**Solution Design Document**

Intact US Insurance Limited

Azure Network Design

Oct 05, 2021

Version 0.1

Table of Contents

[About This Design Process 4](#_Toc85730225)

[Document History 4](#_Toc85730226)

[Document Review 5](#_Toc85730227)

[Introduction 5](#_Toc85730228)

[How does ExpressRoute help? 6](#_Toc85730229)

[Network Privacy 6](#_Toc85730230)

[Reduces Costs 6](#_Toc85730231)

[Cross Region Connectivity 6](#_Toc85730232)

[Consistent Network Performance 6](#_Toc85730233)

[ExpressRoute Provider Model 7](#_Toc85730234)

[Network Service Provider Overview 7](#_Toc85730235)

[Private Access to Microsoft Azure 7](#_Toc85730236)

[Deploying ExpressRoute through a Network Service Provider (Telco) 8](#_Toc85730237)

[Routing IP Prefixes 8](#_Toc85730238)

[Network Requirement 9](#_Toc85730239)

[Option1: Private peering to Single Azure region 10](#_Toc85730240)

[Option2: Private peering to Multi Azure region 11](#_Toc85730241)

[Network Consideration – Feasibility Design 12](#_Toc85730242)

[Environment Separation 12](#_Toc85730243)

[Subnet Design Strategy 13](#_Toc85730244)

[Network Design Considerations 13](#_Toc85730245)

[VNET Peering connection 13](#_Toc85730246)

[Network Security Group & Subnet 14](#_Toc85730247)

[Hub and Spoke Network Topology 14](#_Toc85730248)

[Azure Private Link Service 14](#_Toc85730249)

[Optimized Routing 15](#_Toc85730250)

[Virtual Network Configuration 16](#_Toc85730251)

[Specifying Address Spaces 16](#_Toc85730252)

[Local Network Prefixes 16](#_Toc85730253)

[IP Prefixes for On-Premises or Co-Located Network 16](#_Toc85730254)

[Virtual Network Prefixes 17](#_Toc85730255)

[Available Ranges for Microsoft Azure Virtual Networks 17](#_Toc85730256)

[Subnet CIDR 17](#_Toc85730257)

[Example IP Prefixes for a Microsoft Azure Virtual Network 18](#_Toc85730258)

[Securing Express Route 18](#_Toc85730259)

[Firewalls and Security Appliances 19](#_Toc85730260)

[Securing External Endpoints 19](#_Toc85730261)

[Using Access Control Lists 19](#_Toc85730262)

[Summary 19](#_Toc85730263)

### About This Design Process

|  |  |
| --- | --- |
| Author |  |
| Change Authority | <CCoE US> |
| Internal Reference | <Doc ID> |
| Project Name | Intact US Insurance Limited. |

### Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Status | Reason for Change |
| 0.1 | 26/10/2021 | Draft | Initial version of available options |
| 1.0 | 10/11/2021 | Final | Removed Single Azure region as target architecture |
|  |  |  |  |
|  |  |  |  |

*Table 1 Document history*

### Document Review

After creating an initial draft, the design document will be peer reviewed internally. Internal peer reviewed document will have version less than 1 and customer released version will be greater than 1.

* As a standard offering the document will be once internally peer reviewed and once external/ customer peer reviewed.
* After peer review all comments/feedback will be captured in appendix A and then updated to the document as a final design.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Review Date | Description | Role | Reviewer |
|  |  |  |  |  |
|  |  |  |  |  |

# Introduction

Microsoft Azure ExpressRoute makes it easy to establish dedicated and private circuits between Intact US data center and Microsoft Azure. The infrastructure can be located on-premises in data center or co-located in one of several participating provider locations. ExpressRoute allows you to extend our infrastructure to Microsoft Azure by providing private, reliable, high speed connectivity between you and the cloud.

With ExpressRoute, the network circuit is isolated using industry standard VLANs to allow private, secure access to resources deployed in Microsoft Azure Virtual Networks and to provide connectivity to Microsoft Azure public services.

