**CORE SERVICE DESIGN:**

**Network Security Group**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Network Security Group Core Service Design |
| **File Name** | Ambulance Victoria – Network Security Group Core Service Design v1.0.docx |
| **Version** | 2.0 |
| **Status** | Released |
| **Release Date** | 25/01/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 25/01/2024 |
| 2.0 | Minor Updates | Inbound Intra-Subnet rules clarified |  |  |

Table of Contents

[1. Overview 5](#_Toc157090325)

[1.1 Purpose and Audience 5](#_Toc157090326)

[1.2 Scope and Key Deliverables 5](#_Toc157090327)

[1.3 Glossary and Definitions 6](#_Toc157090328)

[2. Executive Summary 7](#_Toc157090329)

[3. Resource Cost 7](#_Toc157090330)

[4. WAF and Security Control Alignment 7](#_Toc157090331)

[4.1 Reliability 8](#_Toc157090332)

[4.1.1 Overview 8](#_Toc157090333)

[4.1.2 Network Security Group Reliability Checklist 8](#_Toc157090334)

[4.2 Cost Optimisation 9](#_Toc157090335)

[4.2.1 Overview 9](#_Toc157090336)

[4.2.2 Network Security Group Cost Optimisation Checklist 9](#_Toc157090337)

[4.3 Operational Excellence 9](#_Toc157090338)

[4.3.1 Overview 9](#_Toc157090339)

[4.3.2 Network Security Group Operational Excellence Checklist 9](#_Toc157090340)

[4.4 Performance Efficiency 10](#_Toc157090341)

[4.4.1 Overview 10](#_Toc157090342)

[4.4.2 Network Security Group Performance Efficiency Checklist 10](#_Toc157090343)

[4.5 Security 11](#_Toc157090344)

[4.5.1 Overview 11](#_Toc157090345)

[4.5.2 Network Security Group Security Checklist 11](#_Toc157090346)

[5. Architecture Summary 13](#_Toc157090347)

[5.1 Resource Overview 13](#_Toc157090348)

[5.1.1 NSG Flow Logs 13](#_Toc157090349)

[5.1.2 Traffic Analytics 13](#_Toc157090350)

[5.2 RBAC 13](#_Toc157090351)

[5.3 Design Decisions and Justifications 14](#_Toc157090352)

[5.3.1 Network segmentation 14](#_Toc157090353)

[5.3.2 Deny All Rules 14](#_Toc157090354)

[5.3.3 Logging and Monitoring 14](#_Toc157090355)

[6. Azure Policies 15](#_Toc157090356)

[7. Configuration Templates 16](#_Toc157090357)

[7.1 Primary Region Network Security Group 16](#_Toc157090358)

[7.2 Secondary Region Network Security Group 16](#_Toc157090359)

[8. Acceptance 18](#_Toc157090360)

# Overview

This document covers the baseline design for the Network Security Group 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 Network Security Group 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 Network Security Group.

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 Network Security Group 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 |

Table 1: Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Network Security Group 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 Reliability and Security were relevant.

For this service the main baseline configurations include:

* Every subnet must have an NSG attached to it
* Outbound Intra-subnet traffic will be allowed
* Inbound Inter-subnet traffic will be denied
* Internet Inbound will be denied

There are no differences between service tiers with respect to deployment of NSGs.

Note that due to the complex nature of Network Segmentation and Control, it is recommended to always use this document alongside the following accompanying core service design documents:

* Virtual Networks
* Route Tables
* Azure Firewall

# Resource Cost

There is no charge associated with creating Network Security Groups in Azure[[2]](#footnote-3).

# 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

### Network Security Group Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Ensure the communication between Azure PaaS services that have been injected into a Virtual Network is locked down within the Virtual Network using user-defined routes (UDRs) and network security groups (NSGs). | Yes | Yes | IaC | At deployment |
| **R2** | Ensure the communication between Azure PaaS services that have been injected into a Virtual Network is locked down within the Virtual Network using user-defined routes (UDRs) and network security groups (NSGs). | Yes | No | IaC | At deployment |

Table 2: WAF Reliability checklist summary

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[4]](#footnote-5). 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

### Network Security Group Cost Optimisation Checklist

Network Security Groups are a free resource in Azure, so there is no guidance for cost optimisation.

