

Private Link

Last updated by | Subbu Kandhaswamy | May 9, 2022 at 11:05 PM PDT

Contents

- [What is Private Link](#)
- [Concepts](#)
 - [Features and Capabilities](#)
 - [Available Services and Locations](#)
 - [Limitations](#)
- [Setup](#)
 - [Public Doc Reference](#)
 - [Internal Reference](#)

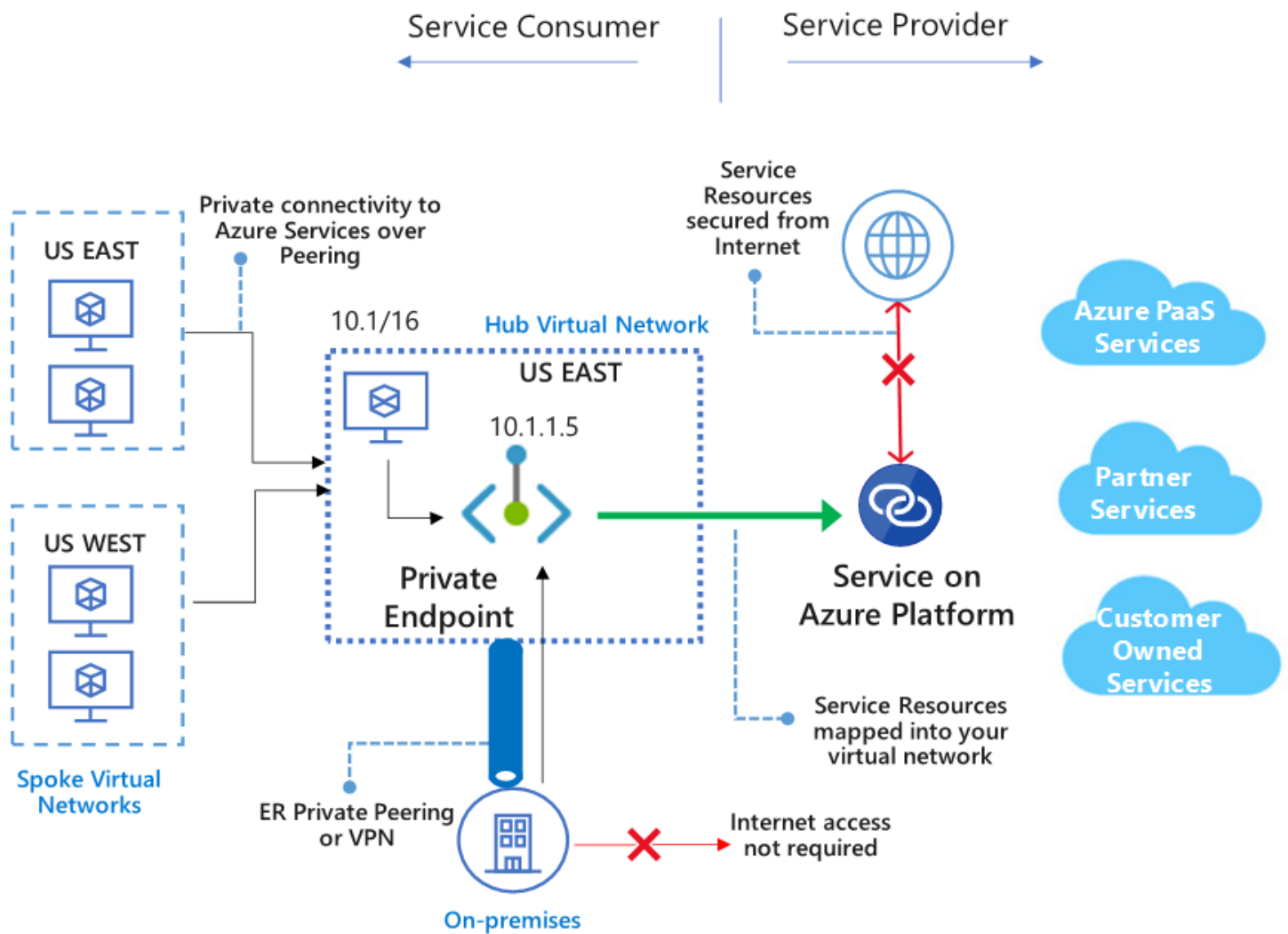
What is Private Link

Azure service resources currently are reachable using public endpoints, for customers with strict network security and compliance regulations, additional technologies are required to connect and secure their access to Azure services.

- Network inspection to validate access to resources from my own organization and prevent exfiltration of critical data to other tenants using the same service provider
- Network translations or Proxy devices to connect over a public endpoint.

Both options not only impact security and performance but also increase the management overhead of validating the consumption of each service based on their network requirements.

Azure PaaS resources provide a managed experience for workloads specialized on data store and processing, reachability from customer's private networks like Virtual Networks and on-premises completely isolated is extremely important.



Concepts

- **Public Endpoint:** A publicly accessible IP address that is used to provide access over public networks, works to connect across organizations
- **Private Endpoint:** A private IP address that is used to provide connectivity from private networks, it's typically defined but not limited to RFC1918 space, routing configuration is limited to network devices within the same private network
- **Private Endpoint (resource):** An Azure network resource that allocates private IP address space for a give service resource, provides network identification to any access to an associated resource.
- **Azure PaaS Resource:** An Azure resource representing the service element being consumed, typically Sql Server, Storage account, Cosmos DB account, etc.

Features and Capabilities

Private Link: Feature Set

Private Endpoints

- ✓ Connectivity from On premises and within VNet
- ✓ Connectivity from peered VNets(regional and global)
- ✓ Mixed deployments with VMs on the same subnet
- ✓ DNS Integration with Private Zone DNS & Custom DNS
- ✓ Approval workflow for cross AD support
