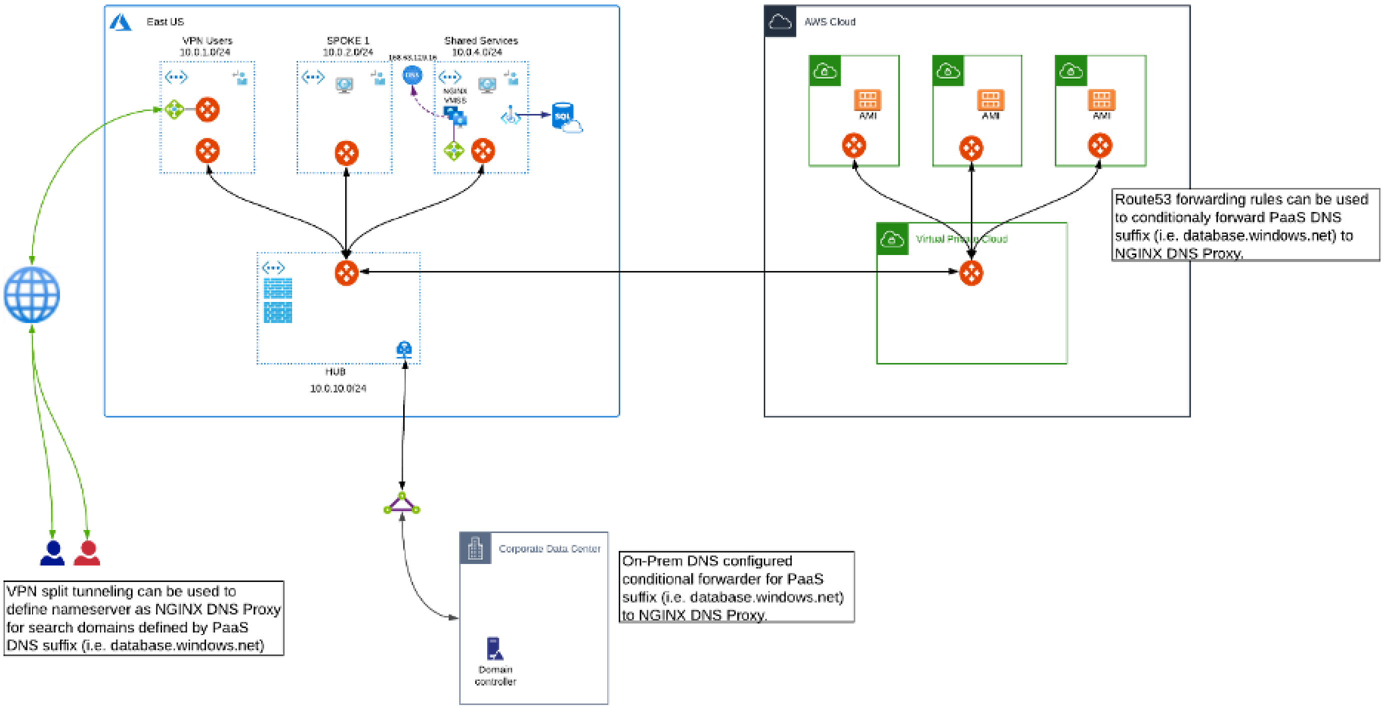
Azure Multi-Cloud Private Link for PaaS

Overview

Azure Private Link is a service that provides private connectivity from an Azure virtual network (VNET) to Azure Platform as a Service (PaaS), customer-owned, or Microsoft partner services. As organizations look to refactor legacy workloads to leverage Azure's rich PaaS offerings, publish applications for customer consumption, or leverage partner solutions, Private Link offers a way to do this over private connections rather than public endpoints.

This Azure Multi-Cloud Private Link for PaaS plus Aviatrix multi-cloud network design fills the gaps in current Azure Private Link for PaaS deployment models. Leveraging the Aviatrix cloud network platform and third-party integrations, Aviatrix delivers simplified access to Private Link enabled PaaS services, regardless of where the source resides – Remote VPN users, on-prem users, or an application residing in AWS – this Azure / Aviatrix network design offers users private access to PaaS resources.



