Charriez la protection utilisant la vérification d'expéditeur

Contenu

Introduction

Par défaut l'appliance de sécurité du courrier électronique de Cisco (ESA) n'empêche pas la livraison d'arrivée des messages qui sont adressés « » du même domaine allant au même domaine. Ceci permet des messages « à charrier » par les sociétés extérieures qui légitiment l'entreprise avec le client. Quelques sociétés comptent sur l'organisation de tiers pour envoyer l'email au nom de la société telle que la santé, des agences de voyages, etc.

Charriez la protection utilisant la vérification d'expéditeur

Configurez la stratégie de flux de courrier (MFP)

1. À partir de la GUI : **Les stratégies de messagerie > les stratégies de flux de courrier > ajoutent la stratégie…**
2. Créez un nouveau MFP utilisant un nom qui est approprié comme SPOOF_ALLOW
3. Dans la section de *vérification d'expéditeur*, changez la configuration de *Tableau d'exception de vérification d'expéditeur d'utilisation du* **par défaut d'utilisation à HORS FONCTION**.
4. Dans des **stratégies de messagerie > des stratégies de flux de courrier > des paramètres de stratégie par défaut**, placez la configuration de *Tableau d'exception de vérification d'expéditeur d'utilisation à* **en fonction**.

Configurez le CHAPEAU

1. À partir de la GUI : **Les stratégies de messagerie > l'aperçu de CHAPEAU > ajoutent le groupe d'expéditeur…**
2. Placez le nom en conséquence au MFP créé plus tôt, c.-à-d. SPOOF_ALLOW.
3. Placez la commande ainsi elle est des groupes au-dessus WHITELIST et de LISTE NOIRE d'expéditeur.
4. Assignez la stratégie **SPOOF_ALLOW aux** configurations de ce groupe d'expéditeur.
5. Cliquez sur Submit **et ajoutez les expéditeurs…**
6. Ajoutez l'IP ou les domaines pour tous les interlocuteurs externes aux lesquels vous voulez permettre pour charrier le domaine interne.

Configurez le Tableau d'exception

1. À partir de la GUI : **Le Tableau de stratégies > d'exception de messagerie > ajoutent**

l'exception de vérification d'expéditeur…

2. Ajoutez le domaine local au Tableau d'exception de vérification d'expéditeur
3. Placez le *comportement* **pour rejeter**

Vérifiez

En ce moment, la messagerie provenant *your.domain à* your.domainwould soit rejetée à moins que l'expéditeur soit répertorié dans le groupe SPOOF_ALLOW d'expéditeur, car il serait associé à un MFP qui n'utilise pas la table d'exception de vérification d'expéditeur.

Un exemple de ceci serait vu en se terminant une session de telnet manuelle à l'auditeur :

```
$ 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 du SMTP 553 est un résultat de réponse directe de la table d'exception comme configurée sur l'ESA des étapes ci-dessus.

Des logs de messagerie, vous pouvez voir que l'adresse IP de 192.168.0.9 n'est pas dans l'adresse IP valide pour le groupe correct d'expéditeur :

```
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 permise s'assortissant avec l'exemple de configuration des étapes ci-dessus serait vue 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

- Grep ESA, SMA, et WSA avec l'expression régulière pour rechercher des logs
- Détermination de disposition de message ESA
- Support et documentation techniques - Cisco Systems