Obraz zawierający tekst, Czcionka, biały, logo

Opis wygenerowany automatycznie

**Programowe i techniczne środki bezpieczeństwa**

Projekt:   
Implementacja podstawowych środków bezpieczeństwa sieciowego w chmurze Microsoft Azure

Tomasz Stanisławczyk w69609

Sebastian Czapka w69553

10.05.2024 r.

Spis treści

[1. Wprowadzenie 3](#_Toc166161361)

[1.1. Cel i zakres projektu 3](#_Toc166161362)

[2. Podstawy Microsoft Azure 3](#_Toc166161363)

[3. Realizacja podstawowej sieci Virtual Network w Azure 5](#_Toc166161364)

[3.1. Założenia projektowe 5](#_Toc166161365)

[3.2. Konfiguracja NSG (Network Security Groups) 6](#_Toc166161366)

[3.3. Weryfikacja i walidacji modelu 8](#_Toc166161367)

[4. Implementacja 9](#_Toc166161368)

[4.1. dd 9](#_Toc166161369)

[5. Wpływ n 18](#_Toc166161370)

[6. Bibliografia 18](#_Toc166161371)

1. Wprowadzenie

W dobie cyfryzacji i rosnącej zależności od technologii, bezpieczeństwo sieciowe stało się kluczowym elementem ochrony danych i infrastruktury IT. Chmura Microsoft Azure, będąca jedną z czołowych platform usług chmurowych, oferuje szeroki zakres możliwości konfiguracji i zabezpieczenia infrastruktury sieciowej.

# Cel i zakres projektu

Celem projektu jest zaprojektowanie i wdrożenie zestawu podstawowych środków bezpieczeństwa sieciowego w środowisku Azure, które zapewnią ochronę infrastruktury sieciowej przed najczęstszymi zagrożeniami cybernetycznymi. Projekt ma na celu stworzenie solidnej i elastycznej architektury sieciowej, która będzie mogła sprostać wymaganiom współczesnych aplikacji biznesowych, jednocześnie zapewniając łatwość zarządzania i monitorowania.

Zakres projektu obejmuje omówienie podstawowych jednostek infrastruktury Azure, przedstawienie konfiguracji wirtualnej sieci wraz z zabezpieczeniem ruchu sieciowego. Infrastruktura zostanie utworzona przy wykorzystaniu narzędzia Infrastructure as a Code – Terraform, z kodem przechowywanym w repozytorium github.

1. Podstawy Microsoft Azure

Chmura Azure (cloud computing) to platforma usług chmurowych firmy Microsoft, która oferuje szeroki zakres usług, w tym obliczeniowe, analityczne, przechowywanie danych i sieciowe. W przeciwieństwie do tradycyjnych rozwiązań “on-premise”, gdzie wszystko jest instalowane i zarządzane lokalnie w infrastrukturze firmy, chmura oferuje dostęp do zasobów komputerowych i usług zarządzanych przez dostawcę usług chmurowych. Podstawową różnicą między chmurami jest lokalizacja, modelu on-premise, infrastruktura IT (serwery, pamięć masowa, itp.) jest fizycznie zlokalizowana w siedzibie firmy. W chmurze, te zasoby są hostowane na serwerach dostawcy usług chmurowych i są dostępne przez Internet.

Podstawową jednostką od której należy zacząć pracę są Grupy zarządzania (Management Groups). Są to kontenery, które pozwalają na organizację subskrypcji w hierarchiczne struktury zapewniając zakres zarządzania powyżej subskrypcji, umożliwiając stosowanie polityk i zarządzanie dostępem na dużą skalę. Każda grupa zarządzania może zawierać inne grupy zarządzania lub subskrypcje, ale nie może zawierać bezpośrednio zasobów.

