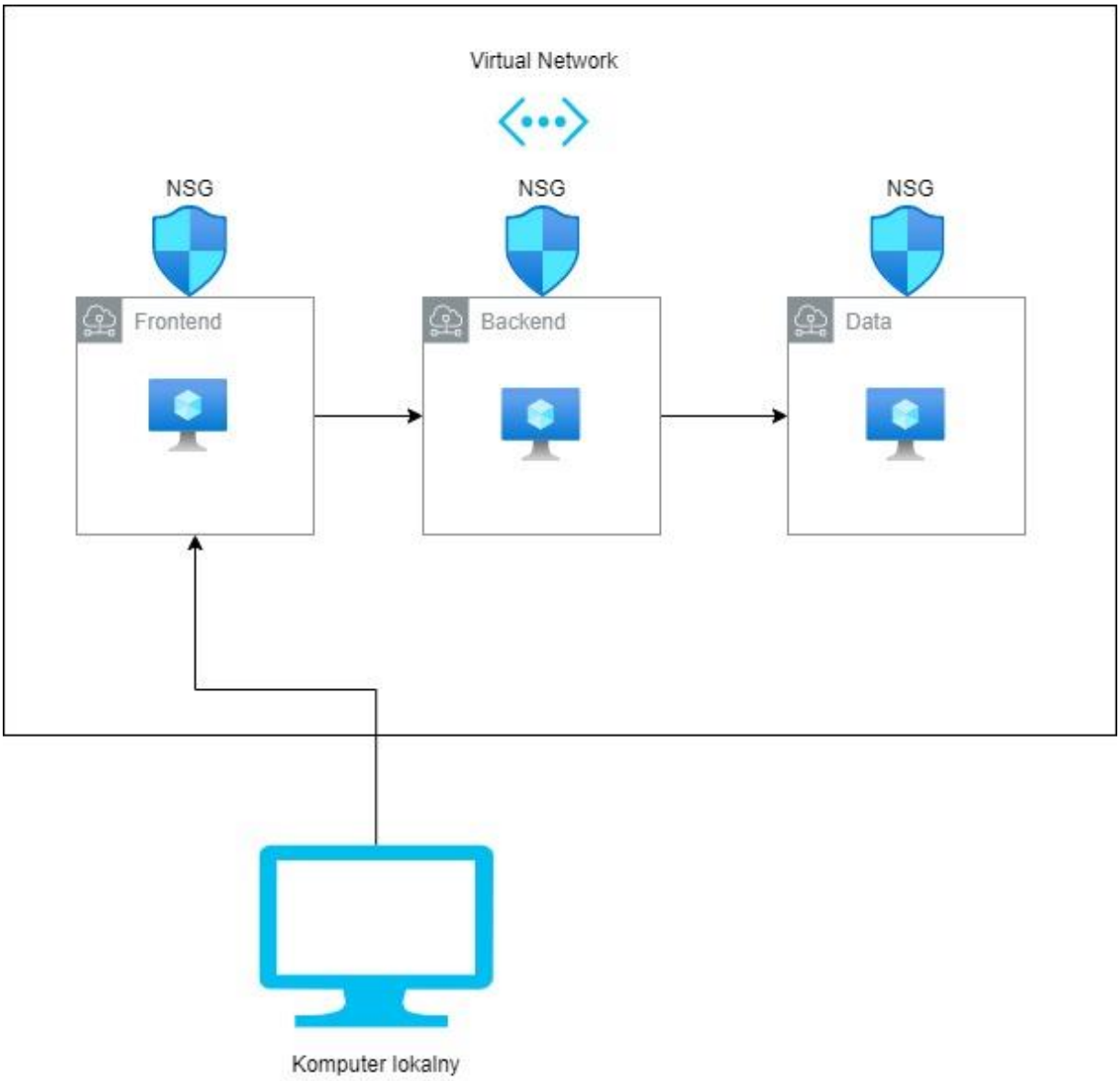
Zadanie 3 – Utworzenie infrastruktury N-Tier

Zadanie polega na utworzeniu infrastruktury N-Tier przedstawionej na poniższym rysunku:



Opis infrastruktury do utworzenia:

Należy utworzyć sieć wirtualną zawierającą 3 podsieci z maszynami wirtualnymi oraz odpowiednimi Network Security Grupami:

- Frontend – Sieć wejściowa. Maszyna wirtualna , która się w niej znajduje, posiada publiczny oraz prywatny adres IP, Network Security Group zezwala na ruch wejściowy z internetu na porcie 22 oraz blokuje całkowicie ruch z innych podsieci znajdujących się w Virtual Network.
- Backend – Network Security Group zezwala wyłącznie na ruch przychodzący z podsieci Frontend, nie akceptuje innego ruchu wchodzącego z innych podsieci

- Data – Network Security Group zezwala wyłącznie na ruch przychodzący z podsieci Backend, nie zezwala na ruch przychodzący z innych podsieci

Projekt Terraform powinien zostać podzielony na foldery, przykładowo:

- TENANT
- NETWORK
- SECURITY
- VMs

Aby prawidłowo pobierać dane zasobów znajdujących się w innych folderach należy wykorzystać Terraform data lub output, pomocna dokumentacja:

- Data - Data Sources - Configuration Language - Terraform by HashiCorp
- Output - Output Values - Configuration Language - Terraform by HashiCorp

W celu poprawnego utworzenia zasobów należy posiłkować się główną dokumentacją Azure Providera Terraform - Docs overview | hashicorp/azurerm | Terraform Registry

Przykładowe zasady sieciowe:

Zezwolenie na ruch wejściowy z podsieci 10.0.1.0/24

```
direction                  = "Inbound"
access                     = "Allow"
protocol                   = "*"
source_port_range          = "*"
destination_port_range     = "*"
source_address_prefix      = 10.0.1.0/24
destination_address_prefix = "VirtualNetwork"
```

Zablokowanie ruchu wejściowego z innych podsieci

```
direction                  = "Inbound"
access                     = "Deny"
protocol                   = "*"
source_port_range          = "*"
destination_port_range     = "*"
source_address_prefix      = "VirtualNetwork"
destination_address_prefix = "VirtualNetwork"
```

Efektem końcowym rozwiązania zadania jest możliwość zalogowania się używając SSH jedynie do maszyny podsieci Frontend z internetu publicznego. Do maszyny w podsieci Frontend nie powinna móc się zalogować żadna inna maszyna z sieci prywatnej. Do maszyny w podsieci Backend może zalogować się wyłącznie maszyna z podsieci Frontend. Do maszyny z sieci Data można zalogować się wyłącznie z maszyny w podsieci Backend.

Wszystkie sekrety powinny zostać przekazane do skryptu Terraform w bezpieczny sposób (w zadaniu stan jest przechowywany na komputerze lokalnym co dalej powoduje rzeczywiste niebezpieczeństwo. Zakłada się, że w rzeczywistości stan jest przechowywany w enkryptowanym bezpiecznym środowisku)

O bezpiecznym przekazywaniu sekretów:

A comprehensive guide to managing secrets in your Terraform code | by Yevgeniy Brikman | Gruntwork