

# Azure Networking

By default, the Front-end and Back-end app services are accessible from the Public Internet. The rest of the utilized Azure resources - Key Vault, Azure SQL Server, Azure Cosmos DB and Storage Account - are secured behind firewalls and private connections.

When deploying SysKit Point, there are two options available when considering Azure network resources:

## 1. Deploy SysKit Point from Azure Marketplace    2. Deploy a custom ARM template

- consider this to be your 'plug-and-play' option
- new Azure network resources are automatically created and configured when you deploy SysKit Point, without the need to perform additional configuration
- SysKit Point is ready to use and secured after the deployment
- use when you want to integrate SysKit Point into already existing Azure network resources
- custom ARM templates are used when deploying SysKit Point
- no Azure network resources are created when deploying SysKit Point through custom ARM templates
- SysKit Point is ready to use but not secured after the deployment - additional configuration of Azure network resources is required

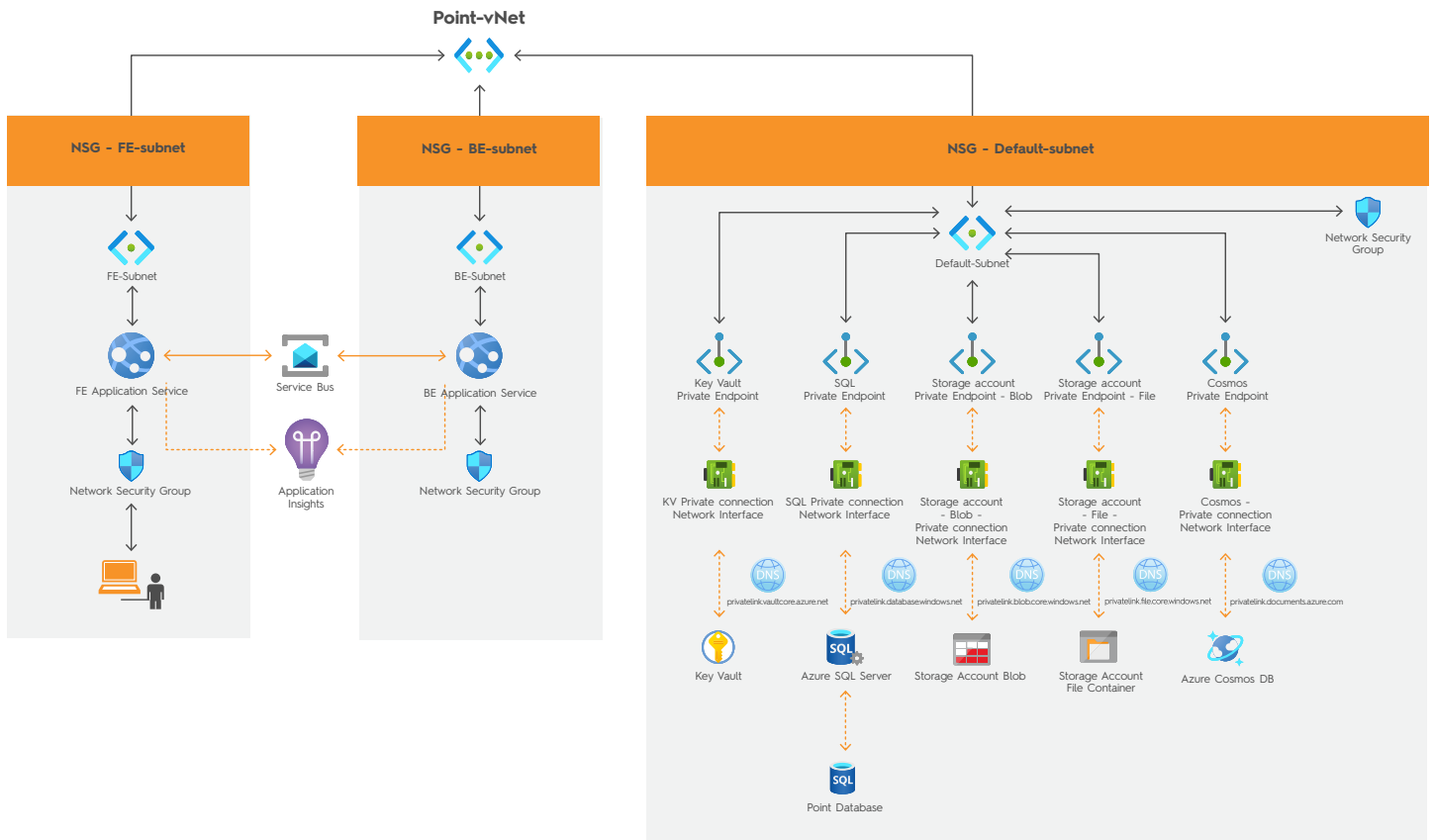
### Please note!

For use cases requiring custom deployment and manual configuration of Azure network resources, [don't hesitate to contact us](#) to provide you with custom ARM templates.

## Architecture Diagram

When SysKit Point is deployed from Azure Marketplace, a virtual network is created named point-vnet, with three subnets:

- fe-subnet (1)
- be-subnet (2)
- default-subnet (3)



# Azure Networking

The subnets have Network security groups associated with the default rules applied. By default, inbound traffic is denied, and outbound traffic is allowed. If you wish to limit outbound traffic, please [contact us](#).

## The following applies to fe-subnet:

- takes up 3 IP addresses + 5 Azure reserved addresses
- used by a Front-end app service that provides end-users with a web interface
- accessible from the Public Internet

## The following applies to be-subnet:

- takes up 3 IP addresses + 5 Azure reserved addresses
- used by a Back-end app service responsible for retrieving data from a Microsoft 365 tenant by utilizing several Microsoft APIs
- accessible from the Public Internet

## The following applies to default-subnet:

- takes up 11 IP addresses + 5 Azure reserved addresses
- used by the following Azure resources:
  - Key Vault
  - Azure SQL Server
  - Azure Cosmos DB
  - Storage Account - Blob
  - Storage Account - File
- secured with private connections for each resource

### Please note!

As the Front-end and Back-end app services are accessible from the Public Internet by default, [use Azure App Service access restrictions](#) to add another layer of security to SysKit Point app services.