**CORE SERVICE DESIGN:**

**DDoS Protection**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – DDoS Protection Core Service Design |
| **File Name** | Ambulance Victoria – DDoS Protection Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 21/12/2023 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 21/12/2023 |

Table of Contents

[1. Overview 5](#_Toc154065765)

[1.1 Purpose and Audience 5](#_Toc154065766)

[1.2 Scope and Key Deliverables 5](#_Toc154065767)

[1.3 Glossary and Definitions 6](#_Toc154065768)

[2. Executive Summary 7](#_Toc154065769)

[3. Resource Cost 7](#_Toc154065770)

[4. WAF and Security Control Alignment 8](#_Toc154065771)

[4.1 Reliability 8](#_Toc154065772)

[4.1.1 Overview 8](#_Toc154065773)

[4.1.2 DDoS Protection Reliability Checklist 8](#_Toc154065774)

[4.2 Cost Optimisation 9](#_Toc154065775)

[4.2.1 Overview 9](#_Toc154065776)

[4.2.2 DDoS Protection Cost Optimisation Checklist 9](#_Toc154065777)

[4.3 Operational Excellence 9](#_Toc154065778)

[4.3.1 Overview 9](#_Toc154065779)

[4.3.2 DDoS Protection Operational Excellence Checklist 9](#_Toc154065780)

[4.4 Performance Efficiency 10](#_Toc154065781)

[4.4.1 Overview 10](#_Toc154065782)

[4.4.2 DDoS Protection Performance Efficiency Checklist 10](#_Toc154065783)

[4.5 Security 11](#_Toc154065784)

[4.5.1 Overview 11](#_Toc154065785)

[5. Architecture Summary 12](#_Toc154065786)

[5.1 Resource Overview 12](#_Toc154065787)

[5.2 RBAC 13](#_Toc154065788)

[5.3 Solution Diagram 14](#_Toc154065789)

[5.4 Design Decisions and Justifications 15](#_Toc154065790)

[5.4.1 Use DDoS Protection plan 15](#_Toc154065791)

[5.4.2 SKU Selection 15](#_Toc154065792)

[5.4.3 Logging 15](#_Toc154065793)

[6. Azure Policies 16](#_Toc154065794)

[7. Configuration Templates 16](#_Toc154065795)

[8. Acceptance 17](#_Toc154065796)

# Overview

This document covers the baseline design for the DDoS Protection 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 DDoS Protection 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 DDoS Protection.

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 DDoS Protection 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 |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |
| **DDoS** | Distributed Denial of Service |

Table : Glossary and definitions

# Executive Summary

This design covers the baseline standards for the DDoS Protection 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, there was no specific guidance for the DDoS Protection service. There is a basic level of DDoS that is built into the Azure platform. The enhanced version, discussed here, should be applied to all networks that have public endpoints (Public IPs) in them.

The SKU chosen is the Network Protection SKU which covers major network resources and includes up to 100 Public IPs. Given that Ambulance Victoria are unlikely to have more than 100 Public IPs that require protection, the IP Protection SKU will not be used.

There is no distinction between the Service Catalog tiers for this service as it is configured at a Platinum level and applied to any network that requires it.

# Resource Cost

The following are the costs for the two available SKUs of Azure DDoS Protection:

|  |  |
| --- | --- |
| Pricing Item | Network Protection SKU |
| Monthly charge (includes protection for 100 public IP resources) | $4,433/month |
| Overage charges (more than 100 public IP resources) | $44.4 per resource per month |
| **Pricing Item** | **IP Protection SKU** |
| Monthly charge per public IP resource protected | $300/month |

Table : Resource 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[[2]](#footnote-3). 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

### DDoS Protection Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Use Azure DDoS Standard Protection Plans to protect all public endpoints hosted within customer Virtual Networks. | Yes | Yes | Governance | At deployment |

Table : WAF Reliability checklist summary

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[3]](#footnote-4). 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

### DDoS Protection Cost Optimisation Checklist

There is no specific guidance for Cost Optimistaion for Azure DDoS Protection plans. The selection of SKU has been made so that Ambulance Victoria receive the best coverage for their use-case.

## 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

### DDoS Protection Operational Excellence Checklist

There is no specific guidance for Operational Excellence for Azure DDoS Protection. It will be applied to all networks that contain Public resources as is best practice.

## 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[[4]](#footnote-5). This covers capacity and scalability:

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

### DDoS Protection Performance Efficiency Checklist

There is no specific guidance for Performance Efficiency for Azure DDoS Protection.

