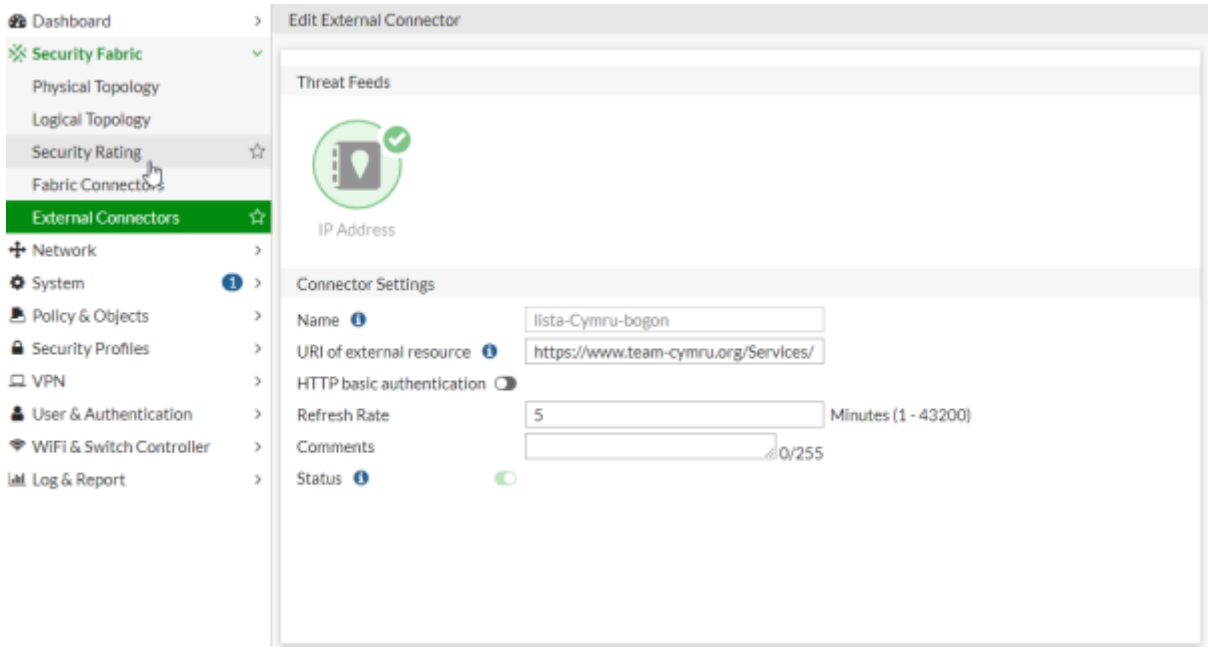
fortigate, 6.4, filtrar, ip, block

Filtrado de IPs usando una fuente externa

Supongamos que tenemos un servidor de correos que es continuamente atacado desde diferentes ips y usando diversas combinaciones de usuarios y/o contraseñas. Normalmente tiene estudiado el tema y limitan los ataques en numero de intentos y en el intervalo para que los sistemas automáticamente no los bloquen.

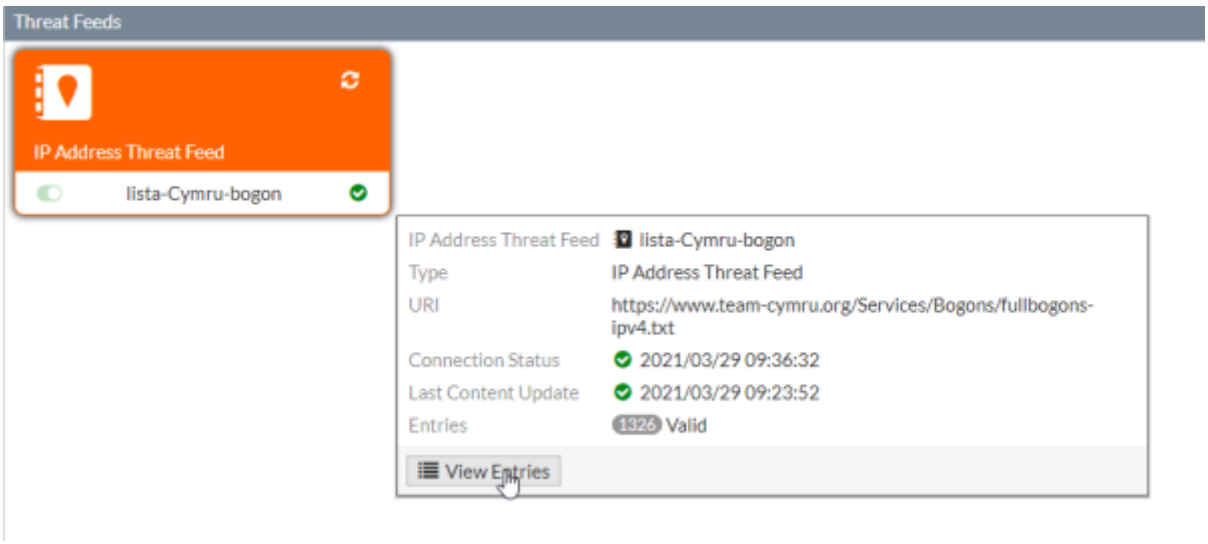
Nosotros podemos desde el Fortiview ver esas direcciones y banearlas permanentemente pero **Cuando reiniciamos ese cortafuegos, esas ip baneadas desaparecen** ya que se almacenan en la RAM del equipo y no se comparten en el caso de tener HA.

