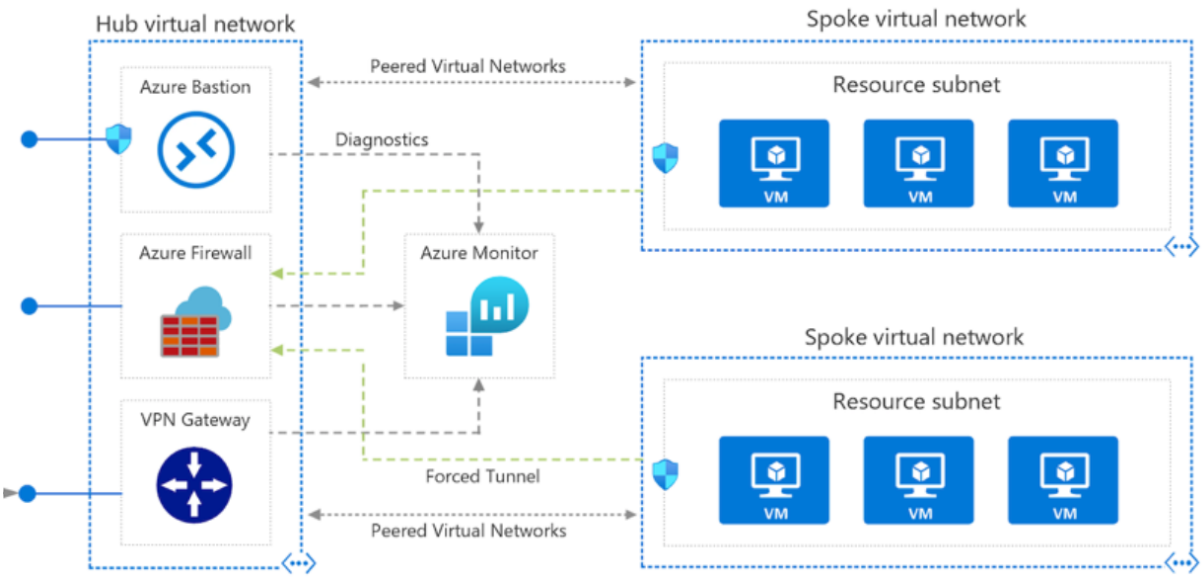
Chmurowisko

Szkolenie Terraform: Dzień 2

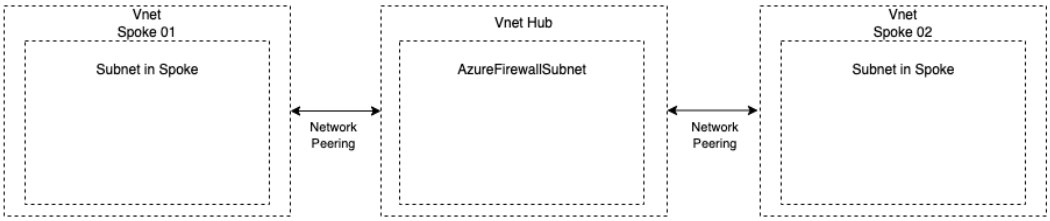
1. Zadanie: Budowa sieci Hub & Spoke

Przykładowa architektura rozwiązania zbudowanego w sieci Hub & Spoke widoczna jest na Rys. *1*.



Rys. 1 Przykładowa architektura sieci Hub & Spoke

Architektura sieciowa oraz zasoby tworzone w ramach zadania 1 są widoczne na Rys. 2.



Rys. 2 Architektura sieciowa Zad 1.

Opis zadania: Należy zbudować strukturę sieciową przedstawioną na Rys. 2.

Należy utworzyć dwie sieci virtualne (nie kolidujące adresacją) oraz w każdej z nich utworzyć 1 subnet po czym utworzyć peering między sieciami spoke a siecią hub zgodnie z rysunkiem.

Peering należy utworzyć w obie strony (w stronę sieci Spoke i w stronę sieci Hub). Podczas tworzenia peeringu należy nadać wartość „true" w parametrach: allow_virtual_network_access oraz allow_forwarded_traffic.

