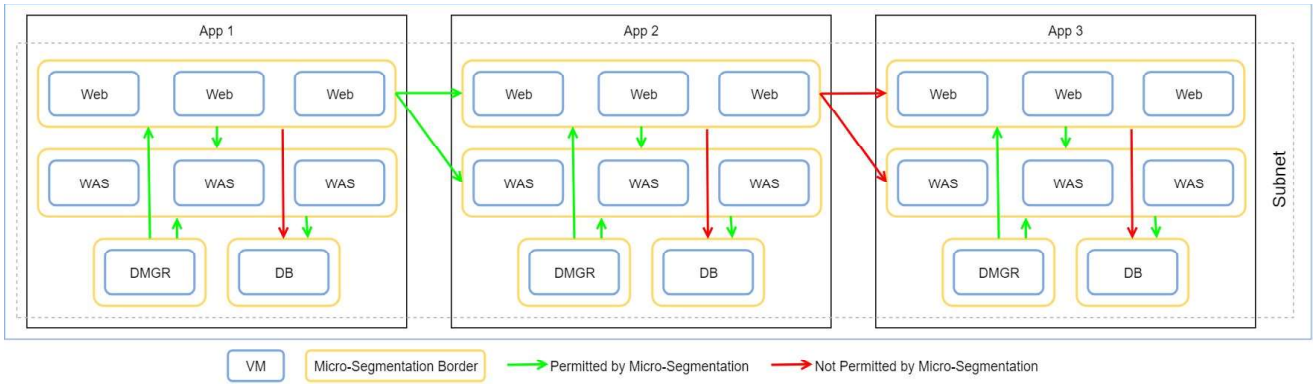
Overview

The aim of micro segmentation is to implement a zero trust policy whereby Virtual Machines cannot communicate with each other unless they are explicitly permitted to, even if they reside on the same subnet.

Network Security Groups, combined with Application Security Groups enable the configuration of network security as a natural extension of an application's structure, allowing the grouping of Virtual Machines and definition of network security policies based on those groups. Application Security Groups enable security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets.

Design Considerations

The following diagram depicts a representation of how Micro-Segmentation will be implemented using BankSphere as a use case;



Design Decisions

Decision Point	Decision	Rationale
Network Security Groups (NSG's), Application Security Groups (ASG's) and Micro-Segmentation	The design and implementation of NSG's and ASG's will support Micro-Segmentation.	Micro-Segmentation is a Production requirement for Applications and Service deployed into the Public Cloud. This mandated by the Global Santander strategy and ratified by Security & Privacy Services / UK CISO.
Default NSG Rules	All Network Security Groups created for Virtual Machines will have a default rule set applied to implement a minimum level of Micro Segmentation.	This will ensure a minimum level of network security is enforced upon provisioning.

Design

This design document will not covered the low level detail of how Micro-Segmentation will be implemented. The requirements for Micro-Segmentation will be defined by Security & Privacy Services / UK CISO and aligned to the Global Santander strategy. Furthermore this design document will not covered the Rule base required to enforce Micro-Segmentation, this will be designed and implemented by the Protect Network Security team. This Network & Application Security Groups section provides design detail on how NSG's and ASG's will be deployed to support Micro-Segmentation.

Default NSG Rules

The tables below provide a summary of the default inbound and outbound rules to be added to be added to a Network Security Group upon creation. These are subject to change, for an up to date view on default rules refer to the following GitLab project linked here.

