Bastionar Zimbra

Protección contra el spam

Denegamos que se pueda enviar o recibir correos desde usuarios desconocidos

```
zmprov mcf zimbraMtaSmtpdRejectUnlistedRecipient yes
zmprov mcf zimbraMtaSmtpdRejectUnlistedSender yes
zmmtactl restart
zmconfigdctl restart
```

DoS

Si al intentar enviar un coreo desde Zimbra nos aparece un mensaje de rerror del tipo “Se ha producido un error en el servicio de red”, puede ser que el Zimbra crea que le estamos haciendo un ataque DoS y nos tenga bloqueado.

Para revisar lo que está ocurriendo tenemos que revisar los logs:

```
tail -f  /opt/zimbra/log/sync.log
```

Buscamos eventos del tipo DosFilter

```
cat  /opt/zimbra/log/zmmailboxd.out  | grep DoSFilter
```

```
 at org.eclipse.jetty.servlets.DoSFilter.doFilter(DoSFilter.java:299)
```

Si aparecen eventos del tipo DosFilter, buscamos en zmmailboxd para saber si es nuestra ip la que está siendo bloqueada

```
cat  /opt/zimbra/log/zmmailboxd.out  | grep 'DOS ALERT'
```

Una vez que verificamos que nuestra ip está siendo bloqueada, ejecutamos el siguiente comando para permitir nuestra red y que no sea detectada como un ataque DosS

```
    zmprov mcf +zimbraHttpThrottleSafeIPs 192.168.1.0/24
```

Reiniciar los servicios

```
    zmmailboxdctl restart
```

Para verificar si las direcciones se han añadido correctamente

```
cat /opt/zimbra/log/mailbox.log | grep whitelist
```

También podemos cambiar el número de intentos de inicio de sesión incorrectos y el tiempo entre reintentos

```
zmprov mcf zimbraInvalidLoginFilterDelayInMinBetwnReqBeforeReinstating 25
zmprov mcf zimbraInvalidLoginFilterMaxFailedLogin 5
zmmailboxdctl restart
```

Referencias

- https://www.jorgedelacruz.es/2014/09/08/zimbra-seguridad-ii-parte-enforcing-a-match-between-from-address-and-sasl-username-en-zimbra-8-5/
- http://wiki.zimbra.com/wiki/DoSFilter

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=aplicaciones:zimbra:seguridad

Last update: **182023/01/ 13:36**