**CORE SERVICE DESIGN:**

**Azure Virtual Network Gateway**

atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | DTS |
| **Contact Name** | Dominic Panzera |
| **Email** |  |
| **Telephone** | N/A |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure Virtual Network Gateway Core Service Design |
| **File Name** | Ambulance Victoria – Azure Virtual Network Gateway Core Service Design v2.0.docx |
| **Version** | 2.0 |
| **Status** | Updated |
| **Release Date** | 08/01/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Daniela Nikolic |  |  |
| **Authorised** | Dileep Pradeep |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| **Version** | **Remarks** | **Change Requested** | **Pages Affected** | **Release Date** |
| 1.0 | Initial Release | N/A | All | 12/12/2023 |
| 2.0 | Updated | Minor Updates | 16, 17 | 08/01/2024 |

Table of Contents

[1. Overview 5](#_Toc155616682)

[1.1 Purpose and Audience 5](#_Toc155616683)

[1.2 Scope and Key Deliverables 5](#_Toc155616684)

[1.3 Glossary and Definitions 6](#_Toc155616685)

[2. Executive Summary 7](#_Toc155616686)

[3. Resource Cost 8](#_Toc155616687)

[4. WAF and Security Control Alignment 9](#_Toc155616688)

[4.1 Reliability 9](#_Toc155616689)

[4.1.1 Overview 9](#_Toc155616690)

[4.1.2 Azure Virtual Network Gateway Reliability Checklist 9](#_Toc155616691)

[4.2 Cost Optimisation 10](#_Toc155616692)

[4.2.1 Overview 10](#_Toc155616693)

[4.2.2 Azure Virtual Network Gateway Cost Optimisation Checklist 10](#_Toc155616694)

[4.3 Operational Excellence 10](#_Toc155616695)

[4.3.1 Overview 10](#_Toc155616696)

[4.3.2 Azure Virtual Network Gateway Operational Excellence Checklist 10](#_Toc155616697)

[4.4 Performance Efficiency 11](#_Toc155616698)

[4.4.1 Overview 11](#_Toc155616699)

[4.4.2 Azure Virtual Network Gateway Performance Efficiency Checklist 11](#_Toc155616700)

[4.5 Security 11](#_Toc155616701)

[4.5.1 Overview 11](#_Toc155616702)

[5. Architecture Summary 12](#_Toc155616703)

[5.1 Resource Diagram 12](#_Toc155616704)

[5.1.1 Example Point-to-Site configuration 12](#_Toc155616705)

[5.1.2 Example Site-to-Site configuration 13](#_Toc155616706)

[5.1.3 Current ExpressRoute Gateway configuration 13](#_Toc155616707)

[5.2 Resource Overview 14](#_Toc155616708)

[5.2.1 Gateway SKUs Selection 14](#_Toc155616709)

[5.2.2 Connection Types 15](#_Toc155616710)

[5.3 RBAC 16](#_Toc155616711)

[5.4 Design Decisions and Justifications 16](#_Toc155616712)

[5.4.1 Connectivity Type Selection 16](#_Toc155616713)

[5.4.2 SKU Selection 16](#_Toc155616714)

[5.4.3 Active-Active Mode 17](#_Toc155616715)

[5.4.4 Diagnostics 17](#_Toc155616716)

[5.4.5 Subscription 17](#_Toc155616717)

[6. Azure Policies 18](#_Toc155616718)

[7. Configuration Templates 18](#_Toc155616719)

[7.1 Point to Site Configurations 18](#_Toc155616720)

[Primary Platinum VPN Gateway – P2S 18](#_Toc155616721)

[DR Platinum VPN Gateway – P2S 19](#_Toc155616722)

[7.2 Site to Site Configurations 20](#_Toc155616723)

[Primary Platinum VPN Gateway – S2S 20](#_Toc155616724)

[Primary DR VPN Gateway – S2S 21](#_Toc155616725)

[7.3 ExpressRoute Configurations 22](#_Toc155616726)

[Primary Production – Platinum ExpressRoute Gateway 22](#_Toc155616727)

[Primary DR– Platinum ExpressRoute Gateway 23](#_Toc155616728)

[8. Acceptance 25](#_Toc155616729)

# Overview

This document covers the baseline design for the Azure Virtual Network Gateway core service. The intention of this document is to define the overall resource design in isolation from a specific application. It is aimed to highlight the general process and requirements for building a Azure Virtual Network Gateway in a repeatable fashion with consistent configurations. Design decisions and justifications have been included in the Architecture section, and this document can be used as a reference for new builds that require a Azure Virtual Network Gateway.