Subskrypcje z kolei są to umowy, które po zamówieniu u dostawcy pozwalają na korzystanie z zasobów Azure i są podstawową jednostką rozliczeniową. Subskrypcje mogą być zorganizowane w grupach zarządzania i dziedziczyć polityki z tych grup. Aby zacząć korzystanie z infrastruktury w Azure, po wykupieniu subskrypcji należy utworzyć grupę (lub grupy) zasobów (Resource Groups) które służą jako logiczne kontenery, w kórych można tworzyć zasoby chmurowe (Resources). Wszystkie zasoby w grupie zasobów muszą znajdować się w tej samej lokalizacji geograficznej.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources

W kontekście sieci wirtualnych, Azure Virtual Network (VNet) jest podstawowym budulcem, który umożliwia tworzenie prywatnej sieci w Azure. VNet pozwala na bezpieczną komunikację między zasobami Azure, internetem oraz sieciami lokalnymi (on-premises). Sieci wirtualne umożliwiają tworzenie izolowanych sieci w chmurze, które mogą być połączone z lokalnymi sieciami on-premise, tworząc hybrydowe środowisko, które łączy w sobie zalety obu podejść. Dzięki temu firmy mogą korzystać z zaawansowanych technologii chmurowych, jednocześnie zachowując niektóre zasoby i aplikacje na własnej infrastrukturze.  
Sieci wirtualne umożliwiają komunikację z internetem, domyślnie komunikować się z Internetem. Można również użyć publicznego adresu IP, bramy NAT lub publicznego balancera obciążenia do zarządzania połączeniami wychodzącymi. Zasoby w Azure mogą bezpiecznie komunikować się ze sobą w ramach VNet. Można również korzystać z punktów końcowych usług sieciowych (VNet Endpoints) , aby rozszerzyć przestrzeń adresową i tożsamość VNet do zasobów Azure umieszczonych w innych VNetach. Możliwe jest również połączenie lokalnych komputerów, serwerów i sieci i sieci z VNet za pomocą bramy VPN lub Azure ExpressRoute, co umożliwia tworzenie hybrydowych architektur sieciowych.

1. Realizacja podstawowej sieci Virtual Network w Azure

# Założenia projektowe

Celem projektu jest konfiguracja sieci VNet pod szerokie zastosowanie praktyczne.

Infrastruktura powstanie w postaci kodu Terraform (Infrastructure as a Code) w repozytorium GitHub, gdzie skonfigurowana zostanie również automatyzacja tworzenia infrastruktury w chmurze Azure, za pomocą GitHub Actions Pipelines.

# Konfiguracja NSG (Network Security Groups)

**nsg\_backend** Inbound Security Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Priority | Port | Protocol | Source | Destination | Action |
| AllowSshInBound | 100 | 22 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowRdpInBound | 200 | 3389 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowHttpsInBound | 300 | 443 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowHttpInBound | 400 | 80 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowMsSqlInBoundTcp | 500 | 1433 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowMsSqlInBoundUdp | 600 | 1434 | Udp | Tooling VNet | VirtualNetwork | Allow |
| AllowPostgreSqlInBoundTcp | 700 | 5432 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowPostgreSqlInBoundUdp | 800 | 5432 | Udp | Tooling VNet | VirtualNetwork | Allow |
| AllowMsSqlVnetInboundTcp | 900 | 1433 | Tcp | VirtualNetwork | VirtualNetwork | Allow |
| AllowMsSqlVnetInboundUdp | 1000 | 1434 | Udp | VirtualNetwork | VirtualNetwork | Allow |
| AllowPostgreSqlVnetInboundTcp | 1100 | 5432 | Tcp | VirtualNetwork | VirtualNetwork | Allow |
| AllowPostgreSqlVnetInboundUdp | 1200 | 5432 | Udp | VirtualNetwork | VirtualNetwork | Allow |
| DenyAllInBound | 4000 | Any | Tcp | Any | Any | Deny |
| AllowVnetInBound | 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| AllowAzureLoadBalancerInBound | 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| DenyAllInBound | 65500 | Any | Any | Any | Any | Deny |

