

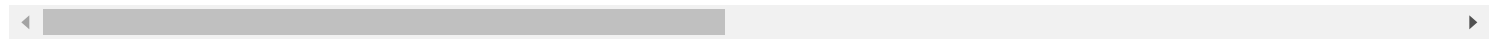
Asymmetric Routing Issues

Last updated by | Vitor Tomaz | Feb 18, 2021 at 3:30 AM PST

Issue

Cx is not able to connect the Azure SQL MI database from on premise SSMS client when "Azure Firewall service" placed getting the following "semaphore timeout" error message.

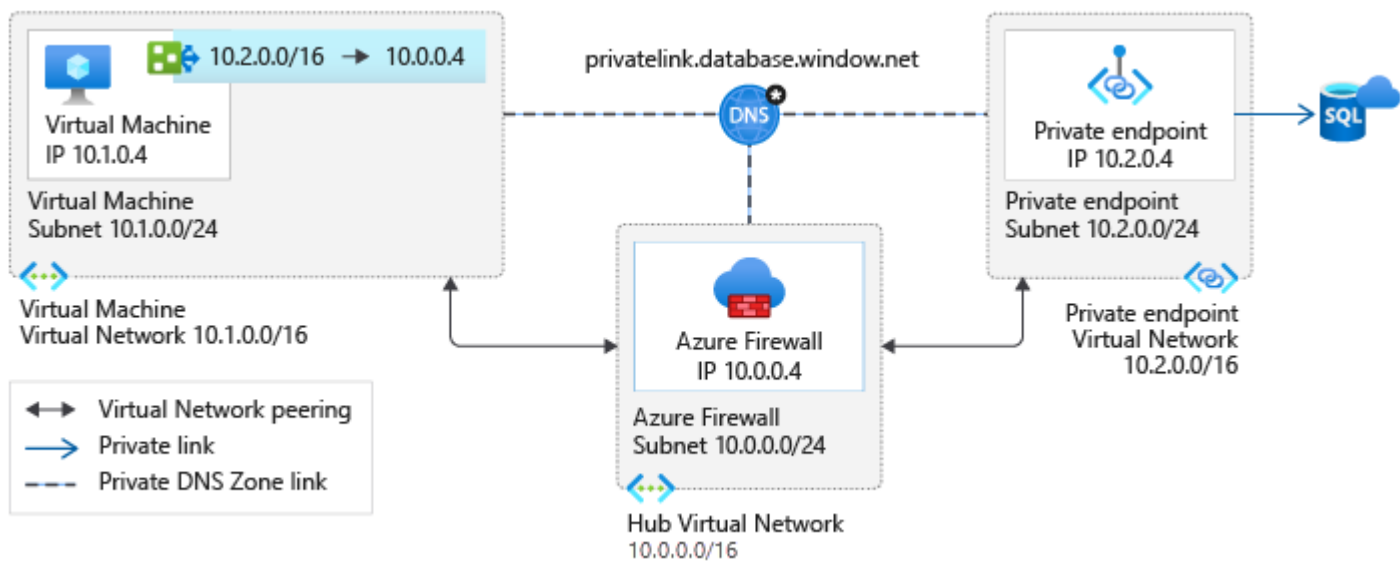
A connection was successfully established with the server, but then an error occurred during the pre-login han



cX is able to connect the Azure SQL MI without Azure Firewall service successfully using the site to site VPN from the on premise location.

Troubleshoot

Customer's network topology



<https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall>

Above network topology works for Azure SQL DB private link, but not SQL MI. SQL Managed Instance doesn't support Azure private link or Azure private endpoint. SQL Managed Instance has private deployment model, but it has nothing to do with private endpoint.

Capture Network Trace

1. From captured network trace, you can identify if the packet is received or not.
2. Involve network team to help check the packet loss through Azure firewall.






Asymmetric Routing

There is an option "Propagate gateway routes" in route table configuration :






[Home](#) > [rt-zhizhwanmi](#)

rt-zhizhwanmi | Configuration



Route table

 Search (Ctrl+/)
 <<
  Save
  Discard
 Overview Activity log Access control (IAM) Tags Diagnose and solve problems


Settings

 Configuration Routes Subnets Properties Locks

Automation

 Tasks (preview) Export template

Support + troubleshooting

 Effective routes New support requestPropagate gateway routes ⓘ

Yes



No

With BGP propagation enabled on SQL MI subnet route table, the traffic will be:

1. Client(SYN) >>> VPN >>> Firewall(allow) >>> SQL MI
2. SQL MI(SYN+ACK) >>> VPN >>> Client # SQL subnet learnt the route from Gateway instead of UDR, so it sent the packet to client without pass through Firewall.
3. Client(ACK) >>> VPN >>> Firewall(deny) # deny due to the firewall did not receive the SYN+ACK
4. Client(pre-login) >>> VPN >>> Firewall (deny) # pre-login was sent due to client believed that the TCP 3-way handshake complete

Above scenario is known as "Asymmetric Routing". In asymmetric routing, reverse network traffic takes a different path from the original flow. Due to stateful device like firewall, it will drop the network packets because the stateful device didn't detect that traffic originated with the device itself.

[See details about Asymmetric Routing](#) 

Solution

Disable BGP propagation on SQL MI subnet route table.

After disable BGP propagation on SQL MI subnet route table, the traffic will be:

1. Client(SYN) >>> VPN >>> Firewall(allow) >>> SQL MI
2. SQL MI(SYN+ACK) >>> Firewall(allow)>>> VPN >>> Client
3. Client(ACK) >>> VPN >>> Firewall(allow) >>> SQL MI
4. Client(pre-login) >>> VPN >>> Firewall(allow) >>> SQL MI
5. SQL MI(response) >>> Firewall(allow)>>> VPN >>> Client

Additional Information

[Tutorial: Deploy and configure Azure Firewall in a hybrid network using the Azure portal](#) 

Please be noted that Managed Instance VNET is one of the Spoke VNET, so it need to follow the practices to set up peering, correct routes to hub network as well as NSG.

Classification

How good have you found this content?