This design caters to a Level 2 design which covers both Microsoft’s WAF (Well Architected Framework)[[1]](#footnote-2) and the Department of Health Control list.

Any deviations required to the standards defined in this document will require separate exemption and approval from the Cloud Governance Forum if they are required for any reason for a specific build.

## Purpose and Audience

This document will outline the standard design and configuration of this Azure service in Ambulance Victoria’s Azure tenancy as a baseline for any application infrastructure deployments.

This design is intended to:

* Meet Microsoft WAF standards.
* Meet the controls stipulated by the Department of Health.
* Define the baseline required for the deployment of the resource.

The audience for this document is those involved in the planning, designing, and implementing of the Application/Data infrastructure. This includes:

* + Ambulance Victoria IT staff

It is assumed that the reader knows and is familiar with Azure Cloud concepts and related topics.

## Scope and Key Deliverables

The scope of this core service design is to define the baseline deployment requirements and standards for the Azure Virtual Network Gateway core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration document that defines the deployment of this resource for each of the Service Tiers, or for any other logical standard such as size
* IaC templates for repeatable deployment of this core service

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **WAF** | Well Architected Framework |
| **CAF** | Cloud Adoption Framework |
| **Level 1** | Refers to a resource that has been designed to a CAF standard |
| **Level 2** | Refers to a resource that has been designed to a WAF standard with Department of Health controls overlayed |
| **AZ 2** | Refers to Ambulance Victoria’s legacy Azure Landing Zone still in use in some regards |
| **AZ 3** | Refers to Ambulance Victoria’s current Azure Landing Zone, also referred to as the Enterprise landing zone. This is the target state for migrations. |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **GB** | Gigabyte |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |
| **VPN** | Virtual Private Network |
| **P2S** | Point to Site |
| **S2S** | Site to site |

Table 1: Glossary and Definitions

# Executive Summary

This design covers the baseline standards for the Azure Virtual Network Gateway Core Service. This service has been assessed against the five pillars of WAF as well as the Department of Health Security Controls.

This section contains a summary of the major design decisions that have been made for defining the baseline of this resource as an outcome of the WAF and Security analysis detailed throughout this document.

Of the five WAF Pillars, it was found that there was no service specific guidance for Azure Virtual Network Gateways.

For Security there were no additional controls in the Department of Health controls, and the MSB has been referenced.

For the configuration of this service there is only a Platinum service due to the nature of the resource, and the fact that it will be placed in a Platform subscription which are all considered Platinum.

# Resource Cost

The pricing for Azure Virtual Network Gateway comes in two main types: VPN and ExpressRoute. The costing for ExpressRoute is not relevant here and is captured as a part of the ExpressRoute Core Service design. For the VPN Azure Virtual Network Gateway configuration the pricing differs based on the SKU used as well as data transfer[[2]](#footnote-3).

|  |  |
| --- | --- |
| VPN Gateway SKU | Pricing per hour |
| Basic | $0.06 |
| VpnGw1 | $0.2861 |
| VpnGw2 | $0.7378 |
| VpnGw3 | $1.8822 |
| VpnGw4 | $3.1620 |
| VpnGw5 | $5.4958 |
| **Data Transfers** | **Pricing per GB** |
| Inbound Inter-virtual | Free |
| Outbound Inter-virtual | $0.1356 |
| Outbound P2S VPN | Routing via preferred ISP transit network for Australia is:  First 100GB/month | Free  Next 10TB/month | $0.1657  Next 40TB/month | $0.1130  Next 100TB/month | $0.1054  Next 350TB/month | $0.0904 |