**nsg\_backend** Outbound Security Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Priority | Port | Protocol | Source | Destination | Action |
| AllowSshOutBound | 100 | 22 | Tcp | Any | Any | Allow |
| AllowHttpsOutBound | 200 | 443 | Tcp | Any | Any | Allow |
| AllowHttpOutBound | 300 | 80 | Tcp | Any | Any | Allow |
| AllowVnetOutBound | 400 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| DenyAllOutBound | 4000 | Any | Any | Any | Any | Deny |
| AllowVnetOutBound | 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| AllowInternetOutBound | 65001 | Any | Any | Any | Internet | Allow |
| DenyAllOutBound | 65500 | Any | Any | Any | Any | Deny |

**nsg\_iaas** Inbound Security Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Priority | Port | Protocol | Source | Destination | Action |
| AllowSshInBound | 100 | 22 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowRdpInBound | 200 | 3389 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowHttpsInBound | 300 | 443 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowHttpInBound | 400 | 80 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowVnetInBound | 500 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| DenyAllInBound | 4000 | Any | Any | Any | Any | Deny |
| AllowVnetInBound | 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| AllowAzureLoadBalancerInBound | 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| DenyAllInBound | 65500 | Any | Any | Any | Any | Deny |

**nsg\_iaas** Outbound Security Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Priority | Port | Protocol | Source | Destination | Action |
| AllowSshOutBound | 100 | 22 | Tcp | Any | Any | Allow |
| AllowHttpsOutBound | 200 | 443 | Tcp | Any | Any | Allow |
| AllowHttpOutBound | 300 | 80 | Tcp | Any | Any | Allow |
| AllowVnetOutBound | 400 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| DenyAllOutBound | 4000 | Any | Any | Any | Any | Deny |
| AllowVnetOutBound | 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| AllowInternetOutBound | 65001 | Any | Any | Any | Internet | Allow |
| DenyAllOutBound | 65500 | Any | Any | Any | Any | Deny |

**nsg\_paas** Inbound Security Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Priority | Port | Protocol | Source | Destination | Action |
| AllowSshInBound | 100 | 22 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowRdpInBound | 200 | 3389 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowHttpsInBound | 300 | 443 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowHttpInBound | 400 | 80 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowVnetInBound | 500 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| DenyAllInBound | 4000 | Any | Any | Any | Any | Deny |
| AllowVnetInBound | 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| AllowAzureLoadBalancerInBound | 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| DenyAllInBound | 65500 | Any | Any | Any | Any | Deny |

**nsg\_paas** Outbound Security Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Priority | Port | Protocol | Source | Destination | Action |
| AllowSshOutBound | 100 | 22 | Tcp | Any | Any | Allow |
| AllowHttpsOutBound | 200 | 443 | Tcp | Any | Any | Allow |
| AllowHttpOutBound | 300 | 80 | Tcp | Any | Any | Allow |
| AllowVnetOutBound | 400 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| DenyAllOutBound | 4000 | Any | Any | Any | Any | Deny |
| AllowVnetOutBound | 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| AllowInternetOutBound | 65001 | Any | Any | Any | Internet | Allow |
| DenyAllOutBound | 65500 | Any | Any | Any | Any | Deny |

**nsg\_public** Inbound Security Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Priority | Port | Protocol | Source | Destination | Action |
| AllowSshInBound | 100 | 22 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowRdpInBound | 200 | 3389 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowHttpsInBound | 300 | 443 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowHttpInBound | 400 | 80 | Tcp | Tooling VNet | VirtualNetwork | Allow |
| AllowVnetInBound | 500 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| DenyAllInBound | 4000 | Any | Any | Any | Any | Deny |
| AllowVnetInBound | 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| AllowAzureLoadBalancerInBound | 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| DenyAllInBound | 65500 | Any | Any | Any | Any | Deny |