For more detailed information, please refer the Microsoft documentation

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

## How does ExpressRoute help?

### Network Privacy

Connectivity between on-premises infrastructure and infrastructure hosted in Microsoft Azure is private and secure through our ExpressRoute circuit. Our traffic never traverses the public Internet when connecting to our own virtual machines or even connecting to other Microsoft Azure public services such as Storage and SQL Database through ExpressRoute.

### Reduces Costs

If we have bandwidth heavy applications and workloads, Microsoft Azure ExpressRoute may reduce our bandwidth costs. Unlimited inbound traffic to Microsoft Azure is included with our circuit.

* If ExpressRoute partner falls under the network service provider billing model you also have unlimited outbound traffic for the same price.
* If provider is an Exchange Provider, a significant amount of outbound traffic is included and any bandwidth between ExpressRoute linked virtual networks is unlimited and included in the cost.

Outbound traffic above and beyond the included amount in our plan will be at significantly reduced rates compared with traditional Internet Service Providers and regular Microsoft Azure bandwidth rates.

### Cross Region Connectivity

It is easy to deploy virtual machines, cloud services and Azure public services within separate Microsoft Azure regions (on the same continent) that can be connected to the same ExpressRoute circuit. This allows you to deploy infrastructure in multiple Microsoft Azure regions that can take advantage of our ExpressRoute circuit while only connecting our on-premises infrastructure to Azure and minimizing costs by eliminating bandwidth expenses between regions.

### Consistent Network Performance

Microsoft Azure ExpressRoute offers circuits with bandwidth starting from 10 Mbps to 10 Gbps depending on our ExpressRoute provider. These connections are dedicated from our network, through our provider, and then to Microsoft Azure to ensure consistent performance. ExpressRoute is highly available by supporting active-active router configurations and provides control for how data is routed. This can provide you a more reliable and consistent experience over traditional Internet based connections.

## On-Premises to Cloud connectivity

### Production Network Topology

* Separate Express Route Circuits will connect to Prod Hub vNET and DR Hub vNET to establish connectivity to On-Premises DC Network.
* Production vNET communicates to Hub vNET via vNET peering in Gateway transit mode.
* DR vNET communicates to Hub DR vNET via vNET peering in Gateway transit mode.

### Non Production Network Topology

* Separate Non-Prod Express Route Circuits will connect to the Non-Prod Hub vNET for on-premises connectivity
* All the Non Prod environments that is Dev, Test, UAT vNET’s connect to the Non Prod Hub vNET via vNET peering, in Gateway Transit mode.

## ExpressRoute Provider Model

### Network Service Provider Overview

Network Service Providers offer bandwidth options from 10 Mbps through 1 Gbps. With a Network Service Provider as our ExpressRoute partner setting up the routing and high availability is provided and managed by the provider. Once connected, our infrastructure in Microsoft Azure and other Microsoft Azure services such as storage and SQL Database will be available to our network over private ExpressRoute circuit.

|  |  |
| --- | --- |
| **Metrics** | **Network Service Provider** |
| Bandwidth | 10 Mbps, 50 Mbps, 100 Mbps, 500 Mbps, 1 Gbps |
| Routing | Managed by the provider |
| High Availability | Managed by the provider |
| MPLS Support | Yes |
| Bandwidth Costs | Inbound and outbound included |

### Private Access to Microsoft Azure

Microsoft Azure ExpressRoute uses Border Gateway Protocol (BGP) for the exchange of routing information between our on-premises networks and Microsoft Azure. Networks use BGP to exchange routing information through a process called peering where the networks are known as autonomous systems exchange routing information with each other.

With ExpressRoute you can configure access to our virtual machines and cloud services hosted in a virtual network and route traffic to them exclusively over our ExpressRoute circuit where the traffic never enters the public Internet. This exchange of routing information between our network on-premises and our network in Microsoft Azure is known as private peering.

In addition to connecting to virtual networks in Microsoft Azure over our ExpressRoute circuit you may also route traffic to Microsoft Azure services such as Microsoft Azure Storage and SQL Database. This allows you to access publicly accessible services without the worry of our data leaving our ExpressRoute circuit and network provider. This exchange of routing information between our network on-premises and Microsoft Azure public services is known as public peering.