Inbound Rules

RuleName	Description	Protocol	Direction	Priority	Source Address Prefix	Source Port Range	Destination Address Prefix	Destination Port Range	Access
DenyInternetInbound	Deny Internet Inbound	*	Inbound	4000	*	*	Internet	*	Deny
AllowAnyInbound	All Any Any (Catch All)	*	Inbound	4001	*	*	*	*	Allow

Outbound Rules

RuleName	Description	Protocol	Direction	Priority	Source Address Prefix	Source Port Range	Destination Address Prefix	Destination Port Range	Access
PermittedSSHOutbound	SSH Permitted Outbound	*	Outbound	2100	*	*	22.98.83.48/32, 22.98.84.48/32	22	Allow

DenySSHRDPOutbound	Deny SSH and RDP.	*	Outbound	2101	*	*	*	22, 3389	Deny
DenyInternetOutbound	Deny Internet Outbound	*	Outbound	4000	Internet	*	*	*	Deny
AllowAnyOutbound	All Any Any (Catch All)	*	Outbound	4001	*	*	*	*	Allow

Network Security Groups & Application Security Groups

Overview

Network Security Groups act as a virtual firewall for Azure subnets and virtual machines (VMs). NSG's control access by permitting or denying communication between the workloads within a VNet, from systems on different networks via cross-premises connectivity, or direct Internet communication.

Application Security Groups enable the configuration of network security as a natural extension of an application's structure and simplify the implementation by allowing Virtual Machines to be grouped and referenced in the rules of Network Security Groups. This enable the security policy to scale without manual maintenance of explicit IP addresses.

Design Considerations

- Microsoft do not recommend NSGs be attached at both the Virtual Subnet and vNic level.
- Only one NSG can be applied to a Virtual Subnet or vNic.
- Microsoft recommend the use of augmented security rules in order to define large and complex rule sets into fewer rules;
    - https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#augmented-security-rules
- At the time of writing the following limits apply only for Network and Application Security Groups per region per subscription. The article linked contains the up to date limits.
    - Network Security Groups (NSG) 5000
    - NSG rules per NSG 1000
    - IP addresses and ranges specified for source or destination in a security group 4000
    - Application security groups 3000
    - Application security groups per IP configuration, per NIC 20
    - IP configurations per Application Security Group 4000
    - Application security groups that can be specified within all security rules of a network security group 100
    - https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits?toc=%2fazure%2fvirtual-network%2ftoc.json#azure-resource-manager-virtual-networking-limits
- You can specify one Application Security Group as the source and destination in a security rule. You cannot specify multiple Application Security Groups in the source or destination.
- All network interfaces assigned to an Application Security Group have to exist in the same virtual network that the first network interface assigned to the Application Security Group is in. For example, if the first network interface assigned to an Application Security Group named ASG_Web is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASG_Web must exist in VNet1. You cannot add network interfaces from different virtual networks to the same Application Security Group.
- If you specify an Application Security Group as the source and destination in a security rule, the network interfaces in both Application Security Groups must exist in the same virtual network. For example, if ASG_WAS contained network interfaces from VNet1, and ASG_DB contained network interfaces from VNet2, you could not assign ASG_WAS as the source and ASG_DB as the destination in a rule. All network interfaces for both the source and destination application security groups need to exist in the same virtual network.
- Virtual IP of the host node: Basic infrastructure services in Azure such as DHCP, DNS, and health monitoring are provided through the virtualized host IP addresses 168.63.129.16 and 169.254.169.254. These public IP addresses belong to Microsoft and are the only virtualized IP addresses used in all regions for this purpose. The addresses map to the physical IP address of the server machine (host node) hosting the virtual machine. The host node acts as the DHCP relay, the DNS recursive resolver, and the probe source for the load balancer health probe and the machine health probe. Communication to these IP addresses is not an attack. If traffic is blocked to or from these IP addresses, a virtual machine may not function properly.
- Network Security Groups and Application Security Groups must support Micro-Segmentation.