## 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

### Network Security Group Operational Excellence Checklist

There is no specific guidance for NSGs under the Operational Excellence pillar in the Well Architected Framework.

## 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[[5]](#footnote-6). This covers capacity and scalability:

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

### Network Security Group Performance Efficiency Checklist

There is no specific guidance for NSGs under the Performance Efficiency pillar in the Well Architected Framework.

## 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[[6]](#footnote-7):

* 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 following Microsoft Security Benchmark Controls are applicable[[7]](#footnote-8):

* NS-1: Establish network segmentation boundaries.
* LT-4: Enable logging for security investigation.

Beyond this, the following table outlines applicable Department of Health Controls.

### Network Security Group Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 12.1.2 | Establish and maintain a secure configuration process for network devices. | Yes | Yes | IaC | At deployment |
| **S4** | 20.1.2 | Establish, maintain and manage a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Ensure explicit “deny all” is used on systems to prevent unauthorised outbound connections to the internet. | Yes | Yes | IaC | At deployment |
| **S6** | 21.2.1 | Perform traffic filtering between network segments, where appropriate - the sensitivity of data needs to be taken into consideration. | Yes | Yes | IaC | At deployment |
| **S7** | 21.2.2 | Collect network traffic flow logs and/or network traffic to review and alert upon from network devices. | Yes | Yes | IaC | At deployment |
| **S8** | 24.2.3 | Maintain separate environments for production and non-production systems. | Yes | Yes | IaC | At deployment |

Table 6: Security checklist summary

# Architecture Summary

## Resource Overview

Network Security Groups are Azure resources that support network segmentation and traffic control[[8]](#footnote-9). They can be thought of as small local firewalls on a subnet or a Network Interface Card. Each rule specifies a source, destination, port and protocol. There are a set of default Microsoft rules that will always be applied and cannot be modified but can be overridden by creating rules with a higher priority.

### NSG Flow Logs

NSG Flow Logs are a feature of Azure Network Watcher that enable you to observe IP traffic that flows through an NSG[[9]](#footnote-10). The flow data is forwarded to a Storage Account which allows you to export and view the data. These logs operate at Layer 4 of the Open Systems Interconnection (OSI) model. The logs contain 5-tuple information and the decision for the traffic and are written in JSON format.

### Traffic Analytics

Traffic Analytics adds additional intelligence to the collection of NSG Flow Logs[[10]](#footnote-11). It aggregates flow logs and then simplifies them by grouping flows that have common source and destination IPs, and destination ports and protocols.

