Deny Public Network Access (DPNA) and Elastic Query

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:23 AM PDT

Contents

Issue

There is a known limitation with Deny Public Network Access (DPNA) and Elastic Query. The reason for this is that DPNA only allows Private Link logins to access the server.

In order for a login to go over PrivateLink, its TCP connection needs to originate inside the VNet that a PL has been set up for. This doesn't work for Elastic Query since the connection originates from the database itself and databases do not live inside customer VNets.

Impact /timeline

There is an Azure-wide feature in incubation that will allow PaaS-to-PaaS connections like this to be allowed under DPNA. We hope to have some preview in early 2022.

Workaround

In the meantime, the best solution is to enable Public Network Access and Allow All Azure Resources to connect. A possible solution if Allow All Azure Resources is not secure enough is to create IP firewall rules for each database. You should be able to catch the firewall errors in EQ and get the public IP of the database attempting to log in.

You could then add that firewall rule to the destination server and retry the query. It's experimental, but could be a legit workaround for the time being

How good have you found this content?