Table 2: Pricing Construct

# WAF and Security Control Alignment

The following are the five pillars of the Microsoft Well Architected Framework:

* [Reliability](https://learn.microsoft.com/en-us/azure/well-architected/#reliability)
* [Cost optimization](https://learn.microsoft.com/en-us/azure/well-architected/#cost-optimization)
* [Operational excellence](https://learn.microsoft.com/en-us/azure/well-architected/#operational-excellence)
* [Performance efficiency](https://learn.microsoft.com/en-us/azure/well-architected/#performance-efficiency)
* [Security](https://learn.microsoft.com/en-us/azure/well-architected/#security)

For this design, the security section will also cover the Department of Health Controls in addition with any Microsoft Security Best Practices. Each of these sections will detail relevant controls or baseline requirements for this core service that will be put in place.

## Reliability

### Overview

The term reliability refers to the availability of the system and its ability to recover from failure[[3]](#footnote-4). Resiliency strategies must be built into each element of the architecture. The pillars of reliability include:

* Design for business requirements
* Design for failure
* Observe application health
* Drive Automation

### Azure Virtual Network Gateway Reliability Checklist

There is no service specific guidance under the Microsoft Well Architected Framework for Azure Virtual Network Gateway.

For some additional information, every Azure VPN gateway consists of two instances that exist in an active-standby mode inherently[[4]](#footnote-5). Any planned maintenance or unplanned disruption that occurs will activate the standby instance. This switch over does cause a brief interruption. For planned maintenance the connectivity outage is approximately 10-15 seconds.

As an alternative for even better redundancy, an active-active mode can be enabled.

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[5]](#footnote-6). It looks at removal of unnecessary spend and improving operational efficiency. The principles of cost optimisation revolve around:

* Choosing the correct resources
* Setting up budgets and maintaining cost constraints
* Dynamically allocate and deallocate resources
* Optimising workloads whilst aiming for scalable costs
* Continuously monitoring and cost managing

### Azure Virtual Network Gateway Cost Optimisation Checklist

There is no service specific guidance under the Microsoft Well Architected Framework for Azure Virtual Network Gateway.

However, it is best to ensure that the selected SKU meets the requirements of the build, without over-reaching as SKUs can be upgraded but cannot be downgraded without redeployment [[6]](#footnote-7). The following limitations apply to the resizing of Gateway SKUs:

* You cannot resize to downgrade a SKU.
* You cannot resize a SKU to another generation SKU.

## Operational Excellence

### Overview

Operational Excellence aims to ensure that once the architecture is built, the ongoing operations are flawless. This includes repeatable and reliable deployments, automating to eliminate human error. To do this the following must be considered:

* Optimise the build and release process (including CI/CD and IaC)
* Understand Operational Health
* Test recovery and failure
* Focus on continuous improvement
* Use loosely coupled architecture

### Azure Virtual Network Gateway Operational Excellence Checklist

There is no service specific guidance under the Microsoft Well Architected Framework for Azure Virtual Network Gateway.

Though there is no specific guidance, the recommendation is to deploy in an active-active mode, as mentioned in the Reliability section to ensure that any outage results in minimal service disruptions.

## Performance Efficiency

### Overview

Performance Efficiency refers to the ability of your systems and applications to meet user demands without breaking or creating a negative user experience[[7]](#footnote-8). This covers capacity and scalability:

* Design for horizontal scaling
* Run stress and performance tests
* Continuously monitor performances, particularly in Production systems

### Azure Virtual Network Gateway Performance Efficiency Checklist

There is no service specific guidance under the Microsoft Well Architected Framework for Azure Virtual Network Gateway.

## Security

### Overview

Security refers to the ability of the environment to resist and manage threats.