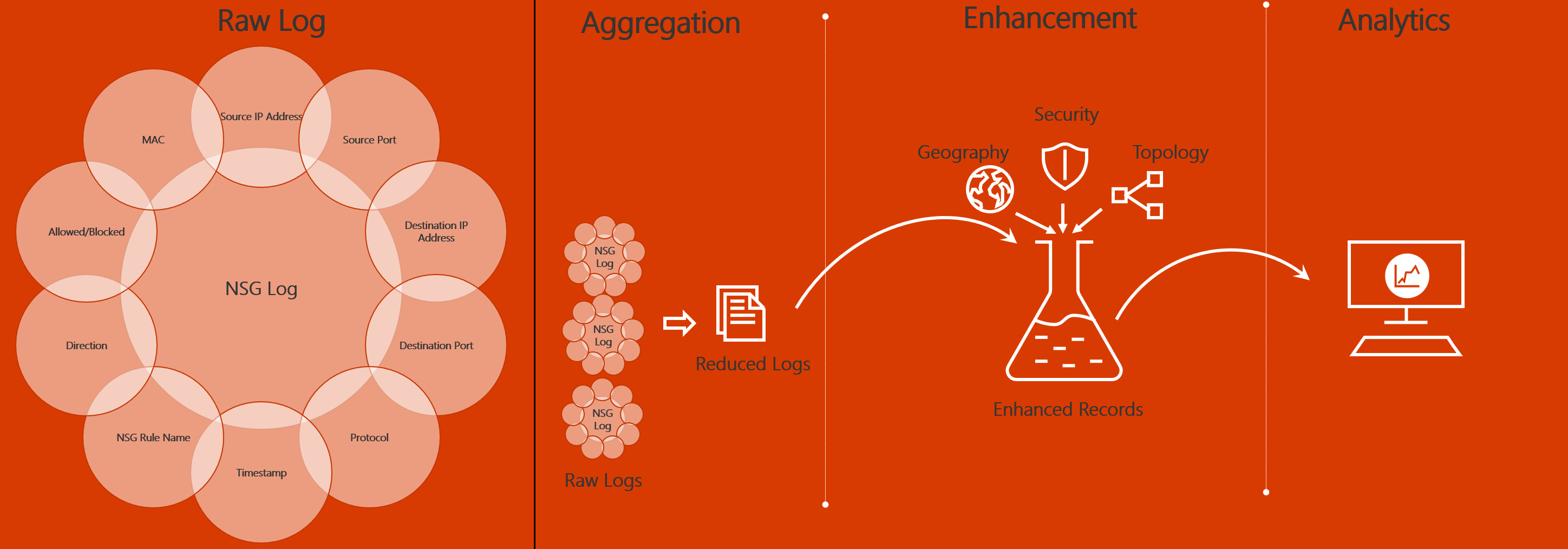


Figure 1: Traffic Analytics Information Flow

## RBAC

For the Network Security Group resource, the following role can be applied:

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

Table 7: RBAC roles relevant for this core service

## 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 Network Security Group 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.

### Network segmentation

**Design Reference:** Table 6 – [S1, S4, S6, S8](#_Network_Security_Group) and Microsoft Security Benchmark [NS-1](#_Network_Security_Group)

**Design Decision**: Every subnet must have its own Network Security Group attached.

**Design Justification**: To achieve granular segmentation a Network Security Group is required to be attached to each subnet so that it can locally control network traffic flow. This will be in addition to the Firewall which controls the macro-security rules. This will simplify the overheads required to manage the overall security architecture, as the NSGs will not need to have replica rules from the Firewall, and this can be managed with appropriate routing rules on the respective Route Table resources.

### Deny All Rules

**Design Reference:** Table 6 – [S4](#_Network_Security_Group)

**Design Decision:** Deny all will be placed for inbound internet and subnet connections to each subnet.

**Design Justification:** Deny all internet traffic inbound will prevent malicious actors from reaching the networks from outside sources. Traffic outbound is not required to be explicitly denied as the Route Tables will push outbound traffic to the Azure Firewall which will then handle the outbound traffic.

Additionally, there will be a rule to deny Inter-subnet traffic inbound. This will support true segmentation and inbound rules from other subnets will need to be specifically allowed.

### Logging and Monitoring

**Design Reference:** Table 6 – S7 and Microsoft Security Benchmark LT-4

**Design Decision:** Diagnostic logs will be enabled for NSGs. Additionally, NSG flow logs will also be configured (note that this will require the creation of a NetworkWatcher if one does not already exist).

**Design Justification:** It is a security mandate that logs are collected so that they can be reviewed and alerted on in case of malicious attackers. For NSGs the standard diagnostic logs will be deployed, however there is also a specific requirement to capture traffic flow logs so that activity can be traced. This will also be enabled for all NSGs.

**Design Details:** For the diagnostic settings allLogs and AllMetrics will be captured and forwarded to the central log analytics workspace for that region.

For NSG Flow Logs there are additional components required. A NetworkWatcher will be required. A NetworkWatcher can be deployed once in each region, so if it already exists it can be used, otherwise a new one will be created. Traffic Analytics will also be enabled on the Flow Logs for additional intelligence[[11]](#footnote-12).

# Azure Policies

The only Azure Policy required is already in place to audit NSGs being applied to subnets:

|  |  |
| --- | --- |
| Policy Name | Scopes |
| Audit subnets without Network Security Group | Landing Zones Management Group  Identity Management Group |

Table 8: Azure Policies

# Configuration Templates

Note that there will be no difference between the service tiers. The subnet and virtual network variables will be changed depending on network they are deployed into. The Microsoft default rules will always be deployed and cannot be changed.

