Protection contre les usurpations à l'aide de la vérification de l'expéditeur

Contenu

Introduction

Par défaut, l'appliance de sécurité de la messagerie Cisco (ESA) n'empêche pas la remise en entrée des messages adressés “ du même domaine ” le même domaine. Cela permet aux messages d'être “ usurpés ” par des sociétés extérieures qui font des affaires légitimes avec le client. Certaines entreprises font appel à des tiers pour envoyer des courriels au nom de l'entreprise, comme Health Care, Travel Agencies, etc.

Protection contre les usurpations à l'aide de la vérification de l'expéditeur

Configurer la politique de flux de courrier (MFP)

1. À partir de la GUI : **Politiques de messagerie > Politiques de flux de messagerie > Ajouter une stratégie...**
2. Créer une MFP à l'aide d'un nom pertinent tel que SPOOF_ALLOW
3. Dans la section *Vérification de l'expéditeur*, modifiez la configuration *Utiliser la table des exceptions de vérification de l'expéditeur* de **Utiliser par défaut** à **Éteindre**.
4. Dans **Politiques de messagerie > Politiques de flux de messagerie > Paramètres de stratégie par défaut**, définissez la configuration *Utiliser la table des exceptions de vérification de l'expéditeur* sur **Activé**.

Configuration de HAT

1. À partir de l'interface utilisateur graphique : **Politiques de messagerie > Vue d'ensemble du TAH > Ajouter un groupe d'expéditeurs...**
2. Définissez le nom en fonction de la MFP créée précédemment, à savoir SPOOF_ALLOW.
3. Définissez la commande de sorte qu'elle soit au-dessus des groupes d'expéditeurs ALLOWLIST et BLOCKLIST.
4. Affectez la stratégie **SPOOF_ALLOW** à ces paramètres de groupe d'expéditeurs.
5. Cliquez sur **Envoyer et ajouter des expéditeurs..**
6. Ajoutez des adresses IP ou des domaines pour toutes les parties externes que vous voulez autoriser à usurper le domaine interne.

Configurer la table des exceptions

1. À partir de la GUI : **Politiques de messagerie > Table des exceptions > Ajouter une exception**

de vérification de l'expéditeur...

2. Ajouter le domaine local à la table des exceptions de vérification de l'expéditeur
3. Définir le *Comportement* par **Rejeter**

Vérification

À ce stade, le courrier provenant de *your.domain* vers *your.domain* sera rejeté, sauf si l'expéditeur figure dans la liste SPOOF_ALLOW du groupe d'expéditeurs, car il sera associé à un MFP qui n'utilise pas la table d'exceptions de vérification de l'expéditeur.

Un exemple de ceci peut être vu en effectuant une session Telnet manuelle à l'écouteur :

```
$ telnet example.com 25
Trying 192.168.0.189...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP
helo example.com
250 example.com
mail from: <test@example.com>
553 Envelope sender <test@example.com> rejected
```

La réponse SMTP 553 est un résultat de réponse directe de la table des exceptions telle que configurée sur le ESA à partir des étapes ci-dessus.

Dans les journaux de messagerie, vous pouvez voir que l'adresse IP 192.168.0.9 ne figure pas dans l'adresse IP valide du groupe d'expéditeurs correct :

```
Wed Aug 5 21:16:51 2015 Info: New SMTP ICID 2692 interface Management (192.168.0.189) address
192.168.0.9 reverse dns host my.host.com verified no
Wed Aug 5 21:16:51 2015 Info: ICID 2692 RELAY SG RELAY_SG match 192.168.0.0/24 SBRS not enabled
Wed Aug 5 21:17:02 2015 Info: ICID 2692 Address: <test@example.com> sender rejected, envelope
sender matched domain exception
```

Une adresse IP autorisée correspondant à l'exemple de configuration des étapes ci-dessus est présentée comme suit :

```
Wed Aug 5 21:38:19 2015 Info: New SMTP ICID 2694 interface Management (192.168.0.189) address
192.168.0.15 reverse dns host unknown verified no
Wed Aug 5 21:38:19 2015 Info: ICID 2694 ACCEPT SG SPOOF_ALLOW match 192.168.0.15 SBRS not
enabled
Wed Aug 5 21:38:29 2015 Info: Start MID 3877 ICID 2694
Wed Aug 5 21:38:29 2015 Info: MID 3877 ICID 2694 From: <test@example.com>
Wed Aug 5 21:38:36 2015 Info: MID 3877 ICID 2694 RID 0 To: <robert@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 Subject 'This is an allowed IP and email'
Wed Aug 5 21:38:50 2015 Info: MID 3877 ready 170 bytes from <test@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim verdict using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim AV verdict using Sophos CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 antivirus negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 AMP file reputation verdict : CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 Outbreak Filters: verdict negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 queued for delivery
```

```
Wed Aug 5 21:38:51 2015 Info: New SMTP DCID 354 interface 192.168.0.189 address 192.168.0.15
port 25
Wed Aug 5 21:38:51 2015 Info: Delivery start DCID 354 MID 3877 to RID [0]
Wed Aug 5 21:38:51 2015 Info: Message done DCID 354 MID 3877 to RID [0] [('X-IPAS-Result',
'A0GJMwA8usJV/w8AqMBbGQSEFRqFGKUygmUBkV2GMAKBcQEBAgEBAQOBB4QbKIEIhxuCQbxmoDcRAYNPAYE0AQSqSZB5gXA
BAQgCAYQjgT8DAgE'), ('X-IronPort-AV', 'E=Sophos;i="5.15,620,1432612800"; \r\n
d="scan\'";a="3877"')]
Wed Aug 5 21:38:51 2015 Info: MID 3877 RID [0] Response '2.0.0 Ok: queued as 1D74E1002A8'
Wed Aug 5 21:38:51 2015 Info: Message finished MID 3877 done
Wed Aug 5 21:38:56 2015 Info: DCID 354 close
```

Informations connexes

- ESA, SMA et WSA Grep avec Regex to Search Logs
- Détermination de la répartition des messages ESA
- Support et documentation techniques - Cisco Systems