This section covers both Microsoft Best Practices as well as relevant security controls provided by the Department of Health. With respect to the Microsoft WAF, Security is underpinned by the following[[8]](#footnote-9):

* Plan resources and how to harden them
* Automate and use least privilege
* Classify and encrypt data
* Monitor system security, plan incident response
* Identify and protect endpoints
* Protect against code-level vulnerabilities
* Model and test against potential threats

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The relevant Microsoft Security Controls include the following:

* DP-3: Encrypt sensitive data in transit
* LT-4: Enable logging for security investigation
* AM-2 Use only approved services

# Architecture Summary

## Resource Diagram

### Example Point-to-Site configuration



Figure 1: Sample Point-to-Site architecture diagram

### Example Site-to-Site configuration



Figure 2: Sample Site-to-Site configuration

### Current ExpressRoute Gateway configuration



Figure 3: Current ExpressRoute configuration

## Resource Overview

Azure Virtual Network Gateway is a resource that can be configured in two primary ways[[9]](#footnote-10) [[10]](#footnote-11):

* ExpressRoute
* VPN

Both options are considered here, though the ExpressRoute Core Service design may contain more information regarding the overall configuration of the ExpressRoute Gateway. The primary difference is that VPN involves encrypted traffic across the public Internet. Point-to-site, site-to-site, and vnet-to-vnet VPNs all use this mode of Gateway. The ExpressRoute on the other hand involves the transfer of network data across a private link.

### Gateway SKUs Selection

#### ExpressRoute SKUs Overview

The currently available SKUs for ExpressRoute include:

* Standard
* HighPerformance
* UltraPerformance

The SKUs will be discussed further in the ExpressRoute Core Service design, though the existing configuration makes use of the Standard SKU.

#### VPN SKUs Overview

The available SKUs for VPN Gateway currently available are shown in the table below[[11]](#footnote-12). The choice of SKU will depend on throughput and total connections required as shown below:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **VPN** **Gateway** **Generation** | **SKU** | **S2S/VNet-to-VNet** **Tunnels** | **P2S** **SSTP Connections** | ****P2S**** ****IKEv2/****  **OpenVPN Connections** | **Aggregate** **Throughput Benchmark** | **BGP** | **Zone-redundant** | **Supported No. of VMs in the Virtual Network** |
| Gen 1 | **Basic** | Max. 10 | Max. 128 | N/A | 100 Mbps | N/A | No | 200 |
| Gen 1 | **VpnGw1** | Max. 30 | Max. 128 | Max. 250 | 650 Mbps | Supported | No | 450 |
| Gen 1 | **VpnGw2** | Max. 30 | Max. 128 | Max. 500 | 1 Gbps | Supported | No | 1300 |
| Gen 1 | **VpnGw3** | Max. 30 | Max. 128 | Max. 1000 | 1.25 Gbps | Supported | No | 4000 |
| Gen 2 | **VpnGw2** | Max. 30 | Max. 128 | Max. 500 | 1.25 Gbps | Supported | No | 685 |
| Gen 2 | **VpnGw3** | Max. 30 | Max. 128 | Max. 1000 | 2.5 Gbps | Supported | No | 2240 |
| Gen 2 | **VpnGw4** | Max. 100 | Max. 128 | Max. 5000 | 5 Gbps | Supported | No | 5300 |
| Gen 2 | **VpnGw5** | Max. 100 | Max. 128 | Max. 10000 | 10 Gbps | Supported | No | 6700 |

Table 3: VPN Gateway SKU specifications

### Connection Types

As mentioned previously, the two main modes of configuration for Azure Virtual Network gateway are VPN or ExpressRoute. However, the VPN configuration also has a subset of options:

* ExpressRoute
* VPN
  + Site-to-site
  + Point-to-site
  + Vnet-to-vnet (same guidance as site-to-site)