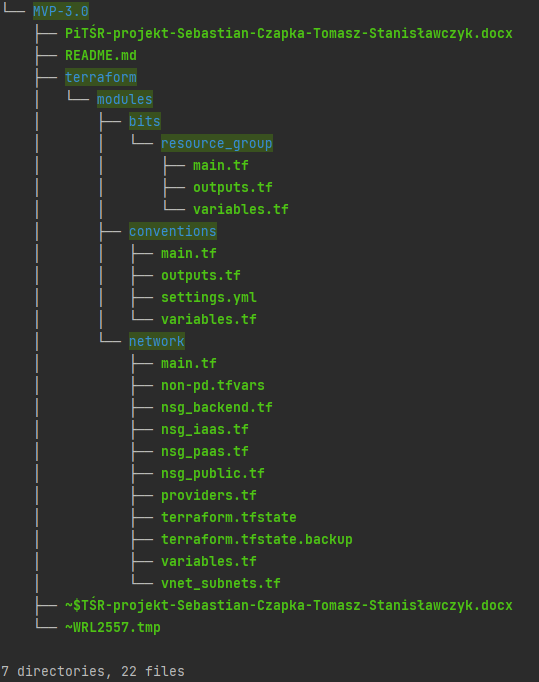
**nsg\_public** Outbound Security Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Priority | Port | Protocol | Source | Destination | Action |
| AllowSshOutBound | 100 | 22 | Tcp | Any | Any | Allow |
| AllowHttpsOutBound | 200 | 443 | Tcp | Any | Any | Allow |
| AllowHttpOutBound | 300 | 80 | Tcp | Any | Any | Allow |
| DenyAllOutBound | 4000 | Any | Any | Any | Any | Deny |
| AllowVnetOutBound | 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| AllowInternetOutBound | 65001 | Any | Any | Any | Internet | Allow |
| DenyAllOutBound | 65500 | Any | Any | Any | Any | Deny |

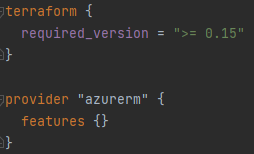
# Weryfikacja i walidacji modelu

Współpraca z kierowcami jest kluczowa. Ich subiektywne doświadczenia i opinie na temat.

1. Implementacja
   1. dd

W o 

Rysunek 1 Widok modelu samochodu ze specyficznymi zagęszczeniami [1]

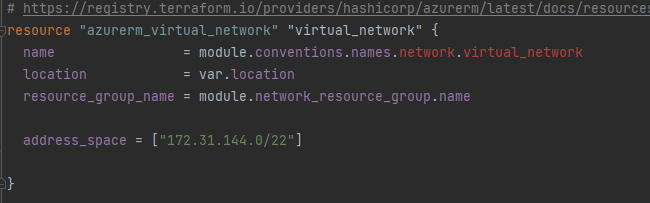


Rysunek 1 Widok modelu samochodu ze specyficznymi zagęszczeniami [1]

Pracę z Terraform należy rozpocząć od konfiguracji providerów. Konfiguracja ta określa wymagania i ustawienia dla dostawcy usług chmurowych, używanego do zarządzania zasobami.

**required\_version**: Określa minimalną wymaganą wersję Terraform, która jest potrzebna do uruchomienia konfiguracji. W tym przypadku, konfiguracja wymaga wersji Terraform 0.15 lub nowszej.

**provider “azurerm”:** Definiuje dostawcę dla Microsoft Azure Resource Manager, który jest używany do interakcji z zasobami Azure. Blok features {} jest wymagany, ale w tym przypadku jest pusty, co oznacza, że nie są ustawione żadne specyficzne funkcje lub opcje dla dostawcy.



Rysunek 1 Widok modelu samochodu ze specyficznymi zagęszczeniami [1]