Route53 forwarding rules can be used to conditionaly forward PaaS DNS suffix (i.e. database.windows.net) to NGINX DNS Proxy.

VPN split tunneling can be used to define nameserver as NGINX DNS Proxy for search domains defined by PaaS DNS suffix (i.e. database.windows.net)

On-Prem DNS configured conditional forwarder for PaaS suffix (i.e. database.windows.net) to NGINX DNS Proxy.

An Azure Multi-Cloud Private Link for PaaS network design simplifies access for remote users, corporate data center users and applications residing in other clouds, all leveraging the combination of Azure Private Link and the Aviatrix cloud network platform for advanced multi-cloud network and security services.

Aviatrix Introduction – Multi-Cloud Network Architecture

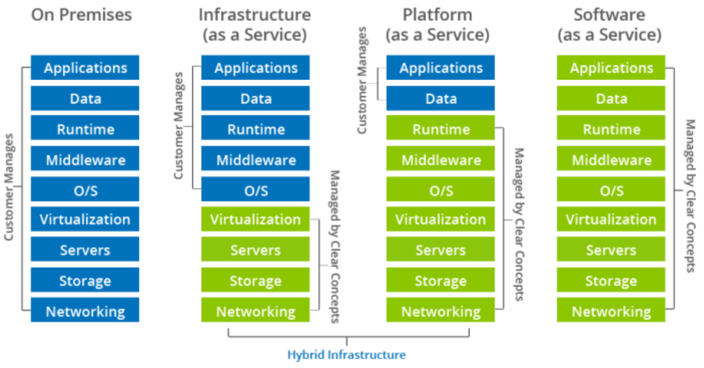
Aviatrix Validated Designs are created based on a Multi-Cloud Network Architecture (MCNA), which has been proven with hundreds of enterprise customers building cloud network infrastructure in AWS, Azure, Google and Oracle clouds across almost every vertical industry around the world. An MCNA is not a product, it is an architectural framework that is used to organize design requirements. An MCNA outlines how architectural pillars such as networking, security, day-one automation and day-two operational visibility span across cloud access, cloud networking and cloud application layers. Similar to a building architecture, the MCNA becomes the go to plan that allows cloud and security architects and their operational counter parts to work together to ensure network designs meets all cross-functional requirements.

To realize their multi-cloud network designs, Aviatrix customers leverage the Aviatrix cloud network platform to deliver multi-cloud networking, security, and operational visibility capabilities that go beyond what any cloud service provider offers. Aviatrix software leverages public cloud provider APIs to interact with and directly program native cloud networking constructs. This abstracts the unique complexities of each cloud, simplifying deployments and forming one multi-cloud network data plane with advanced networking and security features and one, consistent multi-cloud operational model. Aviatrix Transit delivers a superset of enterprise-class capabilities that becomes the foundation of our enterprise customer's multi-cloud network architecture.

Why Azure Private Link Services Are Important

Enterprise organizations have the desire to leverage PaaS offerings for new deployments or when refactoring legacy applications because the PaaS reduces the amount of IT infrastructure they must manage themselves.

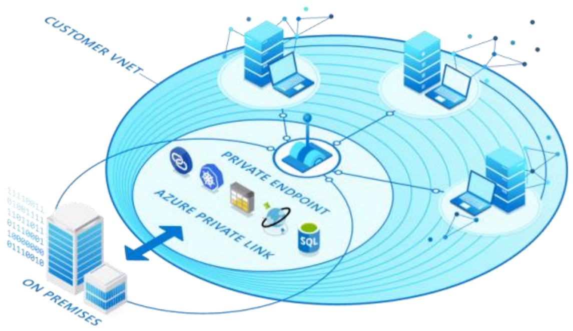
As Microsoft becomes responsible for the care and feeding of PaaS services, IT organizations are freed up from time consuming tasks such as O/S patching, managing compute sizing and base service availability, allowing them to and focus squarely on the application and application data.



