Comment est-ce que je configure l'ESA pour ignorer la lecture d'anti-Spam et/ou d'antivirus pour mes expéditeurs de confiance ?

Contenu

Question :

Comment est-ce que je configure l'ESA pour ignorer la lecture d'anti-Spam et/ou d'antivirus pour mes expéditeurs de confiance ?

AsyncOS offre trois outils principaux que vous pouvez utiliser pour ignorer l'anti-Spam ou l'antivirus vérifiant vos expéditeurs de confiance. Veuillez noter que l'ESA n'informe pas ignorer l'antivirus examinant à tout moment, même pour assurer vos expéditeurs de confiance, en raison du potentiel pour l'infection négligente avec des virus. Ce qui suit est un examen des trois manières que vous pouvez ignorer l'anti-Spam vérifiant un certain sous-ensemble de votre flux des messages.

Le premier outil disponible à vous est les stratégies de flux de courrier de Tableau d'accès au hôte (CHAPEAU). Utilisant des stratégies de flux de courrier, vous pouvez identifier des expéditeurs par l'adresse IP (utilisant les adresses IP numériques ou les noms DNS PTR), par le score de SenderBase, ou par un whitelist local de DN ou la liste noire. Une fois que vous avez identifié des expéditeurs comme fait confiance dans un groupe d'expéditeur dans le CHAPEAU, vous pouvez alors marquer ce groupe d'expéditeur pour ignorer la lecture d'anti-Spam.

Par exemple, permettez-nous supposent que vous avez voulu identifier un partenaire commercial spécifique, EXAMPLE.COM, qui ne devrait pas avoir l'anti-Spam vérifiant sur leur messagerie. Vous devriez découvrir des adresses IP de serveur de messagerie SCU.COM (ou des enregistrements de pointeur de DN). Dans ce cas, permettez-nous supposent qu'EXAMPLE.COM a les serveurs de messagerie qui auront des adresses IP avec des enregistrements PTR de DN de "smtp1.mail.scu.com" à "smtp4.mail.scu.com." se souvenir dans ce cas que nous regardons l'enregistrement PTR (parfois appelé les DN inverses) pour les serveurs de messagerie ; ceci n'a rien à faire avec le nom de domaine que les gens à SCU.COM utiliseront pour le mail sortant.

Vous pourriez créer un nouveau groupe d'expéditeur (ou utiliser un groupe existant d'expéditeur, tel que WHITELIST) avec le groupe d'expéditeur de Policies>Overview>Add de messagerie. Créons un appelé « NotSpammers ». Après que vous ayez soumis cette page, vous serez retourné à l'écran de Policies>Overview de messagerie, où vous aurez l'occasion d'ajouter une nouvelle stratégie pour ce groupe d'expéditeur. Si vous cliquez sur en fonction « ajoutez la stratégie, » vous sera donné l'occasion de créer une nouvelle stratégie. Dans ce cas, nous voulons ignorer seulement la stratégie par défaut dans une zone : Détection de Spam. Donnez à la stratégie un nom et placez le comportement de connexion pour être « reçoivent, » faites descendre l'écran alors à la section de détection de Spam et réglé cette stratégie pour ignorer vérifier de Spam. Soumettez cette nouvelle stratégie, et n'oubliez pas « de commettre des modifications. »

Une approche alternative est d'employer des stratégies de messagerie entrante pour ignorer la lecture d'anti-Spam. La différence les stratégies entre le CHAPEAU et messagerie entrante est que le CHAPEAU est entièrement basé sur les informations IP sur l'expéditeur : l'adresse IP vraie, l'adresse IP comme envisagé dans les DN, le score de SenderBase (qui est basé sur l'adresse IP) ou une entrée de whitelist ou de liste noire de DN basée sur l'adresse IP. Des stratégies de messagerie entrante sont basées sur les informations d'enveloppe de message : derrière à qui le message est ou de qui le message est. Ceci signifie qu'ils sont susceptibles d'être dupé par quelqu'un qui personnifie un expéditeur de message. Cependant, si vous voulez ignorer simplement tout l'anti-Spam vérifiant la messagerie entrante provenant les personnes qui ont des adresses e-mail qui finissent dans « @example.com, » vous pourriez faire cela aussi bien.

Pour créer une telle stratégie, allez envoyer par mail la stratégie de Policies>Add de messagerie de Policies>Incoming. Ceci vous permettra d'ajouter une stratégie qui définit un ensemble d'expéditeurs (ou de récepteurs). Une fois que vous définissez la stratégie de messagerie entrante, elle apparaîtra dans l'écran d'aperçu (stratégies de messagerie de Policies>Incoming de messagerie). Vous pouvez alors cliquer sur en fonction la colonne de « anti-Spam » et éditer les configurations spécifiques pour l'anti-Spam pour cet utilisateur particulier.

Les configurations d'anti-Spam pour une stratégie particulière ont un bon nombre d'options, mais dans ce cas, nous voulons simplement ignorer vérifier d'anti-Spam. Notez ici une autre différence les stratégies entre la stratégie basée sur chapeau et messagerie entrante : le CHAPEAU peut vous a seulement permis d'ignorer ou ne pas ignorer la lecture d'anti-Spam, alors que les stratégies de messagerie entrante ont un contrôle beaucoup plus grand. Par exemple, vous pourriez choisir de mettre en quarantaine le Spam de certains expéditeurs, et supprimez le Spam d'autres expéditeurs.

La troisième option pour ignorer la lecture d'anti-Spam est dans des filtres de message. (Note que des filtres satisfaits ne peuvent pas être utilisé pour ceci parce que les filtres satisfaits se produisent après que la lecture d'anti-Spam se soit déjà produite). Une des actions dans des filtres de message est « saut-spamcheck. » Le filtre de message ci-dessous ignorera l'anti-Spam vérifiant les expéditeurs qui ont une adresse IP particulière ou qui proviennent un nom de domaine particulier :

```
SkipSpamcheckFilter :
    si ((distant-IP == '192.168.195.101') ou
         (\ de @example messagerie- == « \ .com$"))
    {
        saut-spamcheck() ;
    }
```