### Deploying ExpressRoute through a Network Service Provider (Telco)

It is assumed that at this point you already have an existing relationship and MPLS setup over our wide area network with a network service provider such as Level 3 or Verizon.

### Routing IP Prefixes

ExpressRoute uses Border Gateway Protocol (BGP) for exchanging routes between our network and Microsoft Azure. To setup the required BGP sessions for public and private peering you will need to four /30 subnets for our primary and secondary routers for both the public and private peering configuration.

Note: The IP Prefixes for BGP cannot overlap with the IP prefixes within our virtual or on-premises networks.

Example Routing Subnets and VLAND IDs

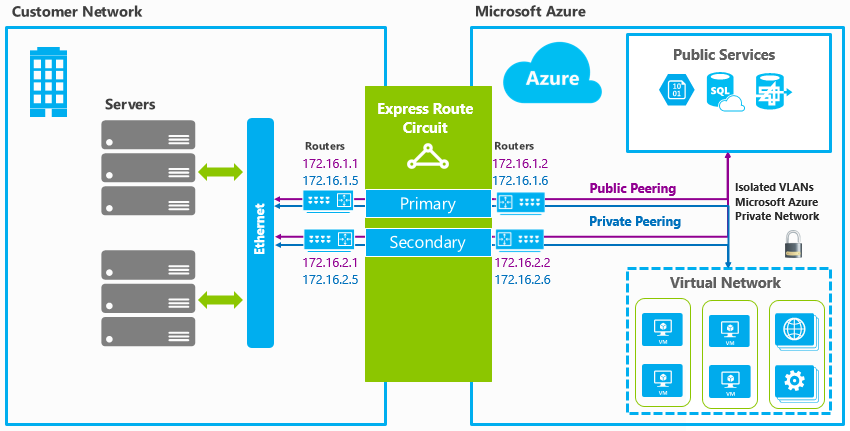
|  |  |  |  |
| --- | --- | --- | --- |
| **Router** | **IP Prefix** | **Peering** | **VLAN ID** |
| **Primary** | 172.16.1.0/30 | Private | 555 |
| **Secondary** | 172.16.2.0/30 | Private | 555 |
| **Primary** | 172.16.1.4/30 | Public | 556 |
| **Secondary** | 172.16.2.4/30 | Public | 556 |

The first available IP address of each subnet will be assigned to our router and the second available IP address will be automatically assigned to the router on the Microsoft Azure side.

Router Configuration IP Address Assignments

|  |  |  |
| --- | --- | --- |
|  | **Customer Router** | **Microsoft Azure Router** |
| **Primary** | 172.16.1.1 | 172.16.1.2 |
| **Secondary** | 172.16.2.1 | 172.16.2.2 |
| **Primary** | 172.16.1.5 | 172.16.1.6 |
| **Secondary** | 172.16.2.5 | 172.16.2.6 |