While enterprise IT reaps the benefit of managing less infrastructure, publicly addressable services become a showstopper for their counterparts with corporate and regulatory responsibility for securing those services.

Azure Private Link offers the perfect middle ground as PaaS services can still be leveraged by enterprise IT while doing so via private address space from the VNET.

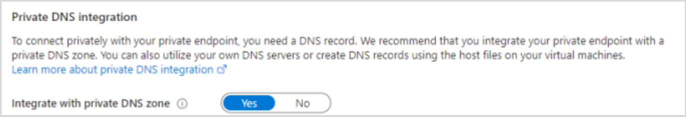
Azure Private Link Design Challenges



Azure Private Link works great when the compute nodes accessing these services are located within Azure.

As Azure began to see strong enterprise interest for consuming PaaS solutions via Private Link, Azure provided DNS integration features which simplified access to private endpoints. The DNS integration feature creates a private DNS zone, which contains the private endpoint IP address for Fully Qualified Domain Names (FQDN) of services being accessed.

Leveraging the DNS integration feature, Azure PaaS services are initially provisioned with FQDNs, which resolve to public IP addresses. This allows easier access to Private Link resources at the application level.



Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines.
Learn more about private DNS integration

Integrate with private DNS zone [✓ Yes] No

Using this method, applications owners do not have to make any changes when accessing their BLOB storage account or SQL Database but can access the same FQDN and allow the Azure DNS service to redirect the traffic to the private IP rather than the public IP.

However, additional steps must be taken if the source accessing these services resides on-prem or is a remote user connected via VPN for example. In these instances, the DNS integration that Azure offers is limited, because those types of source users do not have visibility into the Azure private DNS zone. This problem also exists if sources reside in a different cloud such as AWS or GCP.

Customers looking to leverage Private Link for sources outside of Azure have to figure out a way of accessing these services privately via DNS as most PaaS services are TLS encrypted. Simply hardcoding a private IP will result in certificate errors so a DNS based solution must be provided

Common Use Cases for Azure Private Link Plus Aviatrix Designs

The Azure Multi-Cloud Private Link for PaaS plus Aviatrix multi-cloud network design leverages Azure Private Link with DNS Integration and extends this functionality by using the Aviatrix cloud network platform to provide transit network connectivity to all sources while leveraging a DNS proxy solution to handle DNS resolution for non-Azure sources. Using this design, remote VPN users, on-prem, data center or branch office users, and even users or applications in other clouds, are able to leverage private connectivity to Azure PaaS resources using Azure Private Link.

SSL VPN Remote User Connectivity to Azure Private Link PaaS Services

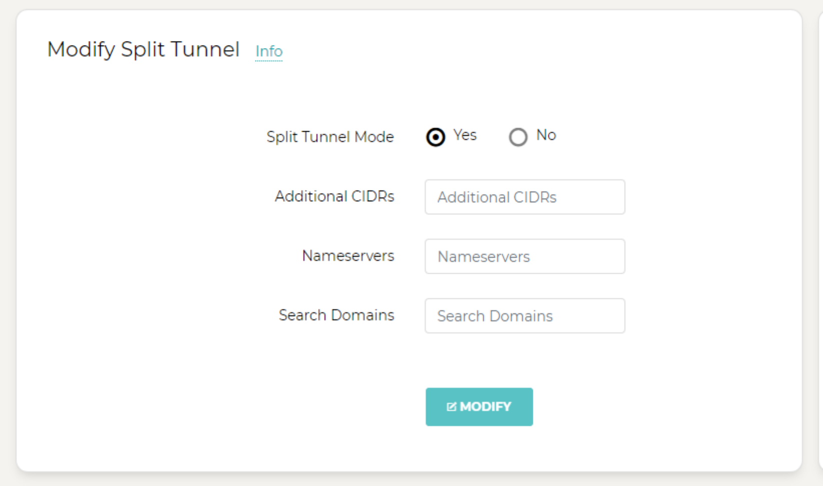
A common use case requiring SSL VPN users accessing PaaS services delivered via Private Link, are database administrators who need access a Azure SQL DB service for remote management. In these cases, users are connected through any number of VPN solutions, including Aviatrix's SAML VPN Service, and need a way to resolve the Azure private zone from their laptop.

