Comment est-ce que je peux vérifier que ma règle d'accès TCPREFUSE ou d'ANOMALIE fonctionne ?

Contenu

Comment est-ce que je peux vérifier que ma règle d'accès TCPREFUSE ou d'ANOMALIE fonctionne ?

Environnement : Appliance de sécurité du courrier électronique de Cisco (ESA), toutes les versions d'AsyncOS

TCPREFUSE et **ANOMALIE** sont les deux comportements de connexion qui sont normalement associés avec la stratégie BLOQUÉE de flux de courrier. Ces règles d'accès te permettent pour choisir si bloquer des messages d'un serveur distant avec une notification (rebond dur) ou simplement à l'arrêter la connexion. Voyez ce qui est la différence entre l'ANOMALIE et le TCPREFUSE ?

Si vous voudriez déterminer si un serveur distant est dû abandonné à **TCPREFUSE** ou à **ANOMALIE**, vous pouvez visualiser des entrées dans les logs de messagerie. Les logs de messagerie contiendront seulement des entrées pour **TCPREFUSE** si se connecter bavard de connexion est activé. Supplémentaire vous pouvez employer un analyseur de protocole, tel que le **tcpdump**, pour surveiller les conversations au niveau de paquet. Quand utilisant un analyseur de protocole, vous noterez différentes conversations pour **TCPREFUSE** contre l' **ANOMALIE**.

L'écoulement de connexion TCP entre l'ESA et le message transfer agent distant (MTA) pour la connexion d'anomalie est comme ceci :

```
                          SYN
Remote MTA -----------> ESA
                        SYN, ACK
ESA -----------> Remote MTA
                          ACK
Remote MTA -----------> ESA
                        5XX Code
ESA -----------> Remote MTA
                         FIN, ACK
ESA -----------> Remote MTA
                          ACK
Remote MTA -----------> ESA
                         FIN, ACK
Remote MTA -----------> ESA
                          ACK
```

```
ESA -----------> Remote MTA
```

L'écoulement de connexion TCP entre l'ESA et le distant MTA pour la connexion d'ordures de TCP est comme ceci :

```
                           SYN
Remote MTA -----------> ESA
                       SYN, ACK
ESA -----------> Remote MTA
                            ACK
Remote MTA -----------> ESA
                        RST, ACK
ESA -----------> Remote MTA
```