Example Deployment



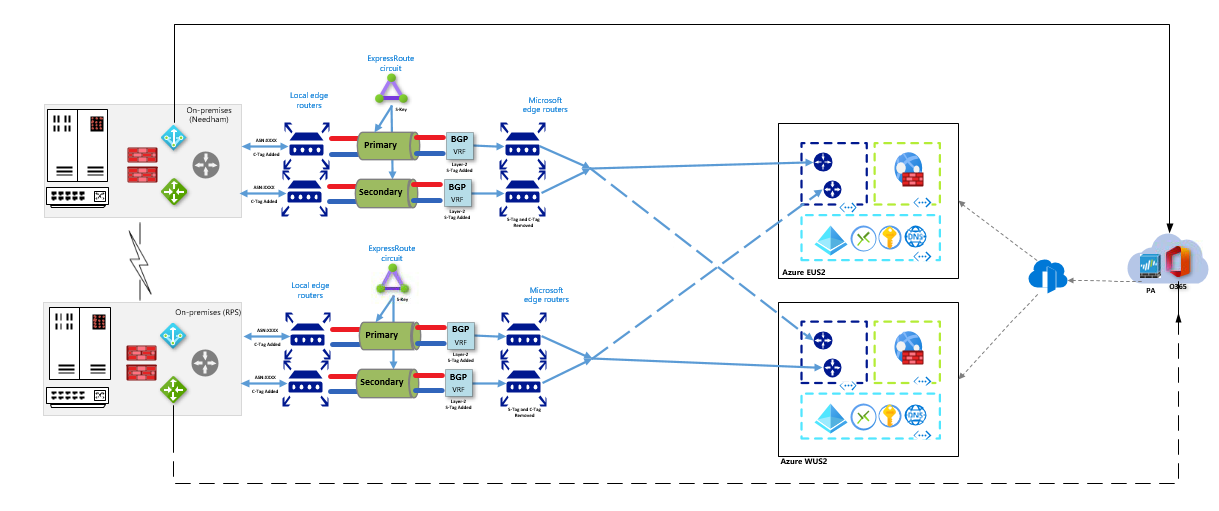
## Network Requirement

The customer needed complete isolation between the Azure prod/non-prod vNets. The Azure Hub and Spoke vNets had to be accessed as a direct connection from the Azure prod/non-prod vNets, but also could be accessed from on-prem directly if needed. The main requirements are,

1. Multi region end-to-end redundancy with East US2 and West US2
2. Azure Vnets to be consolidated within each subscription using appropriate options (Hub & Spoke Vnets)
3. Each Azure environment to connect to On-prem with dedicated private peering using Express Route Circuit
4. Each Shared Services environment to be utilised by each environment (Prod/Non-prod) via direct peering within the cloud, not traversing ExpressRoute.
5. Prod and Non-Prod environments can only interface via on-prem. Need to ensure prod and non-prod cannot talk to each other direct or by using the Shared Services vNet as transit.

### Private peering to Multi Azure region

The diagram below uses Azure dedicated express route circuit (private site-to-site peering with the secure/direct connectivity) to the azure services using cross connectivity between two azure regions with traditional segmented Hub & Spoke reference assuming DR in place which would minimize latency rates



Detailed view of implementation is explained as shown below,

Diagram, engineering drawing

Description automatically generated

**Highlights:**

1. Disaster recovery between two Azure regions (No Geo Replication)
2. High availability in each Azure region (Multi AZ’s Redundancy)
3. Complete isolation between Azure Management and Multiple Spoke Vnet

**Lowlights:**

1. Expected low latency rate of 2-3 mins during on-premises region failovers (assuming 1GBPS direct connectivity)
2. Provided 10GBPS direct connectivity provides minimal or zero latency rates

**Obligations:**

1. Enabling site office for Microsoft as trusted partner can be considered as near option for on-premises DC and site offices
2. Allow SD Wan / VWAN with Global peering enabled

**Next Focus:**

1. Aiming to enable BFD (Bi-directional Forward Link Detection) Failures towards increased network level monitoring for quicker resolution

### Network Consideration – Feasibility Design

* Express route setup which is already in place from on-prem to Azure, there is no need of Global VNET Peering / VPN gateway connectivity between Prod & DR regions.
* The Express Route setup consisting of Express Route circuit and Express Route Gateway connects the vNET’s across regions using the Microsoft Edge routers (MSEEs) in the Microsoft backbone, hence achieving the Geo Replication.
* Network cost is reduced upto 50% when the DR region is connected via Express route over Global VNET Peering.
* Global VNET Peering has limitations for Geo Replication for SQL MI and Redis cache as per recent article from Microsoft
* We recommended to consider the below options but required POC to be done during the migration phase especially for Azure SQL Managed Instance with Auto Failover and Geo-Replication setup and Azure Redis Cache Premium SKU Plan with Geo-Replication.
  + Enable redundancy and connectivity between regions and on-premise is to bow-tie connect ExpressRoute Gateways with adjacent ExpressRoute circuits in different regions provide connectivity to on-premises.
  + Establish connectivity between the ExpressRoute circuits to the cross-regional vNET.
  + The bow-tie cross-regional connectivity between vNET's to the ExpressRoute circuits would enable communications between the East VNET Hub and Spokes to communicate with the West VNET Hub and Spokes.