Using native Private Link and DNS integration, users would resolve the FQDN of the SQL database and the public IP address would be returned. Using the Aviatrix / Private Link design, the Aviatrix SAML OpenVPN-based service can be used to provide these remote database administrators access to the cloud environment, while also providing private access to Azure PaaS services provisioned with Private Link.

Aviatrix OpenVPN provides Full Tunnel and Split Tunnel configuration and allows specific search domains to be specified as the dedicated name server to query when that domain is specified.

For example, applying this to our Private Link implementation, the FQDN of the SQL database (i.e. *.database.windows.net) would be inserted as the search domain with the private IP of our NGINX proxy as the Nameserver.

This results in the standard nameserver being used for all DNS requests except requests to [*.database.windows.net], which would be redirected to our proxy DNS Server. If a Private Link with DNS integration exists, the private IP would be returned to the remote user, if not a public IP address would be returned.



Modify Split Tunnel Info

Split Tunnel Mode ● Yes ○ No

Additional CIDRs: Additional CIDRs

Nameservers: Nameservers

Search Domains: Search Domains

On-prem Data Center and Corporate Network Connectivity to Azure Private Link PaaS Services

This use case is for customers with on-prem applications that need access to Private Link services, for example, Azure Blob Storage or Azure Service Bus message broker, where the on-prem applications are decoupled from these services in the Azure cloud. In this use case, the PaaS services are internal and cannot be accessed from the outside world.

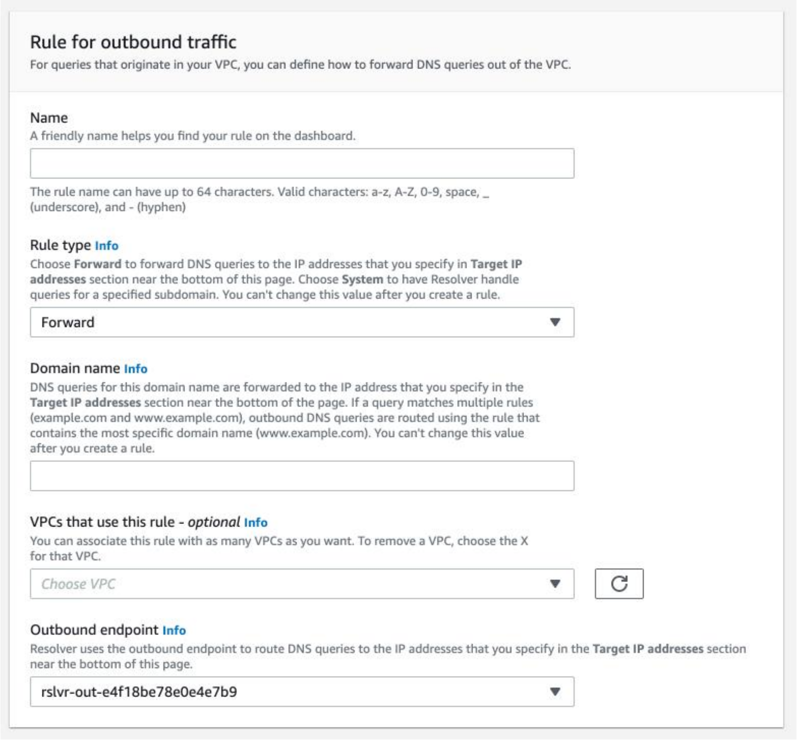
On-prem environments typically have a local DNS server which is providing resolution for all internal domains. Root hints are configured for unknown domains, so public domains associated with these PaaS services will always be returned as the public address using these standard mechanisms. It is possible to create A records for these services, with the private address, however, they would then become authoritative for the entire domain which is not desired.