- ✓ Private Endpoint to a PaaS resource on a different region
- ✓ Application Security Groups for group IP addresses **(GA)**
- ✓ Network Security Groups to restrict traffic to PaaS resources **(GA)**
- ✓ Gateway bypass for on premise traffic **(GA)**



Available Services and Locations

Check updated information at: <https://docs.microsoft.com/en-us/azure/private-link/private-link-overview#availability>

Limitations





Check updated information at: <https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview#limitations>

Limitation	Description	Mitigation
Network Security Group (NSG) rules and User Defined Routes do not apply to Private Endpoint	NSG is not supported on private endpoints. While subnets containing the private endpoint can have NSG associated with it, the rules will not be effective on traffic processed by the private endpoint. You must have network policies enforcement disabled to deploy private endpoints in a subnet. NSG is still enforced on other workloads hosted on the same subnet. Routes on any client subnet will be using an /32 prefix, changing the default routing behavior requires a similar UDR	Control the traffic by using NSG rules for outbound traffic on source clients. Deploy individual routes with /32 prefix to override private endpoint routes. NSG Flow logs and monitoring information for outbound connections are still supported and can be used

Setup

- [How to set up Private Link for Azure SQL Database](#)
- [Azure SQL DB Private Link Private Endpoint Connectivity Troubleshooting](#)

Public Doc Reference

- <https://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sql-db-private-link-private-endpoint-connectivity/ba-p/1235573> 
- <https://docs.microsoft.com/en-us/azure/private-link/private-link-service-overview> 
- <https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview> 
- <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-private-endpoint-overview> 
- <https://docs.microsoft.com/en-us/azure/private-link/> 
- <https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet#enable-vnet-integration> 

Internal Reference

- [Private Link - Limitations](#)
- [Private Link for PaaS Overview.pptx](#)
- [Private Link - Collaboration With VNET depth queue](#)

How good have you found this content?



How good have you found this content?

