

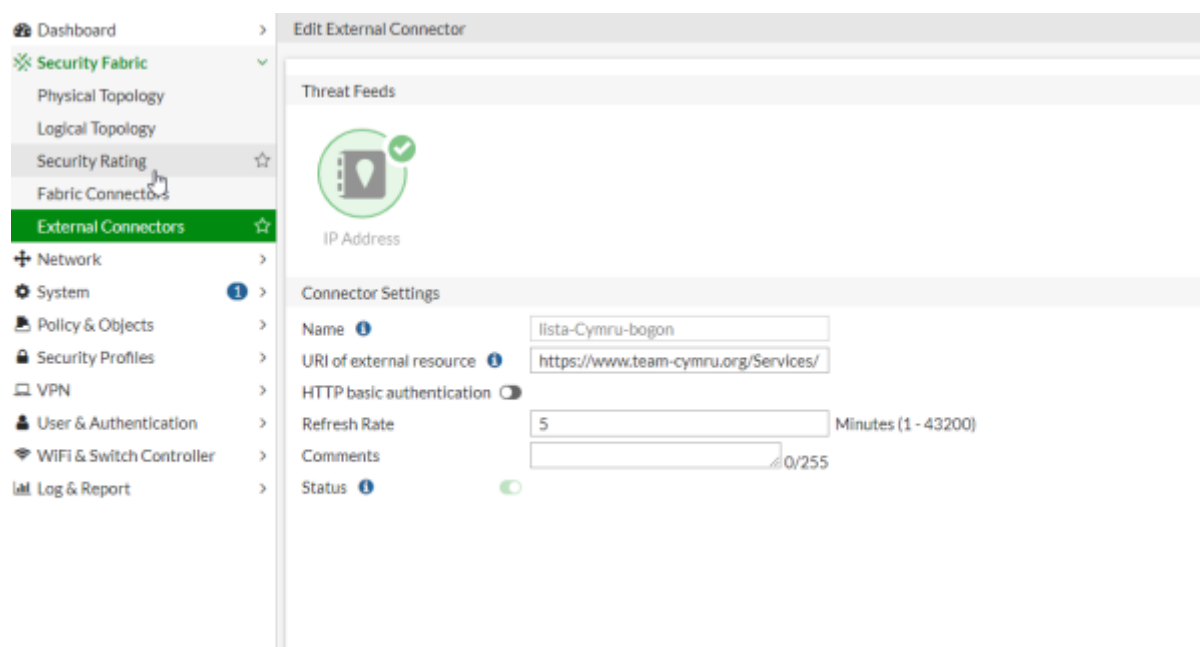
[fortigate](#), [6.4](#), [filtrar](#), [ip](#), [block](#)

Filtrador 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



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

Threat Feeds



IP Address Threat Feed

lista-Cymru-bogon

IP Address Threat Feed

lista-Cymru-bogon

TypeIP Address Threat Feed

URI<https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt>

Connection Status

2021/03/29 09:36:32

Last Content Update

2021/03/29 09:23:52

Entries

1326

Valid

View Entries

From:
<https://intrusos.info/> - LCWIKI

Permanent link:
<https://intrusos.info/doku.php?id=hardware:fortigate:filtradoip&rev=1617007470>

Last update: 2023/01/18 14:16