## 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[[5]](#footnote-6):

* 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 Microsoft Security Benchmark controls that apply are:

* LT-4: Enable logging for security investigation

There are no Department of Health controls above and beyond the Microsoft Security Benchmark.

# Architecture Summary

## Resource Overview

Azure DDoS Protection is service that protects the environment from Distributed Denial of Service attacks[[6]](#footnote-7). These attacks attempt to exhaust the resources of an application or service to the point where it is unavailable to end users. Any publicly reachable resource is vulnerable to this type of attack. DDoS protects resources at Layers 3 and 4.

As it is an expensive resource, it will only be created in the Primary region, and applied to the East hub and any other network that has a Public IP.

Azure has two paid tiers of this offering, above the base DDoS protection that is enabled without any intervention required. The two tiers are[[7]](#footnote-8):

* Network Protection
* IP Protection

The following table summarises the differences between the two SKUs:

|  |  |  |
| --- | --- | --- |
| Feature | IP Protection | Network Protection |
| Active traffic monitoring & always on detection | Yes | Yes |
| L3/L4 Automatic attack mitigation | Yes | Yes |
| Automatic attack mitigation | Yes | Yes |
| Application based mitigation policies | Yes | Yes |
| Metrics & alerts | Yes | Yes |
| Mitigation reports | Yes | Yes |
| Mitigation flow logs | Yes | Yes |
| Mitigation policies tuned to customers application | Yes | Yes |
| Integration with Firewall Manager | Yes | Yes |
| Microsoft Sentinel data connector and workbook | Yes | Yes |
| Protection of resources across subscriptions in a tenant | Yes | Yes |
| Public IP Standard tier protection | Yes | Yes |
| Public IP Basic tier protection | No | Yes |
| DDoS rapid response support | Not available | Yes |
| Cost protection | Not available | Yes |
| WAF discount | Not available | Yes |
| Price | Per protected IP | Per 100 protected IP addresses |

Table : Summary of DDoS SKU Features

## RBAC

For the Virtual Network resource, the specific roles that can be applied are as follows[[8]](#footnote-9):

|  |  |
| --- | --- |
| Role Name | Description |
| Network Contributor | Lets you manage networks, but not access to them. |

Table : RBAC roles relevant for this core service

## Solution Diagram

Figure : DDoS Protection architecture diagram

Azure DDoS only needs to be created in one region. In this case it will be created in a resource group in the Primary region. As shown, it will be applied to the Australia East hub network, as well as any spoke subscription with a Public IP. This must be configured manually in the DDoS plan itself each time a new Public IP is brought into the platform.

## 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 DDoS Protection 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.

### Use DDoS Protection plan

**Design Reference:** Table 3 – [R1](#_DDoS_Protection_Reliability)

**Design Decision**: DDoS Protection will be applied to networks with public resources.

**Design Justification**: It is a security requirement to ensure that any Public IPs or public resources have an additional level of security. Each time a new Public IP is brought onto the platform, the DDoS plan must be applied to the Virtual Network that hosts the Public IP.

### SKU Selection

**Design Reference:** N/A

**Design Decision:** DDoS Network Protection will be used.

**Design Justification:** DDoS Network Protection offers more features than IP Protection. Additionally, Ambulance Victoria are limiting the number of Public IPs to only those that are necessary, so it is unlikely that they will exceed the 100 that are covered in this plan.

### Logging

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Overview)

**Design Decision:** Logs will be sent to the Australia Southeast central log analytics workspace.

**Design Justification:** To meet the Azure Security Benchmark controls it is a requirement to send all logs to the log analytics workspace so that they can be queried and reviewed as required.

# Azure Policies

The following Azure policy should be applied:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Public IP addresses should have resource logs enabled for Azure DDoS Protection | av management group (under tenant root) |

Table : Azure Policies

# Configuration Templates

Note that the following already DDoS resource has already been created in the Connectivity hub as a part of the initial landing zone rollout. The configuration that needs to be made moving forward is for every new Public IP that is onboarded. It will be required to be added to the DDoS Protection plan.

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ Connectivity |
| Resource Group | rg-prd-ause-connectivity-01 |
| Name | ddos-prd-hub-01 |
| Protected Resources | All Virtual Networks with a Public IP are to be added here |
| SKU | Network Protection |

To add a new Virtual Network to DDoS Protection navigate to the DDoS Protection plan and under the “Protected Resources” tab there is an option to add a new resource. Select the subscription and the resource group of the Virtual Network to be added, and all applicable resources will be automatically added with the Virtual Network.

# 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://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-sku-comparison [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/ddos-protection/manage-permissions [↑](#footnote-ref-9)