The below table outlines each option and when they may be used as a guide for selecting connectivity type[[12]](#footnote-13):

|  |  |  |  |
| --- | --- | --- | --- |
|  | Point-to-site | Site-to-site | ExpressRoute |
| **Azure Supported Services** | Cloud Services and Virtual Machines | Cloud Services and Virtual Machines | [Services list](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#supported-services) |
| **Typical Bandwidths** | Based on the gateway SKU | Typically < 10 Gbps aggregate | 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, 100 Gbps |
| **Protocols Supported** | Secure Sockets Tunneling Protocol (SSTP), OpenVPN and IPsec | IPsec | Direct connection over VLANs, NSP's VPN technologies (MPLS, VPLS,...) |
| **Routing** | RouteBased (dynamic) | We support PolicyBased (static routing) and RouteBased (dynamic  routing VPN) | BGP |
| **Connection resiliency** | active-passive | active-passive or active-active | active-active |
| **Typical use case** | Secure access to Azure virtual networks for remote users | Dev / test / lab scenarios and small to medium scale production workloads for cloud services and virtual machines | Access to all Azure services (validated list), Enterprise-class and mission critical workloads, Backup, Big Data, Azure as a DR site |
| **SLA** | [SLA](https://azure.microsoft.com/support/legal/sla/) | [SLA](https://azure.microsoft.com/support/legal/sla/) | [SLA](https://azure.microsoft.com/support/legal/sla/) |
| **Pricing** | [Pricing](https://azure.microsoft.com/pricing/details/vpn-gateway/) | [Pricing](https://azure.microsoft.com/pricing/details/vpn-gateway/) | [Pricing](https://azure.microsoft.com/pricing/details/expressroute/) |

Table 4: Technical guidance for connectivity selection

Note that if there is a requirement for greater than 100 S2S VPN tunnels, Virtual WAN is the required deployment option.

## RBAC

There was no resource specific RBAC roles for Azure Virtual Network Gateway. The standard Reader, Contributor, and Owner roles allow this service to be managed.

## Design Decisions and Justifications

This section covers the design decisions and justifications that reflect the findings of the WAF and Security alignment. This will form the baseline requirements for the Azure Virtual Network Gateway core service and will be captured in the accompanying Configuration Template with a set of pre-approved deployment settings for this resource. Any changes, modifications or removals to the pre-approved deployments must have specific approval from the Cloud Governance Forum prior to deployment.

### Connectivity Type Selection

**Design Reference:** Section 5.1.2

**Design Decision:** ExpressRoute will not likely be required again in future. For VPN the choice of Point-to-site or Site-to-Site will be dependent upon specific application requirements.

**Design Justification:** Point-to-site is typically for secure access to Azure Virtual networks for remote users, and Site-to-Site would be for small to medium Production workloads for cloud services and virtual machines as outlined in Table 3. Either of these can be used based on the use case.

**Design Details:** Note that when deploying the different VPN connectivity types, there are different post-service deployment steps required. Site-to-site in particular requires additional resources such as a Local Network Gateway and a Connection resource.

### SKU Selection

**Design Reference:** MSB – AM-2, Section 5.1.1.2

**Design Decision:** Limit use to VpnGw1 and VpnGw2 SKUs, with VpnGw1 assumed as the default.

**Design Justification:** Given the size and expected growth of Ambulance, and the currently identified use cases, larger SKUs will not be required. SKUs cannot be sized down once selected, only increased, so it is recommended to start with VpnGw1 as a default option and increase only as necessary or with specific approvals based on rigorous application design. Note that should a SKU require resizing, there will be approximately 45 minutes of downtime required[[13]](#footnote-14).

The Basic SKU cannot be selected in the portal currently however it will also be explicitly restricted to ensure that it is never selected as it is in breach of the MSB AM-2 control.

### Active-Active Mode

**Design Reference:** [Section 4.1.2](#_Azure_Virtual_Network)

**Design Decision:** Use active-active mode when available.

**Design Details:** For Point-to-site configurations there is only active-passive available. For Site-to-Site either active-active or active-passive modes can be selected, and the recommendation is to use active-active for reliability. ExpressRoute is active-active by default and cannot be made active-passive.

Note that for active-active configurations there are some additional downstream requirements for endpoints. Even when both VPN tunnels are part of the same connection, the downstream VPN device will need to be configured to accept or establish two VPN tunnels to two VPN Gateway Public IPs[[14]](#footnote-15).

