VNET - Service for Azure SQL Database

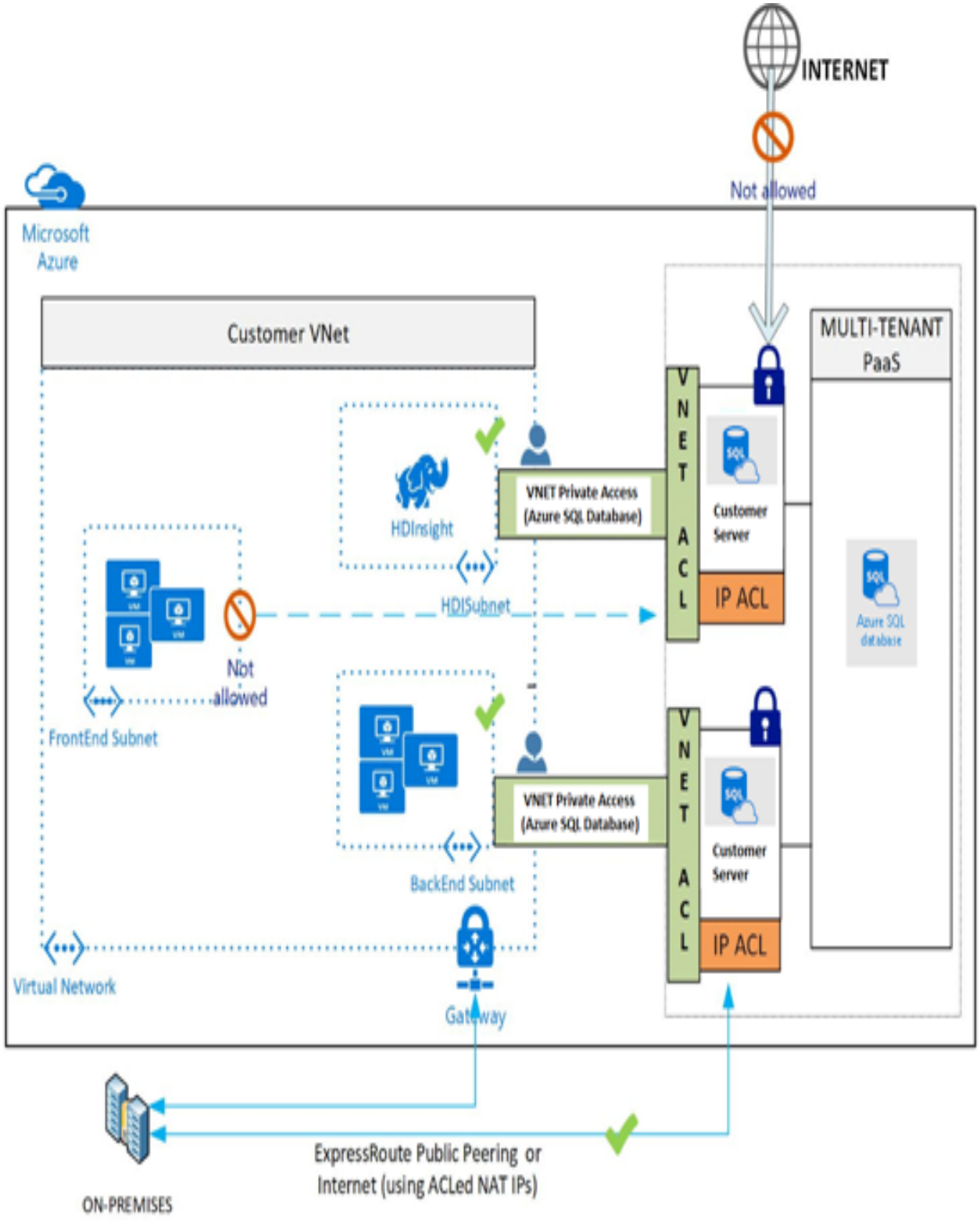
Last updated by | Vitor Tomaz | Aug 5, 2020 at 12:40 PM PDT

Contents

VNET - Service for Azure SQL Database

Getting Started

Azure SQLDB allows you to set firewall rules for specific public IPs and allows you to 'Allow all Azure Services' IPs to connect to your Servers. Customers looking for finer grained connectivity limitations requires the customer to provision a Static Public IP which can be hard to manage and costly when done at scale. This feature allows customers to limit connectivity to their Azure SQL Database Servers from given Subnets within a VNET.



Benefits

VNET Private Access allows you to use all the benefits of our PaaS service like Geo-replication, backup/restore, Active directory integration and all other features while limiting connectivity in an easy to use fashion. Even though the connectivity will be on Azure SQL Databases public endpoint the traffic will stay within the Azure backbone network. This direct route will be preferred over any forced-tunneling route to take Internet traffic back to on-premises. We also provide for separation of roles with the ability to provision VNET Private Access either on the Network Admin, the Database Admin, splitting the roles between these two or ability to create a new entity with the help of custom RBAC roles.

Limitations

1. Each SQL Server can have up to 128 Virtual Network based ACLs.
2. Applies only to ARM VNETs
3. Does not extend to on-premises via Expressroute or Site-to-Site (S2S) VPN or Peered VNets.

Considerations

At the time of this preview, Network Security Groups (NSGs) should be opened to Internet to allow Azure SQL Database traffic. In future, NSGs could be opened to only IP ranges for the PaaS services. IP tags for Azure SQL Database are on the roadmap for CY17.

With VNET Private Access, source IP addresses of resources in your VNet's subnet will switch from using public IPV4 addresses to VNet's private addresses, for traffic to Azure SQL Database. Any existing open TCP connections to your databases service may be closed, during this switch. Please make sure no critical tasks are run when Private Access is turned on or off.

When the switch to Private Access is completed there may be preexisting connections outside the VNET/Subnet, for maximum security it is recommended that you close all connections to your databases.

If traffic to Azure SQL Database is to be inspected by a network virtual appliance (NVA), it is recommended that VNET Private Access is turned on for the NVA subnet, instead of the subnet where the Azure SQL Database is originating from in the given VNET.

When Private Access is turned ON a Subnet it is sequentially applied to all VMs in that Subnet, the call commits only when Private Access is successfully applied to all VMs. You will be able to ACL given VNET/Subnet your Server only after Private Access from the VNET/Subnet is successfully applied. So there can be potential downtime after Private Access call is issued till when you ACL the Server.

How good have you found this content?