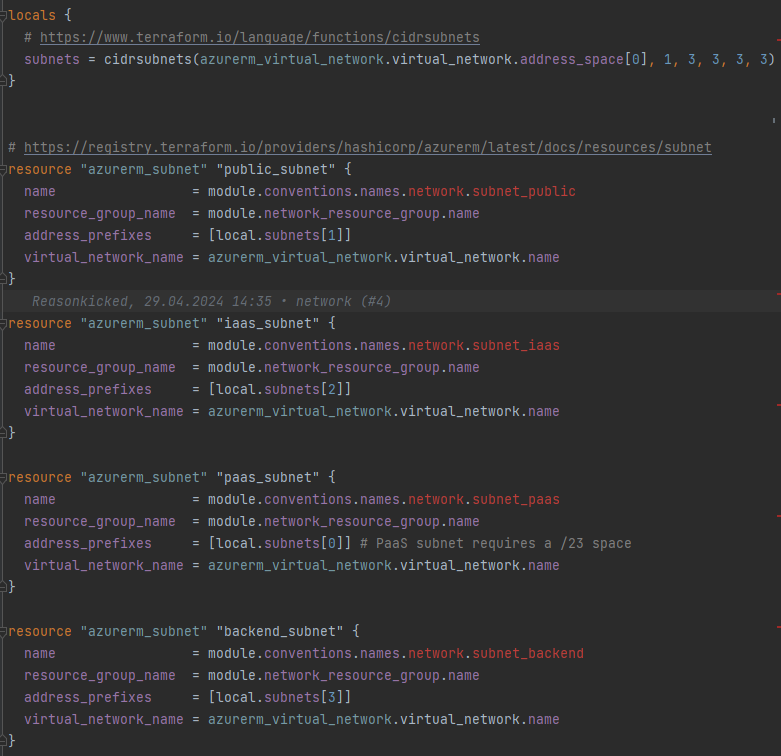
Konfiguracja, którą widzimy, jest fragmentem kodu Terraform, który definiuje zasób **azurerm\_virtual\_network** w chmurze Azure.

**name:** Określa nazwę wirtualnej sieci (VNet). W tym przypadku używana jest wartość zwrócona przez moduł conventions.names.network.virtual\_network.

**location:** Wskazuje lokalizację, w której VNet zostanie utworzone. Jest to miejsce, w którym fizycznie znajduje się infrastruktura Azure.

**resource\_group\_name:** Określa nazwę grupy zasobów, do której VNet zostanie przypisane. Grupa zasobów jest logicznym kontenerem dla zasobów w Azure.

**address\_space**: Definiuje przestrzeń adresową VNet. W tym przypadku używany jest zakres adresów IP w formacie CIDR (np. “172.31.144.0/22”), który określa dostępne adresy IP dla zasobów wewnątrz VNet.



Rysunek 1 Widok modelu samochodu ze specyficznymi zagęszczeniami [1]

Konfiguracja subnetów w Terraform definiuje cztery subnety w ramach wirtualnej sieci.

**locals:** Definiuje lokalną zmienną subnets, która korzysta z funkcji cidrsubnets do generowania listy podsieci na podstawie przestrzeni adresowej VNet. Argumenty 1, 3, 3, 3, 3 określają, jak podzielić przestrzeń adresową na mniejsze podsieci.

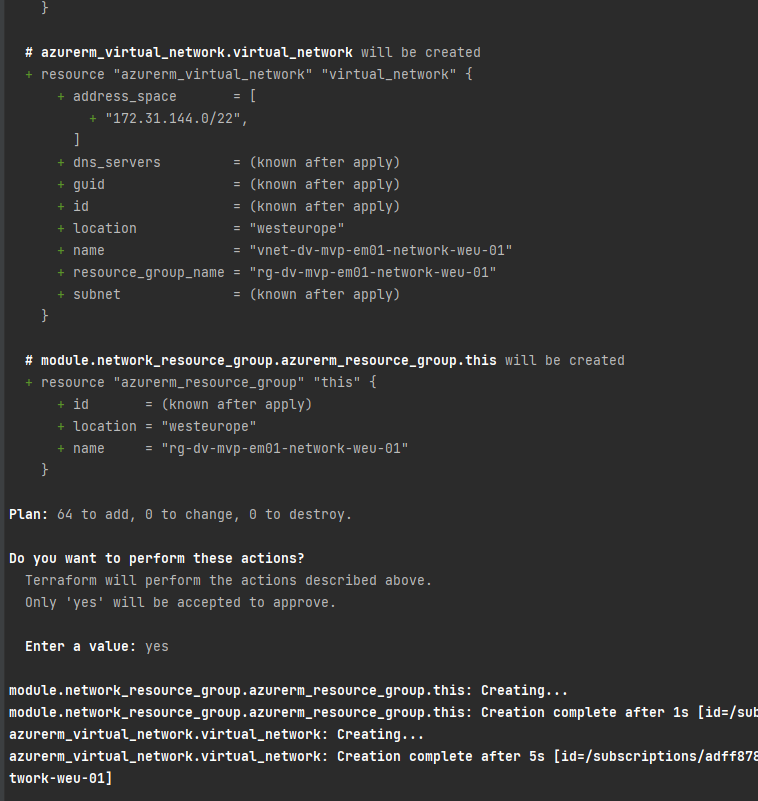
**resource “azurerm\_subnet” “public\_subnet”:** Tworzy publiczną podsieć o nazwie określonej przez moduł conventions.names.network.subnet\_public. Używa drugiego adresu z listy local.subnets jako swojej przestrzeni adresowej.