**Reference** [URL:https://github.com/microsoft/Common-Design-Principles-for-a-Hub-and-Spoke-VNET-Archiecture#option-1-leveraging-bow-tied-expressroute-connections](https://github.com/microsoft/Common-Design-Principles-for-a-Hub-and-Spoke-VNET-Archiecture)

### Environment Separation

* Each environment will have dedicated VNET and Subnet



* There won’t be any common services shared between any environment esp., DEV, NONPROD and PROD
* There is no connectivity between 2 spoke vNET’s.
* Each spoke vNET can make a direct communication to On-Premises network via Hub vNET.
* Each vNET must have a unique address space and should not overlay with on-premises network.

### Subnet Design Strategy

* Each subnet is dedicated to a particular service, and it should not be shared with any other service.
* Each subnet must be have a unique address ranges (CIDR) within the address space of the vNET.

|  |  |  |
| --- | --- | --- |
| **Subnet Name** | **Network Topology** | **CIDR** |
| ER Gateway Subnet | HUB | 172.180.0.0/27 |
| WAF Subnet | HUB | 172.180.2.0/27 |
| Bastion Subnet | HUB | 172.180.3.0/27 |
| Firewall Subnet | HUB | 172.180.5.0/27 |
| Web Subnet | SPOKE1 | 172.190.0.0/24 |
| APP Subnet | SPOKE1 | 172.190.3.0/24 |
| Data Subnet | SPOKE1 | 172.190.2.0/24 |
| Integration Subnet | SPOKE1 | 172.190.1.0/24 |

* By default, Azure routes allow network traffic between all subnets in a virtual network. but we recommend to create network security group at each subnet level to apply rules for deny or allow based on requirement.
* Leverage Private Link Endpoint Service to limit access over the internet for Azure PaaS resources such as an Azure Storage Account. Azure Key Vault, Azure Container Registry.
* Network Security Group will be associated to each subnet level and rules will applied based on requirements either allow or deny rules in between subnet access based on the requirements.
* By Default, Outbound to Internet access will be disabled at the each subnet level by using NSG

## Network Design Considerations

### VNET Peering connection

* Considered the Global VNET Peering to establish network connectivity between Production VNET ( East) to DR VNET ( West).
* If there are any limitation to enable Geo-replication across region for Azure SQL Managed Instance, Azure Container Registry, Azure Redis Cache Services, Leverage Express Route connection.

### Network Security Group & Subnet

Azure Network Security Group to control over network traffic flowing in and out between subnets

By default, allow rules will be applied in between subnets / On-Prem Network. Other traffic will be deny which includes Outbound internet traffic

NSG rules has to be added for Azure SQL Managed Instance, Azure Batch Service, AKS Subnet based on Azure Microsoft recommendations

Subnets are derived based on the isolation level that is supported by the Azure PaaS service such as SQL Managed Instance, AKS, Redis cache, Batch account. The other services which does not support isolation but does support private link end point are also tagged to dedicated subnet classified to each Azure service.

### Hub and Spoke Network Topology

**HUB vNET:** The hub is the central point of connectivity to your on-premises network, and a place to host the common services (Example: Firewall Appliance, DevOps self hosted agent) that can be utilized by the spoke vNET’s.

**Spoke vNET’s:** Dev, QA,UAT, Prod and DR Virtual Networks that are used as spokes in the hub-spoke topology. There Virtual Networks and VNET associated resources are isolated. Each spoke VNET have multiple subnets.

### Azure Private Link Service

**Azure Private Link Service:** It enables to access the Azure PaaS Services such as Azure Storage Account, Azure Container Registry, Azure Key vault over the private endpoint service which will be created in the specific Virtual Network.

Traffic between the virtual network and service communicates over Microsoft backbone network and exposing those services to the public internet is no longer necessary.