Design Decisions

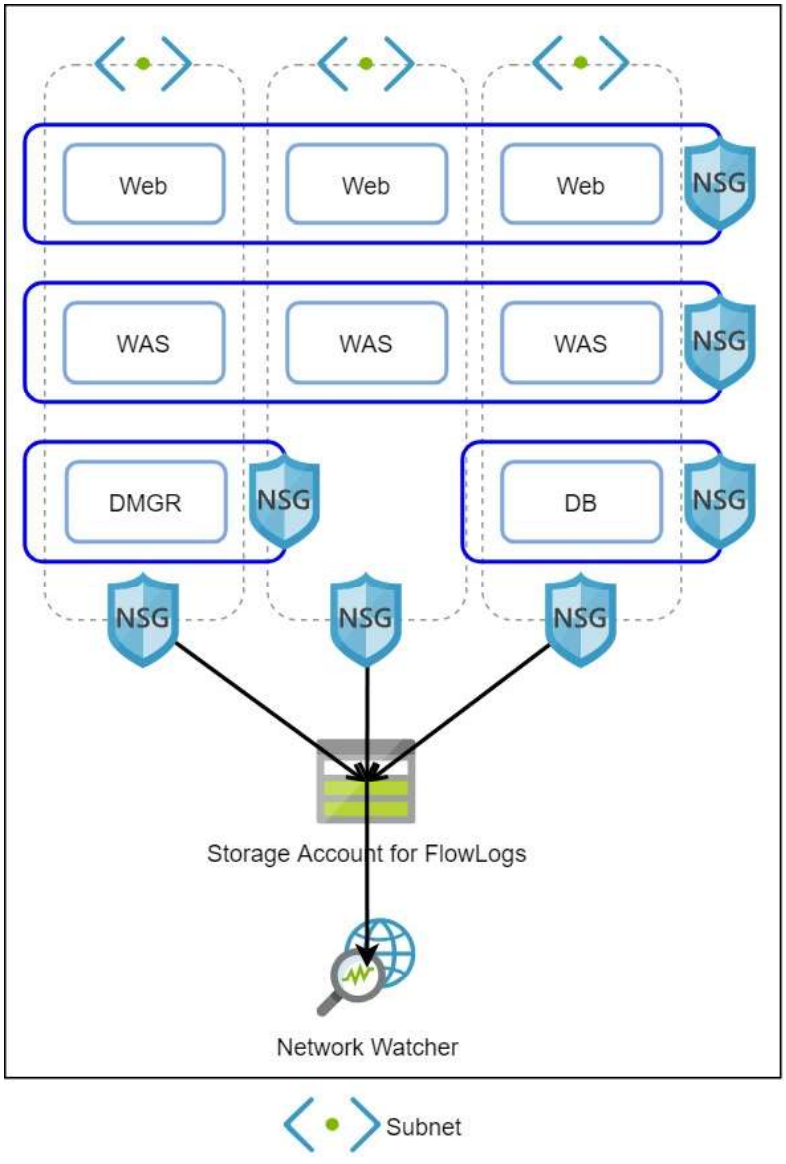
Decision Point	Decision	Rationale
Network Security Groups - Subnets	A Network Security Group will be applied to every subnet. By default the subnet NSG will not enforce any restrictions. The NSG will have FlowLogs enabled.	This enables FlowLogs to be captured for the whole subnet for monitoring. If circumstances require it, a rule can be applied to the NSG to quickly restrict access to the entire subnet.
Network Security Groups - vNics	A Network Security Group will be applied to every vNic. The vNic NSG's will be used to enforce the rules to implement Network Security and Micro-Segmentation. The vNic NSG's will not have FlowLogs enabled by default.	This is required to enforce Network Security and implement Micro-Segmentation.
Network Security Group per App per Server Function	A Network Security Group will be deployed for each Application and Server Function / Tier for example each BankSphere Cell will have a Network Security Group each for it's Web, WAS, DMGR and DB Tiers.	This is required to enforce Network Security and implement Micro-Segmentation. This will simplify the implementation of Network Security and implement Micro-Segmentation and also ensure that NSG limits are not reached.
Application Security	An Application Security Group will be deployed for each Application and Server Function / Tier for example each BankSphere Cell will have	This is required to enforce Network Security and implement Micro-Segmentation.

