# Comment configurer l'ESA pour ignorer l'analyse antivirus et/ou antispam de mes expéditeurs de confiance ?

## Contenu



## Question

Comment configurer l'ESA pour ignorer l'analyse antivirus et/ou antispam de mes expéditeurs de confiance ?

## Réponse

AsyncOS propose trois outils principaux que vous pouvez utiliser pour ignorer la vérification antivirus ou antispam de vos expéditeurs les plus fiables. Veuillez noter que l'ESA ne conseille pas d'ignorer la vérification antivirus à tout moment, même pour vos expéditeurs les plus fiables, en raison du risque d'infection par virus par inadvertance. Vous trouverez ci-dessous une présentation des trois façons d'ignorer la vérification antispam pour un sous-ensemble de votre flux de messages.

Le premier outil à votre disposition est les stratégies de flux de messagerie HAT (Host Access Table). À l'aide des stratégies de flux de messages, vous pouvez identifier les expéditeurs par adresse IP (en utilisant des adresses IP numériques ou des noms DNS PTR), par score SenderBase, ou par liste d'autorisation ou de blocage DNS local. Une fois que vous avez identifié les expéditeurs comme étant approuvés dans un groupe d'expéditeurs du TAH, vous pouvez marquer ce groupe d'expéditeurs pour ignorer l'analyse antispam.

Par exemple, supposons que vous souhaitiez identifier un partenaire commercial spécifique, EXAMPLE.COM, qui ne devrait pas avoir de contrôle anti-spam sur son courrier. Vous devez trouver les adresses IP du serveur de messagerie SCU.COM (ou les enregistrements de pointeurs DNS). Dans ce cas, supposons que EXAMPLE.COM a des serveurs de messagerie qui auront des adresses IP avec des enregistrements PTR DNS de « smtp1.mail.scu.com » via « smtp4.mail.scu.com ». N'oubliez pas dans ce cas que nous examinons l'enregistrement PTR (parfois appelé DNS inverse) pour les serveurs de messagerie ; cela n'a rien à voir avec le nom de domaine que les utilisateurs de SCU.COM utiliseront pour le courrier sortant.

Vous pouvez créer un nouveau groupe d'expéditeurs (ou utiliser un groupe d'expéditeurs existant, tel que ALLOWLIST) avec Politiques de messagerie>Vue d'ensemble>Ajouter un groupe d'expéditeurs. Créons-en un appelé « NotSpammers ». Après avoir envoyé cette page, vous revenez à l'écran Politiques de messagerie>Vue d'ensemble, où vous aurez la possibilité d'ajouter une nouvelle stratégie pour ce groupe d'expéditeurs. Si vous cliquez sur Ajouter une stratégie, vous aurez la possibilité de créer une nouvelle stratégie. Dans ce cas, nous ne voulons remplacer la stratégie par défaut que dans une zone : Détection du spam. Donnez un nom à la stratégie et

définissez le comportement de connexion sur Accepter, puis faites défiler jusqu'à la section Détection du spam et définissez cette stratégie pour ignorer la vérification du spam. Soumettez cette nouvelle stratégie et n'oubliez pas de valider les modifications.

Une autre approche consiste à utiliser les stratégies de messagerie entrante pour ignorer l'analyse antispam. La différence entre les stratégies de TAH et de courrier entrant est que le TAH est entièrement basé sur les informations IP de l'expéditeur : l'adresse IP réelle, l'adresse IP telle que reflétée dans le DNS, le score SenderBase (basé sur l'adresse IP) ou une entrée de liste d'autorisation ou de bloc DNS basée sur l'adresse IP. Les stratégies de messagerie entrante sont basées sur les informations d'enveloppe de message : qui est le message ou de qui provient. Cela signifie qu'ils sont susceptibles d'être trompés par quelqu'un qui se fait passer pour un expéditeur de message. Cependant, si vous voulez simplement ignorer toutes les vérifications anti-spam pour les messages entrants provenant de personnes qui ont des adresses e-mail qui se terminent par "@exemple.com », vous pouvez le faire également.

Pour créer une telle stratégie, accédez à **Politiques de messagerie > Politiques de messagerie entrante > Ajouter une stratégie**. Cela vous permettra d'ajouter une stratégie qui définit un ensemble d'expéditeurs (ou de destinataires). Une fois que vous avez défini la stratégie de messagerie entrante, elle apparaît dans l'écran de présentation (Politiques de messagerie>Politiques de messagerie entrante). Vous pouvez ensuite cliquer sur la colonne « Antispam » et modifier les paramètres spécifiques de l'antispam pour cet utilisateur particulier.

Les paramètres antispam d'une stratégie particulière ont beaucoup d'options, mais dans ce cas, nous voulons simplement ignorer le contrôle antispam. Notez ici une autre différence entre les stratégies basées sur HAT et les stratégies de messagerie entrante : le TAH ne peut que vous permettre d'ignorer ou non l'analyse antispam, tandis que les stratégies de messagerie entrante ont un contrôle beaucoup plus important. Par exemple, vous pouvez choisir de mettre en quarantaine le spam de certains expéditeurs et de supprimer le spam d'autres expéditeurs.

La troisième option pour ignorer l'analyse antispam consiste à configurer et à utiliser un filtre de messages.

> **Note**: Les filtres de contenu ne peuvent pas être utilisés pour cela car les filtres de contenu se produisent après une analyse antispam.

L'une des actions dans les filtres de messages est « skip-spamcheck ». Le filtre de messages ci-dessous ignore la vérification antispam pour les expéditeurs qui ont une adresse IP particulière ou qui proviennent d'un nom de domaine particulier :

```
SkipSpamcheckFilter:
   if ( (remote-ip == '192.168.195.101') or
        (mail-from == '@example\\.com$')      )
   {
       skip-spamcheck();
   }
```

Pour plus d'informations sur l'utilisation des filtres de messages, consultez le Guide de l'utilisateur pour votre version d'AsyncOS déployée.

# Informations connexes

- Support et documentation techniques - Cisco Systems