### Optimized Routing

We can assign a higher weight to the local connection than to the remote connection

We can also influence routing from VNet to our on-premises network, if we have multiple ExpressRoute circuits, by configuring the weight of a connection instead of applying AS PATH prepending. For each prefix, we will always look at the connection weight before the AS Path length when deciding how to send traffic.

* Express route setup which is already in place from on-prem to Azure, there is no need of Global VNET Peering / VPN gateway connectivity between Prod & DR regions.
* The Express Route setup consisting of Express Route circuit and Express Route Gateway connects the vNET’s across regions using the Microsoft Edge routers (MSEEs) in the Microsoft backbone, hence achieving the Geo Replication.
* Network cost is reduced upto 50% when the DR region is connected via Express route over Global VNET Peering.
* Global VNET Peering has limitations for Geo Replication for SQL MI and Redis cache as per recent article from Microsoft
* We recommended to consider the below options but required POC to be done during the migration phase especially for Azure SQL Managed Instance with Auto Failover and Geo-Replication setup and Azure Redis Cache Premium SKU Plan with Geo-Replication.
  + Enable redundancy and connectivity between regions and on-premise is to bow-tie connect ExpressRoute Gateways with adjacent ExpressRoute circuits in different regions provide connectivity to on-premises.
  + Establish connectivity between the ExpressRoute circuits to the cross-regional vNET.
  + The bow-tie cross-regional connectivity between vNET's to the ExpressRoute circuits would enable communications between the East VNET Hub and Spokes to communicate with the West VNET Hub and Spokes.

Reference [URL:](https://github.com/microsoft/Common-Design-Principles-for-a-Hub-and-Spoke-VNET-Archiecture)

<https://github.com/microsoft/Common-Design-Principles-for-a-Hub-and-Spoke-VNET-Archiecture#option-1-leveraging-bow-tied-expressroute-connections>

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-optimize-routing>

# Virtual Network Configuration

After our ExpressRoute circuit has been provisioned you will need to create and link one or more virtual networks to the circuit. You can link multiple virtual networks to an ExpressRoute circuit from any region on the same continent. For example: West US and East US may connect directory as well as North Europe and West Europe. However, virtual networks created in West US and North Europe could not be linked together on the same circuit.

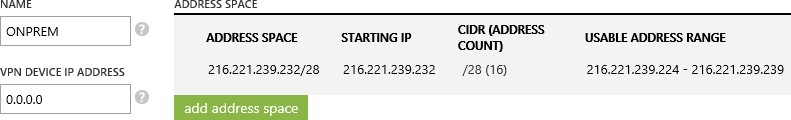
## Specifying Address Spaces

To configure ExpressRoute you must specify the address spaces or IP prefixes for our on-premises and Microsoft Azure-based Virtual Networks. The address spaces should not overlap.

### Local Network Prefixes

The IP Prefixes used on our on-premises network configuration can include public or private IP prefixes. When configuring our virtual network you should add all of the IP prefixes you wish to be able to communicate to the Microsoft Azure Virtual Network.

### IP Prefixes for On-Premises or Co-Located Network



**Note:** When creating a virtual network using the management portal you are currently required to specify an IP address for the VPN device. This value is not used with ExpressRoute and any placeholder address can be used such as 0.0.0.0.

### Virtual Network Prefixes

The IP prefixes that will be used within our Microsoft Azure Virtual Network(s) should not overlap with our on-premises network connected to Microsoft Azure. Only IP prefixes from RFC1918 are supported within Microsoft Azure Virtual Networks.

### Available Ranges for Microsoft Azure Virtual Networks

|  |  |
| --- | --- |
| 10.0.0.0 | 10.255.255.255 (10/8 prefix) |
| 172.16.0.0 | 172.31.255.255 (172.16/12 prefix) |
| 192.168.0.0 | 192.168.255.255 (192.168/16 prefix) |

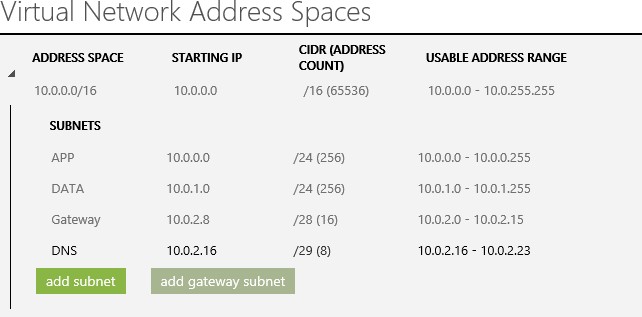
As part of creating virtual network you should partition our address space into subnets.