Para solucionarlo vamos a utilizar importar una lista de ips usando un nuevo **External Connector** llamado IP address Threat Feed. Desde Security Fabric → Externan Connectors . Creamos uno nuevo del tipo Threat Feeds

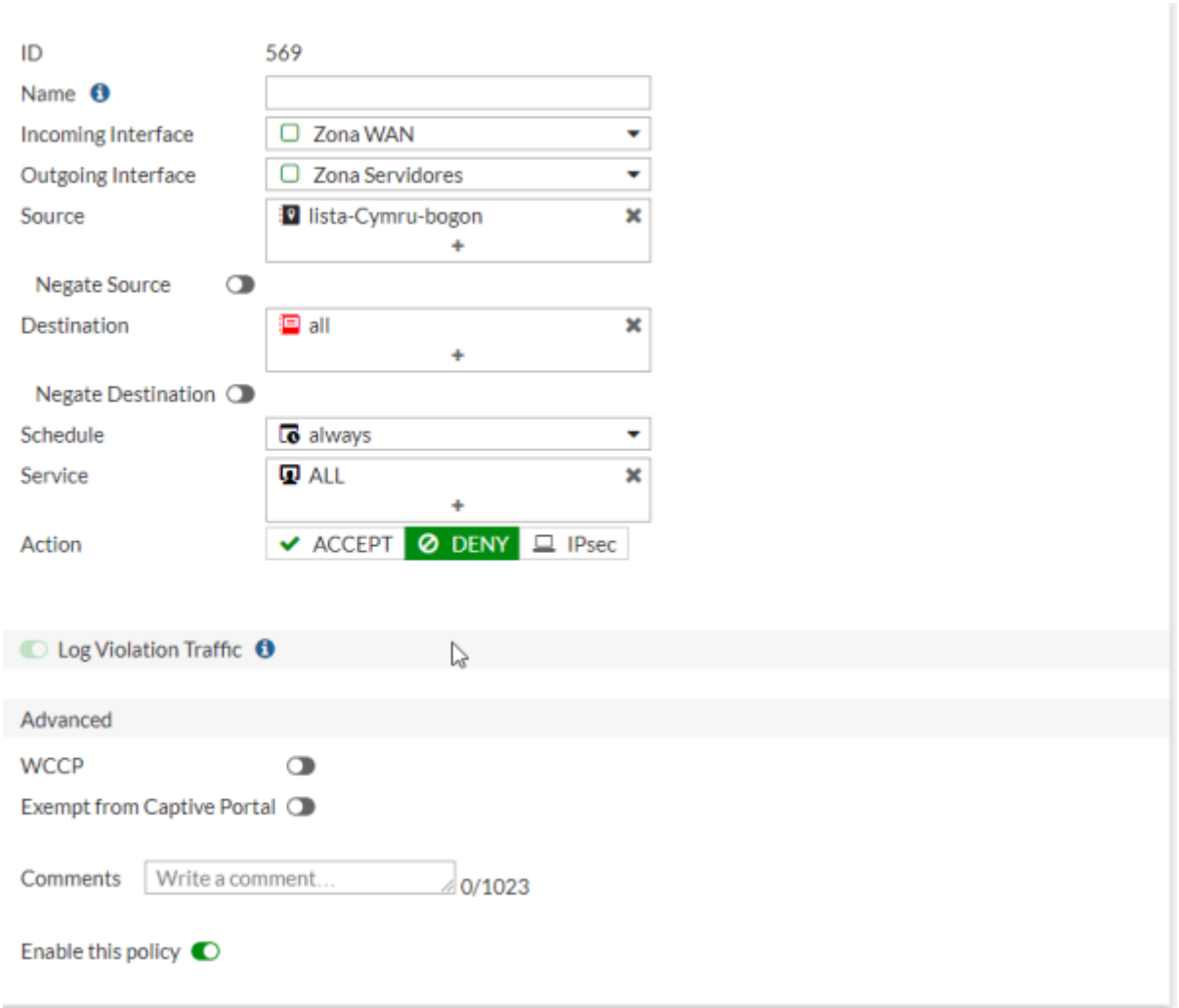


En mi caso he creado un Threat Feeds usando la lista del Teeam-Cymru.org (https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt)

Para comprobar la lista de ips , pincha sobre el nuevo conector y pordrás ver su validez y el número de entradas



Una vez creada la lista ya sólo necesitamos crear una nueva política usando como dirección está lista para bloquear su acceso



Listas con host sospechosos

- https://iplists.firehol.org/

Referencias

- http://geekstuff.org/2019/12/24/threat-feed-fortigate/
- https://yurisk.info/2020/08/08/fortigate-using-external-threat-feeds-and-ip-domain-block-lists/

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

Permanent link:
https://intrusos.info/doku.php?id=hardware:fortigate:filtradoip&rev=1640612024

Last update: **2023/01/18 14:16**