### Diagnostics

**Design Reference:** MSB – LT-4

**Design Decision:** diagnostic logs will be enabled for Virtual Network Gateways.

**Design Justification:** logging is mandatory as per the Microsoft Security Benchmark as well as the DH Controls list.

**Design Details:** The allLogs and allMetrics diagnostics will be enabled and sent to the central Log Analytics Workspace in the same region that the resource is deployed into.

### Subscription

**Design Reference:** N/A

**Design Decision:** Virtual Network Gateway resources will be deployed into the AV ALZ Connectivity subscription.

**Design Justification:** These resources are typically used for centralised connectivity to other locations (similar to express route circuits). The default deployment location will be in the AV ALZ Connectivity hub subscription unless approved by exception to be placed into another location.

# Azure Policies

There are no specific Azure Policies required that relate to Azure Virtual Network Gateway.

# Configuration Templates

It is assumed due to the nature of these services being used for connectivity that they must be Platinum and only in Production and Disaster Recovery environments. The configuration templates here include VPN Gateway and ExpressRoute Gateway.

## Point to Site Configurations

### Primary Platinum VPN Gateway – P2S

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| **Subscription** | AV ALZ Connectivity |
| **Resource Group** | Auto-selects the same Resource Group as the chosen Virtual Network |
| **Name** | gw-p2s-prd-ause-hub-01 |
| **Gateway Type** | VPN |
| **SKU** | VpnGw1 |
| **Virtual Network** | vnet-prd-ause-hub-01 |
| **Subnet** | GatewaySubnet |
| **Public IP Address Details** | |
| **Name** | pip-gw-p2s-prd-ause-hub-01 |
| **Assignment** | Static |
| **Enable active-active mode** | Enabled |
| **Second Public IP Address Details** | |
| **Name** | pip-gw-p2s-prd-ause-hub-02 |
| **Assignment** | Static |
| **Enable active-active mode** | Enabled |
| **Configure BGP** | Yes/No |
| **Post Resource Creation Configurations for Point-to-site** | |
| **Tunnel Type** | OpenVPN (SSL) / SSTP (SSL) / IKEv2 / IKEv2 and OpenVPN (SSL)/ IKEv2 and SSTP (SSL) |
| **Authentication type** | Azure Certificate/RADIUS Authentication/Azure Active Directory |
| **Public IP for User VPN Configuration** | |
| **Name** | pip-gw-p2s-prd-ause-hub-03 |
| **SKU** | Standard |
| **Assignment** | Static |

### DR Platinum VPN Gateway – P2S

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| **Subscription** | AV ALZ Connectivity |
| **Resource Group** | Auto-selects the same Resource Group as the chosen Virtual Network |
| **Name** | gw-p2s-prd-auea-hub-01 |
| **Gateway Type** | VPN |
| **SKU** | VpnGw1 |
| **Virtual Network** | vnet-prd-auea-hub-01 |
| **Subnet** | GatewaySubnet |
| ***Public IP Address Details*** | |
| **Name** | pip-gw-p2s-prd-auea-hub-01 |
| **Assignment** | Static |
| **Enable active-active mode** | Enabled |
| ***Second Public IP Address Details*** | |
| **Name** | pip-gw-p2s-prd-auea-hub-02 |
| **Assignment** | Static |
| **Enable active-active mode** | Enabled |
| **Configure BGP** | Yes/No |
| ***Post Resource Creation Configurations for Point-to-site*** | |
| **Tunnel Type** | OpenVPN (SSL) / SSTP (SSL) / IKEv2 / IKEv2 and OpenVPN (SSL)/ IKEv2 and SSTP (SSL) |
| **Authentication type** | Azure Certificate/RADIUS Authentication/Azure Active Directory |
| ***Public IP for User VPN Configuration*** | |
| **Name** | pip-gw-p2s-prd-auea-hub-03 |
| **SKU** | Standard |
| **Assignment** | Static |