**Note:** You must create a /28 subnet named Gateway for the Microsoft Azure gateway roles.

### Subnet CIDR

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Subnet Classification** | **Dev Subnet Size** | **Test Subnet Size** | **UAT Subnet Size** | **Prod Subnet Size** | **DR Subnet Size** |
| AKS (Kubenet) | 256 Ips (/24 CIDR) | 256 Ips (/24 CIDR) | 256 Ips (/24 CIDR) | 256 Ips (/24 CIDR) | 256 Ips (/24 CIDR) |
| Batch Account | 128 Ips (/25 CIDR) | 128 Ips (/25 CIDR) | 128 Ips (/25 CIDR) | 256 Ips (/24 CIDR) | 256 Ips (/24 CIDR) |
| Application Gateway | 32 Ips (/27 CIDR) | 32 Ips (/27 CIDR) | 32 Ips (/27 CIDR) | 32 Ips (/27 CIDR) | 32 Ips (/27 CIDR) |
| SQL MI | 32 Ips (/27 CIDR) | 32 Ips (/27 CIDR) | 32 Ips (/27 CIDR) | 32 Ips (/27 CIDR) | 32 Ips (/27 CIDR) |
| Redis | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) |
| ACR | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) |
| Storage Account | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) |
| App Configuration | 8 Ips (/29 CIDR) | 8 Ips (/29 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) |
| Keyvault | 8 Ips (/29 CIDR) | 8 Ips (/29 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) | 16 Ips (/28 CIDR) |
| **Vnet Size** | **512 Ips (/23 CIDR)** | **512 Ips (/23 CIDR)** | **1024 Ips (/22 CIDR)** | **1024 Ips (/22 CIDR)** | **1024 Ips (/22 CIDR)** |

### Example IP Prefixes for a Microsoft Azure Virtual Network



# Securing Express Route

Microsoft Azure ExpressRoute is more secure than a traditional Internet connection due to the private and dedicated nature of its connection. However, there are several additional approaches that you can utilize to decrease our attack surface and lower the risk of our network being attacked.

### Firewalls and Security Appliances

Microsoft Azure ExpressRoute places you in control of our network. This means you can place additional firewalls, security appliances or further protect our network with IPSEC.

### Securing External Endpoints

When creating virtual machines in Microsoft Azure, endpoints are automatically created for Remote Desktop and Remote PowerShell for Windows-based virtual machines and SSH for Linux-based virtual machines. You can further secure access to these virtual machines by removing the endpoints altogether and accessing the management features using the virtual machines internal IP address from our ExpressRoute network.

### Using Access Control Lists

If management endpoints on Microsoft Azure Virtual Machines are required to be exposed to external networks it is highly recommended to do so only using access control lists to restrict the visibility and access to the these ports to a whitelist of IP addresses or networks.

Managing Virtual Machines by connecting to internal IP addresses for internal management and external endpoints with an access control list (ACL) for external access.

# Summary

Microsoft Azure ExpressRoute provides private and consistent network capabilities to enable the hybrid cloud with Microsoft Azure.

ExpressRoute is ideal for workloads that require transferring large amounts of data, low latency, or solutions that require a higher degree of security, privacy and control over the network. ExpressRoute may also provide significant cost savings related to bandwidth costs by providing a lower cost alternative for high bandwidth workloads.

ExpressRoute also enables you to connect virtual machines and public services from multiple Microsoft Azure regions directly to our on-premises network providing hybrid cloud capabilities and enabling you to bring our infrastructure closer to our customers.