UWAGA: W podsieci w sieci VNet Hub, będzie tworzony Azure Firewall więc musi nazywać się „AzureFirewallSubnet" oraz posiadać maskę /26 np. 10.0.0.0/26.

Przykładowa adresacja sieci:

- Vnet Hub – 10.0.0.0/16
- Vnet Spoke 1 – 10.1.0.0/16
- Vnet Spoke 2 – 10.2.0.0/16
- Subnet in Hub – 10.0.0.0/26 (musi nazywać się „AzureFirewallSubnet”).
- Subnet in Spoke 1 – 10.1.0.0/24
- Subnet in Spoke 2 – 10.2.0.0/24

Zasoby które należy utworzyć:

- Sieć wirtualna Vnet Hub
- Sieć wirtualna Vnet Spoke 1
- Sieć wirtualna Vnet Spoke 2
- Subnet w sieci wirtualnej Vnet Hub
- Subnet w sieci wirtualnej Vnet Spoke 1
- Subnet w sieci wirtualnej Vnet Spoke 2
- Peering z sieci Vnet Hub do sieci Vnet Spoke 1
- Peering z sieci Vnet Spoke 1 do sieci Vnet Hub
- Peering z sieci Vnet Hub do sieci Vnet Spoke 2
- Peering z sieci Vnet Spoke 2 do sieci Vnet Hub

Przydatne linki:
Terraform dokumentacja sieci wirtualnych
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/virtual_network

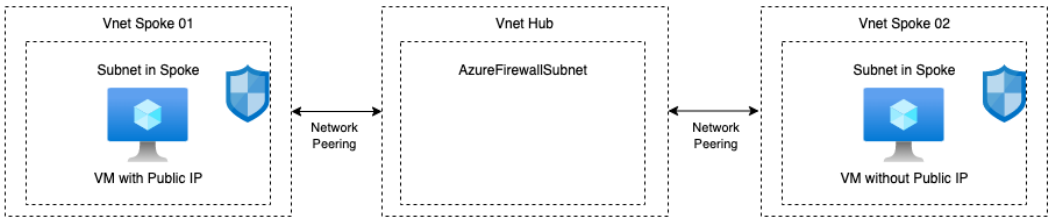
Terraform dokumentacja subnetów
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/subnet

Terraform dokumentacja peeringu
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/virtual_network_peering

Przykładowe rozwiązanie znajduje się w folderze „1-HubAndSpoke”

2. Zadanie: Utworzenie maszyn wirtualnych w sieciach Spoke oraz NSG

Należy utworzyć dwie maszyny wirtualne: jedna w sieci spoke 1, druga w sieci spoke 2. Maszyna w sieci spoke 1 powinna posiadać również publiczny adres IP jak widoczne poniżej:



Rys. 3 Architektura Zad 2.

Zasoby które należy utworzyć (w kolejności):

- Publiczny adres IP dla maszyny w vnet spoke 1
- 2x Network interface dla maszyn wirtualnych
- 2x NSG dla maszyn wirtualnych
- 2x network interface security group association (powiązanie NSG z interfejsem maszyny)
- 2x Maszyna wirtualna – Ubuntu z logowaniem po użytkowniku i haśle

Na NSG maszyny wirtualnej z publiczny adresem IP dodaj regułę, która pozwala na ruch poprzez SSH. Zaloguj się poprzez SSH na maszynie wirtualnej w Spoke 1 posiadającej publiczny adres IP i spróbuj połączyć się z maszyną Spoke 2.