## Site to Site Configurations

### Primary Platinum VPN Gateway – S2S

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| **Subscription** | AV ALZ Connectivity |
| **Resource Group** | Auto-selects the same Resource Group as the chosen Virtual Network |
| **Name** | gw-s2s-prd-ause-hub-01 |
| **Gateway Type** | VPN |
| **SKU** | VpnGw1 |
| **Virtual Network** | vnet-prd-ause-hub-01 |
| **Subnet** | GatewaySubnet |
| ***Public IP Address Details*** | |
| **Name** | pip-gw-s2s-prd-ause-hub-01 |
| **Assignment** | Static |
| **Enable active-active mode** | Enabled |
| ***Second Public IP Address Details*** | |
| **Name** | pip-gw-s2s-prd-ause-hub-02 |
| **Assignment** | Static |
| **Enable active-active mode** | Enabled |
| **Configure BGP** | Yes/No |
| ***Post Resource Creation Configurations for Site-to-site requires:***   * ***Local Network Gateway*** * ***Connection*** | |
| ***Local Network Gateway Configuration*** | |
| **Subscription** | Same as the associated VPN Gateway |
| **Resource Group** | Same as the associated VPN Gateway |
| **Name** | lng-s2s-prd-ause-hub-01 |
| **Endpoint** | IP address/FQDN |
| **IP Address or FQDN details** | IP address or FQDN Path |
| **Configure BGP** | Yes/No |
| ***Connection Configuration*** | |
| **Name** | con-gw-s2s-vnet-prd-ause-hub-01 |
| **Connection Type** | Site-to-site(IPSEC)/Vnet-to-vnet |
| **Vnet Gateway** | gw-s2s-prd-ause-hub-01 |
| **Local Network Gateway** | lng-s2s-prd-ause-hub-01 |
| **Shared Key (PSK)** | To be randomly generated |
| **IKE Protocol** | IKEv2 |
| **Use Azure Private IP** | Yes |
| **Enable BGP** | Yes/No |
| **IPsec / IKE policy** | Default |
| **Use policy-based traffic selector** | Disable/Enable |
| **DPD Timeout seconds** | 45 |
| **Connection Mode** | Default/InitatorOnly/ResponderOnly |

### Primary DR VPN Gateway – S2S

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| **Subscription** | AV ALZ Connectivity |
| **Resource Group** | Auto-selects the same Resource Group as the chosen Virtual Network |
| **Name** | gw-s2s-prd-auea-hub-01 |
| **Gateway Type** | VPN |
| **SKU** | VpnGw1 |
| **Virtual Network** | vnet-prd-auea-hub-01 |
| **Subnet** | GatewaySubnet |
| ***Public IP Address Details*** | |
| **Name** | pip-gw-s2s-prd-auea-hub-01 |
| **Assignment** | Static |
| **Enable active-active mode** | Enabled |
| ***Second Public IP Address Details*** | |
| **Name** | pip-gw-s2s-prd-auea-hub-01 |
| **Assignment** | Static |
| **Enable active-active mode** | Enabled |
| **Configure BGP** | Yes/No |
| ***Post Resource Creation Configurations for Site-to-site requires:***   * ***Local Network Gateway*** * ***Connection*** | |
| ***Local Network Gateway Configuration*** | |
| **Subscription** | Same as the associated VPN Gateway |
| **Resource Group** | Same as the associated VPN Gateway |
| **Name** | lng-s2s-prd-ause-hub-01 |
| **Endpoint** | IP address/FQDN |
| **IP Address or FQDN details** | IP address or FQDN Path |
| **Configure BGP** | Yes/No |
| ***Connection Configuration*** | |
| **Name** | con-gw-s2s-vnet-prd-auea-hub-01 |
| **Connection Type** | Site-to-site(IPSEC)/Vnet-to-vnet |
| **Vnet Gateway** | gw-s2s-prd-auea-hub-01 |
| **Local Network Gateway** | lng-s2s-prd-auea-hub-01 |
| **Shared Key (PSK)** | To be randomly generated |
| **IKE Protocol** | IKEv2 |
| **Use Azure Private IP** | Yes |
| **Enable BGP** | Yes/No |
| **IPsec / IKE policy** | Default |
| **Use policy-based traffic selector** | Disable/Enable |
| **DPD Timeout seconds** | 45 |
| **Connection Mode** | Default/InitatorOnly/ResponderOnly |

