaque fois qu'un utilisateur final doit exempter l'analyse du spam pour un expéditeur.

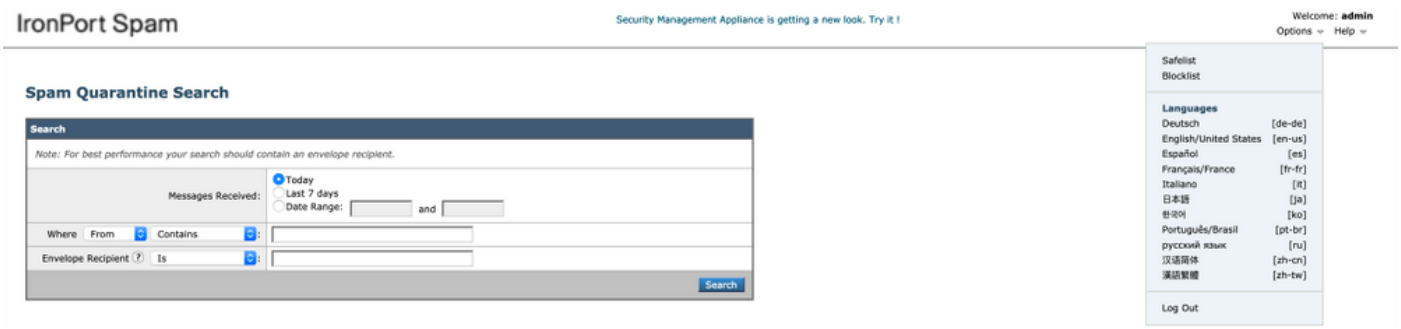
Pour la liste sécurisée, l'accès à la quarantaine de l'utilisateur final doit être activé pour les utilisateurs finaux et la liste sécurisée/liste de blocage de l'utilisateur final comme activé (dans ESA ou SMA). De cette manière, ils peuvent accéder au portail de quarantaine du spam et, parallèlement à **Release/Delete** des e-mails mis en quarantaine, ils peuvent également **Ajouter/Supprimer** des expéditeurs dans la liste sécurisée.

L'accès **à la quarantaine de l'utilisateur final** peut être activé sous :

ESA : Accédez à **GUI > Monitor > Spam Quarantine**. Activez le bouton **Radio** pour **Accès à la quarantaine de l'utilisateur final**. Sélectionnez la méthode d'authentification pour l'accès selon les besoins (None/LDAP/SAML/IMAP ou POP). Publiez cela, activez la liste sécurisée/liste de blocage de l'utilisateur final.

SMA : Accédez à **GUI > Services centralisés > Quarantaine du spam**. Activez le bouton **Radio** pour **Accès à la quarantaine de l'utilisateur final**. Sélectionnez la méthode d'authentification pour l'accès selon les besoins (None/LDAP/SAML/IMAP ou POP). Publiez cela, activez la liste sécurisée/liste de blocage de l'utilisateur final.

Une fois activé, lorsqu'un utilisateur final accède au portail de quarantaine du spam, il peut **ajouter/modifier** sa liste sécurisée selon les options de la liste déroulante en haut à droite.



Expéditeurs approuvés avec stratégies de messagerie entrante

Vous pouvez également ajouter un expéditeur approuvé dans la stratégie de messagerie entrante et désactiver les analyses **antivirus/antispam** selon les besoins. Une nouvelle stratégie de messagerie personnalisée peut être créée avec un nom tel que **Trusted Senders/Safe Senders**, etc. selon vos choix, puis vous pouvez ajouter les détails de l'expéditeur tels que les noms de domaine ou les adresses e-mail de l'expéditeur à cette stratégie personnalisée.

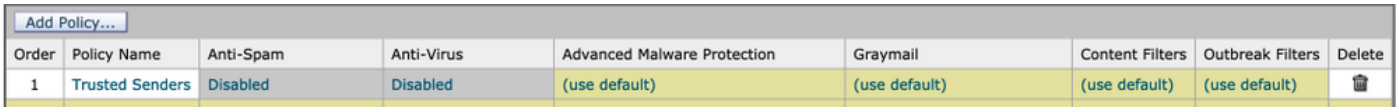
Une fois que vous avez envoyé la stratégie après l'ajout requis, vous pouvez cliquer sur les colonnes **Antispam** ou **Antivirus,** et sur la page suivante, sélectionnez **Désactiver**.

Avec cette configuration, les domaines ou adresses e-mail d'expéditeur approuvés ajoutés à cette stratégie de messagerie seront exemptés des analyses antivirus ou antispam.

> **Note**: Les moteurs anti-spam et anti-virus désactivés ignorent les analyses de spam ou de virus pour les e-mails entrants dans ESA traités via cette politique de messagerie personnalisée. Cela ne doit être fait que si vous êtes totalement sûr que les analyses ignorées pour ces expéditeurs de confiance ne présentent aucun risque.

La stratégie de messagerie personnalisée peut être créée à partir de l'**interface utilisateur graphique ESA > Politiques de messagerie > Politiques de messagerie entrante > Ajouter une stratégie**. Entrez le nom de la stratégie par choix, puis sélectionnez **Ajouter un utilisateur**. Activez la case d'option pour les **expéditeurs suivants.** Ajoutez le domaine ou les adresses e-mail requis dans la zone et cliquez sur **OK**.

Après la création de la stratégie de courrier, vous pouvez sélectionner pour désactiver les analyses antivirus et antispam selon les besoins de l'entreprise. Voici un exemple de capture d'écran :



Informations connexes

- [Cisco Email Security Appliance - Guides de l'utilisateur final]
- [Support et documentation techniques - Cisco Systems]