Using the Azure Private Link / Aviatrix multi-cloud network design, on-prem DNS servers have a conditional forwarder for the respective FQDNs and forwards these requests to the NGINX proxy. Taking this approach, on-prem does not have to be authoritative for the entire domain and merely forwards these requests to Azure. If a Private Link with DNS integration exists, the private IP will be returned to the user and if not, the public IP address will be returned.

This configuration also ensures private PaaS connectivity stays on private circuits (i.e. ExpressRoute) while all non-production Blob Storage traffic, for example, traverses public Internet connections.

Multi-Cloud Access Connectivity to Azure Private Link PaaS Services

This design is for multi-cloud access. In this use case an application resides in another cloud but needs to leverage Azure Key Vault for certificate or password management, for example. While the capabilities of the CSPs vary, there are several examples for which this design provides the ideal multi-cloud network architecture and Azure Private Link connectivity. In AWS environments, for example, customers leverage Route53 forwarding rules to the NGINX proxy in Azure.



Rule for outbound traffic

For queries that originate in your VPC, you can define how to forward DNS queries out of the VPC.

Name

A friendly name helps you find your rule on the dashboard.

The rule name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

Rule type Info

Choose **Forward** to forward DNS queries to the IP addresses that you specify in **Target IP addresses** section near the bottom of this page. Choose **System** to have Resolver handle queries for a specified subdomain. You can't change this value after you create a rule.

Forward ▼

Domain name Info

DNS queries for this domain name are forwarded to the IP address that you specify in the **Target IP addresses** section near the bottom of the page. If a query matches multiple rules (example.com and www.example.com), outbound DNS queries are routed using the rule that contains the most specific domain name (www.example.com). You can't change this value after you create a rule.

VPCs that use this rule - *optional* Info

You can associate this rule with as many VPCs as you want. To remove a VPC, choose the X for that VPC.

Choose VPC ▼

Outbound endpoint Info

Resolver uses the outbound endpoint to route DNS queries to the IP addresses that you specify in the **Target IP addresses** section near the bottom of this page.

rslvr-out-e4f18be78e0e4e7b9 ▼

In addition to providing connectivity from all sources, the Aviatrix platform provides additional network and security featur es to these Azure Private Link data flows. Private endpoints are isolated to a secured VNET which is only accessible through a central next generation firewall, for example. Furthermore, all the troubleshooting and visibility delivered by the Aviatrix platform is applied to these private endpoints for advanced Day-2 operational visibility and control.

Design Elements and Features

Aviatrix Intelligent Centralized Controller

The Aviatrix controller is the brain of the cloud network platform. The platform leverages the centralized intelligence and knowledge of the controller to dynamically program both native cloud network constructs and Aviatrix's own gateway's advanced services. Combined with Aviatrix's multi-cloud Terraform provider this design enables network and security Infrastructure-as-Code automation across a multi-cloud environment.

Aviatrix Gateways

Aviatrix gateways deliver advanced cloud networking and security services. For this validated design Aviatrix Gateways are deployed to provide. Aviatrix Gateways in these network designs are primarily deployed to deliver transit network, SAML-based Remote User VPN and security services such as intelligent dynamic routing, active-active network high-availability, end-to-end and high-performance encryption and to collect operational visibility data. Other Aviatrix Gateway services include distributed Internet egress filtering services, based on policies (FQDN White lists or IP addresses) to limit VNet egress traffic to only known domain names or domain paths with wild card support. Aviatrix gateway replaces native NAT gateways and provide high throughput with limited compute requirements. Gateways services can be combined on single VMs but may require higher-performance cloud compute capacity.

Aviatrix CoPilot (optional)

Aviatrix CoPilot provides a global operational view of your multi-cloud network not available from any cloud provider. Enterprise IT teams – who need day-two operational visibility for cloud networking – use CoPilot's dynamic topology mapping to maintain an accurate view of their global multi-cloud networks, FlowIQ to analyze global network traffic flows and global heat maps and time series trend charts to easily pinpoint and troubleshoot traffic anomalies. CoPilot leverages the intelligence and advanced network and security services delivered by the Aviatrix cloud network platform. With Aviatrix, cloud network and security operations teams have familiar day-two operational capabilities such as packet capture, trace route and ping to resolve problems faster. Operational features include resource tagging, resource clustering, infrastructure monitoring and alerting, all specifically built for multi-cloud network operations.