Group per App per Server Function	a Application Security Group each for it's Web, WAS, DMGR and DB Tiers.	This will simplify the implementation of Network Security and implement Micro-Segmentation and also ensure that ASG limits are not reached.
Adhoc Application Security Groups	Additional Application Security Groups may be created and applied to Virtual Machines as required, for example an ASG could be created for all Virtual Machines in an Application regardless of the Function.	This will enable simpler Network Security rules to be written in Network Security Groups.

Design

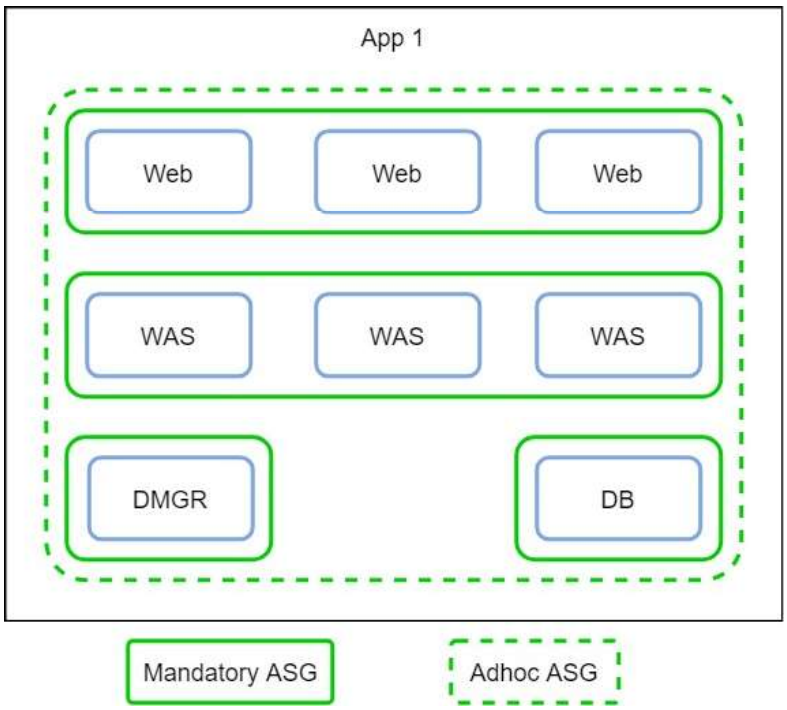
Network Security Groups

The following diagram depicts how Network Security Groups will be deployed using BankSphere as a use case;



Application Security Groups

The following diagram depicts how Application Security Groups will be deployed using BankSphere as a use case;



Data Security

Overview

Microsoft Azure has been designed with security at its core and provides the classical dimensions of information security: Confidentiality, Integrity, and Availability. Azure ensures confidentiality of customer data through identity and access management (authorised access), data encryption (underlying control channels), and isolation (logical and physical).

Below are some high-level points on how Azure secures its Data Centre;

- Restricted physical access to Azure Data Centres
- Logical and physical separation of duties and responsibilities at each Azure Data Centre
- The service management API (SMAPI) runs over TLS and is authenticated by a customer generated certificate and private key
- TLS Mutual Authentication for Internal Control Traffic
- Isolation of Hyper-visor, Root OS, Guest VMs
- Isolation of Fabric Controllers
- Hyper-visor and Root OS network packet filtering
- Multiple levels of monitoring, logging, and reporting

Azure Key Vault & Encryption Keys

Azure Key Vault is a tool for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates and a Vault is logical group of secrets.

Azure Key Vault helps solve the following problems;

- Secrets Management
  - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
- Key Management
  - Azure Key Vault can also be used as a Key Management solution to make it easy to create and control the encryption keys used to encrypt your data
- Certificate Management
  - Azure Key Vault lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL /TLS) certificates
- Store secrets backed by Hardware Security Modules
  - Secrets and keys can be protected either by software or FIPS 140-2 Level 2 validates HSMs

Azure Key Vault integrates with other Azure services and can be used as a secure store to simplify scenarios like;

- Azure Disk Encryption
- The always encrypted functionality in SQL server and Azure SQL Database
- Encryption of;
  - Storage Accounts
  - Event hubs
  - Log Analytics