Przydatne linki:
Terraform dokumentacja publiczny adres IP
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/public_ip

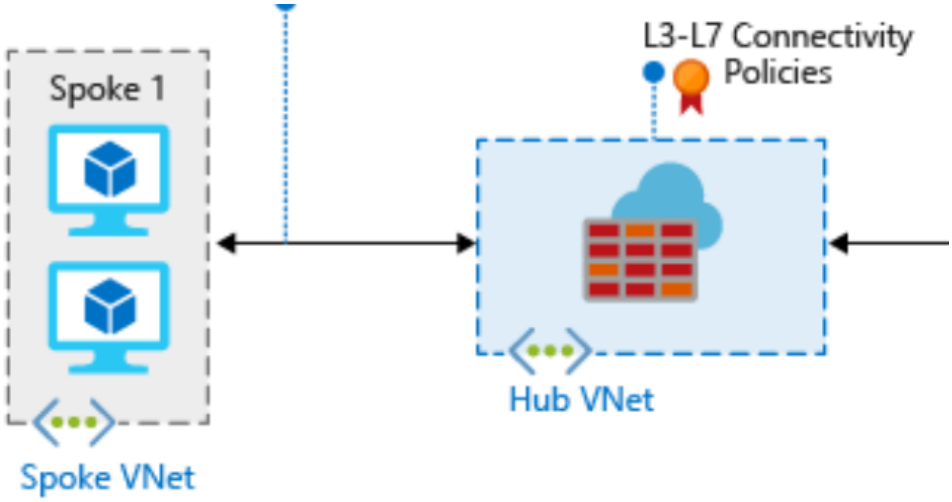
Terraform dokumentacja network interface
https://registry.terraform.io/providers/hashicorp/aws/latest/docs/resources/network_interface

Terraform dokumentacja NSG
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/network_security_group

Terraform dokumentacja dowiązania NSG do network interface
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/network_interface_security_group_association

Terraform dokumentacja linux VM
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/linux_virtual_machine

3. Zadanie: Utworzenie Azure Firewall oraz reguł



W tym zadaniu wykorzystamy utworzą wcześniej podsieć w ramach sieci Hub o nazwie „AzureFirewallSubnet”.

Do reguł firewalla należy dodać regułę, która pozwala na ruch z wykorzystaniem:

- Port: 22
- Adresy źródłowe: *
- Adresy docelowe: *
- Protokół: TCP

Zasoby które należy utworzyć (w kolejności):

- Publiczny adres IP wykorzystywany przez Azure Firewall
- Azure Firewall Policy
- Azure Firewall Policy Rule Collection Group
- Azure Firewall (tworzenie zasobu trwa długo w Azure – około 5-10 minut)

Przydatne linki:
Terraform dokumentacja publiczny adres IP
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/public_ip

Terraform dokumentacja Azure Firewall Policy
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/firewall_policy

Terraform dokumentacja Azure Firewall Policy Rule Collection Group
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/firewall_policy_rule_collection_group

Terraform dokumentacja Azure Firewall
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/firewall

4. Zadanie: Utworzenie UDR kierującego ruch do sieci spoke przez Azure Firewall w sieci hub

Zasoby które należy utworzyć (w kolejności):

- Route Table dla Spoke 1
- Route Table dla Spoke 2
- Dowiązanie Route Table do podsieci posiadającej VM w sieci Spoke 1
- Dowiązanie Route Table do podsieci posiadającej VM w sieci Spoke 2

W przypadku Route Table dowiązanego do podsiecie w Spoke 1, należy dodać trasę kierującą na:

- Nazwa: toSpoke2
- Address: 10.2.0.0/16
- Next_hop_type: „VirtualAppliance”
- Next_hop_in_ip_address: Prywatny adres IP Firewalla

W przypadku Route Table dowiązanego do podsiecie w Spoke 2, należy dodać trasę kierującą na:

- Nazwa: toSpoke1
- Address: 10.1.0.0/16
- Next_hop_type: „VirtualAppliance”
- Next_hop_in_ip_address: Prywatny adres IP Firewalla

Przydatne linki:
Terraform dokumentacja Route Table
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/route_table

Terraform dokumentacja dowiązania Route Table do podsieci
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/subnet_route_table_association

5. Zadanie: Przetestowanie komunikacji

Zaloguj się poprzez SSH na maszynie wirtualnej w Spoke 1 posiadającej publiczny adres IP i spróbuj połączyć się z maszyną Spoke 2.