Automation, Visibility and Operational Control

Deployment and updates easily fit into existing CI/CD pipelines with Terraform and the Aviatrix API. Visibility and operational control over internet bound traffic is an important element of any enterprise cloud architecture. Aviatrix provides the visibility to understand what applications are communicating with and gives the control to control those communications.

Design Considerations

When designing for Azure Private Link connectivity, organizations should consider availability, manageability, performance and cost to make sure proposed design meet the business and technical requirements.

Security

Private Link resources provide a mechanism for connecting IaaS resources to PaaS resources natively through the Azure backbone. Given these endpoints can be deployed directly into a VNET, these traffic flows have the ability to bypass existing security measures (i.e. NGFW inspection). Using the Aviatrix platform and transit capabilities, Private Link endpoints can be placed within a shared services VNET that is secured behind a NGFW device. This allows for traffic inspection and logging of all Private Link access while also ensuring that traffic to this private endpoint is encrypted while in motion.

Repeatability

While Private Link implementations and DNS integration may vary across CSP providers, when leveraging Azure Private Link for access to PaaS resources leveraging the Aviatrix cloud network platform provides a repeatable framework for customer deployments, independent of cloud environment. The private endpoints can remain accessible to all users regardless of how the user is onboarded to the cloud environment while maintaining transit connectivity and without any sacrifice in enterprise security.

High-Availability

This validated design recommends at least two Aviatrix gateways, each in different availability zones to provide infrastructure high availability. Gateways are deployed in Active/Active mode. In case of an outage, the Aviatrix Controller will automatically rebalance the load to the available gateway. The Aviatrix platform is constructed with redundant active/active gateways and leverages dynamic routing algorithms to ensure that resources remain accessible during failure scenarios. Additionally, full transit capabilities within and across clouds ensures that localized failures do not affect the overall connectivity to critical Private Link resources

Manageability

Simple manageability is an important factor of this design. The Aviatrix cloud network platform allows several options including UI, API or Terraform automated deployments.

Performance

Instance/VM size plays an important role in achieving desired performance goals. Instances/VMs provide performance limits published by the Cloud Service Providers (CSP). It is important to determine the transit throughput required upfront before implementing the solution to achieve optimal performance.

Other Design Considerations

- DNS Integration – the biggest consideration when leveraging Private Link remotely is with DNS resolution. Mechanisms for this integration may vary so understanding the implications to DNS forwarding is important.
- PaaS resources without Private Link – there may be instances where some PaaS resources are deployed with Private Link while some other PaaS resources of the same type are not. For example, an organization may deploy a production BLOB storage account with Private Link in EAST US while individual users may also deploy a BLOB storage account in EAST US without Private Link. As the domain suffix will be the same for both storage accounts, the DNS proxy will provide resolution for both. This architecture will provide DNS resolution for both and only return the private address for the Private Link enabled storage account.
- Private Link for Customer Owned & Partner Resources – while this document focuses solely on Azure PaaS services, the same principles apply for customer owned applications and partner resources deployed with Private Link. The DNS proxy architecture should allow for connectivity to these resources using the same methodology.

To learn more about how the Azure Aviatrix Private Link Architecture can help your organization leverage Azure Private Link for private access to PaaS resources or see a demo of this architecture, please reach out to info@aviatrix.com and schedule some time with our solutions architects today!

Engage with Aviatrix

Online Documentation: docs.aviatrix.com

Help with MCNA Architecture or this validated design: info@aviatrix.com

Join the Aviatrix Community

About the Author

Bryan Ashley is a Principal Solutions Architect at Aviatrix. Bryan created this validated design for several different Azure customers. These designs have been validated and adopted for Aviatrix enterprise customers.

Bryan can be reached at bashley@aviatrix.com