## Primary Region Network Security Group

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Name | nsg-[env]-ause-[appname]-[workload]-01 |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia Southeast |
| Resource Group | rg-[env]-ause-[appname]-[workload]-01 |
| Virtual Network | vnet-[env]-ause-[appname]-01 |
| Associated Subnets | snet-[env]-ause-[appname]-[workload]-01 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Inbound Security Rules | |  |  |  |  |  |
| **Priority** | **Name** | **Port** | **Protocol** | **Source** | **Destination** | **Action** |
| **100** | DenyInternetInbound | Any | Any | Internet | Local subnet IP | Deny |
| **200** | DenyInterSubnetInbound | Any | Any | Local subnet IP | Virtual Network IP | Deny |
| **65000** | AllowVnetInBound | Any | Any | VirtualNetwork | Virtual Network IP | Allow |
| **65001** | AllowAzureLoadBalancerInBound | Any | Any | AzureLoadBalancer | Any | Allow |
| **65500** | DenyAllInBound | Any | Any | Any | Any | Deny |
| **Outbound Security Rules** | |  |  |  |  |  |
| **Priority** | **Name** | **Port** | **Protocol** | **Source** | **Destination** | **Action** |
| **100** | AllowIntraSubnetOutbound | Any | Any | Local subnet IP | Local subnet IP | Allow |
| **65000** | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| **65001** | AllowInternetOutBound | Any | Any | Any | Internet | Allow |
| **65500** | DenyAllOutBound | Any | Any | Any | Any | Deny |

## Primary Region NetworkWatcher and NSG Flow Logs

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Name | NetworkWatcher\_australiasoutheast |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia Southeast |
| Resource Group | NetworkWatcher |
| Flow Log Name | nsgfl-[name of the NSG attached] |
| Flow Logs Version | Version 2 |
| Storage Account | st[env]ause[appname]dg01 [or the name of a target Storage Account already deployed in the subscription] |
| Retention Days | 90 |
| Enable Traffic Analytics | Yes |
| Processing Interval | 10 minutes |
| Log Analytics Workspace | law-prd-ause-mgmt-01 |

## Secondary Region Network Security Group

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Name | nsg-[env]-auea-[appname]-[workload]-01 |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia East |
| Resource Group | rg-[env]-auea-[appname]-[workload]-01 |
| Virtual Network | vnet-[env]-ause-[appname]-01 |
| Associated Subnets | snet-[env]-ause-[appname]-[workload]-01 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Inbound Security Rules | |  |  |  |  |  |
| **Priority** | **Name** | **Port** | **Protocol** | **Source** | **Destination** | **Action** |
| **100** | DenyInternetInbound | Any | Any | Local subnet IP | Local subnet IP | Deny |
| **200** | DenyInterSubnetInbound | Any | Any | Local subnet IP | VirtualNetwork | Deny |
| **65000** | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| **65001** | AllowAzureLoadBalancerInBound | Any | Any | AzureLoadBalancer | Any | Allow |
| **65500** | DenyAllInBound | Any | Any | Any | Any | Deny |
| **Outbound Security Rules** | |  |  |  |  |  |
| **Priority** | **Name** | **Port** | **Protocol** | **Source** | **Destination** | **Action** |
| **100** | AllowIntraSubnetOutbound | Any | Any | Local subnet IP | Local subnet IP | Allow |
| **65000** | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| **65001** | AllowInternetOutBound | Any | Any | Any | Internet | Allow |
| **65500** | DenyAllOutBound | Any | Any | Any | Any | Deny |

## Secondary Region NetworkWatcher and NSG Flow Logs

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Name | NetworkWatcher\_australiaeast |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia East |
| Resource Group | NetworkWatcher |
| Flow Log Name | nsgfl-[name of the NSG attached] |
| Flow Logs Version | Version 2 |
| Storage Account | st[env]auea[appname]dg01 [or the name of a target Storage Account already deployed in the subscription] |
| Retention Days | 90 |
| Enable Traffic Analytics | Yes |
| Processing Interval | 10 minutes |
| Log Analytics Workspace | law-prd-auea-mgmt-01 |

# 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://azuremarketplace.microsoft.com/en-us/marketplace/apps/Microsoft.NetworkSecurityGroup?tab=Overview [↑](#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/well-architected/cost/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/virtual-network-security-baseline [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics [↑](#footnote-ref-12)