## ExpressRoute Configurations

### Primary Production – Platinum ExpressRoute Gateway

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| **Subscription** | AV ALZ Connectivity |
| **Resource Group** | Auto-selects the same Resource Group as the chosen Virtual Network |
| **Name** | gw-er-prd-ause-hub-01 |
| **Gateway Type** | ExpressRoute |
| **SKU** | Standard |
| **Virtual Network** | vnet-prd-ause-hub-01 |
| **Subnet** | GatewaySubnet |
| ***Public IP Address Details*** | |
| **Name** | pip-gw-er-prd-ause-hub-01 |
| **Assignment** | Static |
| **SKU** | Standard |
| **Tier** | Regional |
| ***First Connection Details*** | |
| **Name** | con-gw-er-vnet-prd-ause-hub-01-to-avsoutheast |
| **Virtual Network** | vnet-prd-ause-hub-01 |
| **Virtual Network Gateway** | gw-er-prd-ause-hub-01 |
| **Circuit** | er-circuit-prd-ause-mcn-01 |
| **Routing Weight** | 100 |
| ***Second Connection Details*** | |
| **Name** | con-gw-er-vnet-prd-ause-hub-01-to-aveast |
| **Virtual Network** | vnet-prd-ause-hub-01 |
| **Virtual Network Gateway** | gw-er-prd-ause-hub-01 |
| **Circuit** | er-circuit-prd-auea-mcn-01 |
| **Routing Weight** | 0 |

### Primary DR– Platinum ExpressRoute Gateway

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| **Subscription** | AV ALZ Connectivity |
| **Resource Group** | Auto-selects the same Resource Group as the chosen Virtual Network |
| **Name** | gw-er-prd-auea-hub-01 |
| **Gateway Type** | ExpressRoute |
| **SKU** | Standard |
| **Virtual Network** | vnet-prd-auea-hub-01 |
| **Subnet** | GatewaySubnet |
| ***Public IP Address Details*** | |
| **Name** | pip-gw-er-prd-auea-hub-01 |
| **Assignment** | Static |
| **SKU** | Standard |
| **Tier** | Regional |
| ***First Connection Details*** | |
| **Name** | con-gw-er-vnet-prd-auea-hub-01-to-avsoutheast |
| **Virtual Network** | vnet-prd-auea-hub-01 |
| **Virtual Network Gateway** | gw-er-prd-auea-hub-01 |
| **Circuit** | er-circuit-prd-auea-mcn-01 |
| **Routing Weight** | 100 |
| ***Second Connection Details*** | |
| **Name** | con-gw-er-vnet-prd-auea-hub-01-to-aveast |
| **Virtual Network** | vnet-prd-auea-hub-01 |
| **Virtual Network Gateway** | gw-er-prd-auea-hub-01 |
| **Circuit** | er-circuit-prd-auea-mcn-01 |
| **Routing Weight** | 0 |

# Acceptance

Signature of this page by appropriately delegated representatives of ​Ambulance Victoria​ signifies acceptance of this design document. Logicalis will commence build and implementation work once it receives a signed copy of this design document.

Signature of this page by appropriately delegated representatives of Ambulance Victoria signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 1.0 |

**Signed on behalf of Ambulance Victoria**

|  |  |
| --- | --- |
| Name | Dan Howarth |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| Name | Daniela Nikolic |
| Position | Senior Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://portal.azure.com/#create/Microsoft.VirtualNetworkGateway-ARM [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/vpn-gateway/about-gateway-skus [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwtype [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/azure/vpn-gateway/about-gateway-skus [↑](#footnote-ref-12)
12. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways [↑](#footnote-ref-13)
13. https://learn.microsoft.com/en-us/azure/vpn-gateway/gateway-sku-resize [↑](#footnote-ref-14)
14. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable#active-active-vpn-gateways [↑](#footnote-ref-15)