**resource “azurerm\_subnet” “iaas\_subnet”:** Tworzy podsieć IaaS (Infrastructure as a Service) z trzecim adresem z listy local.subnets.

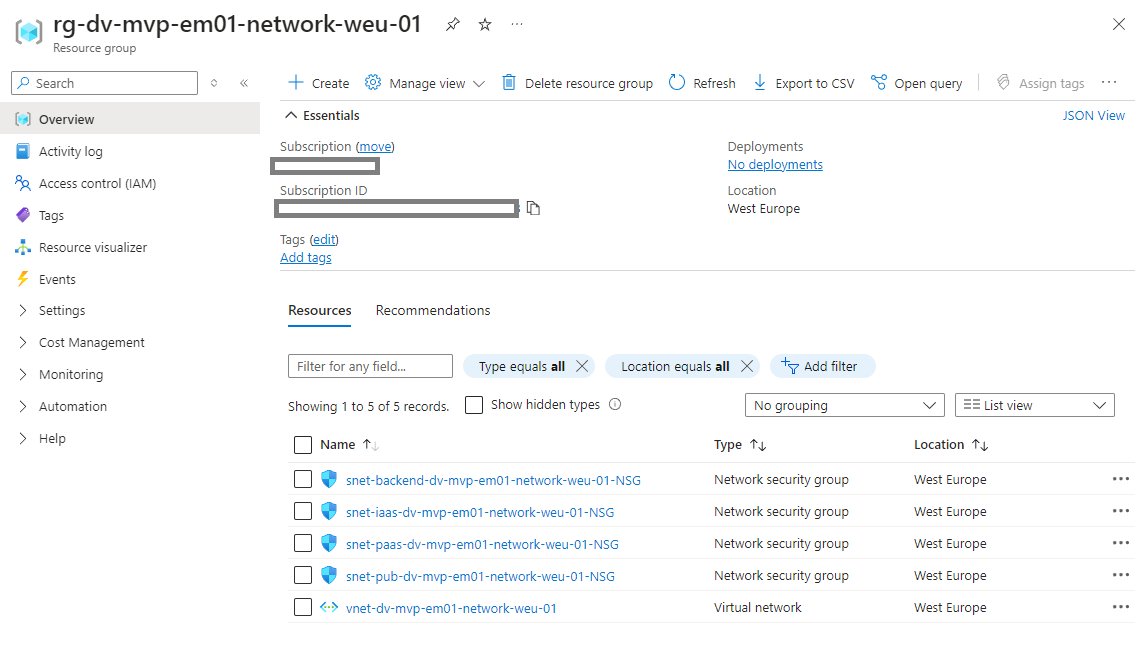
**resource “azurerm\_subnet” “paas\_subnet”:** Tworzy podsieć PaaS (Platform as a Service) z pierwszym adresem z listy local.subnets. Komentarz wskazuje, że ta podsieć wymaga przestrzeni adresowej /23.

**resource “azurerm\_subnet” “backend\_subnet”:** Tworzy backendową podsieć z czwartym adresem z listy local.subnets.

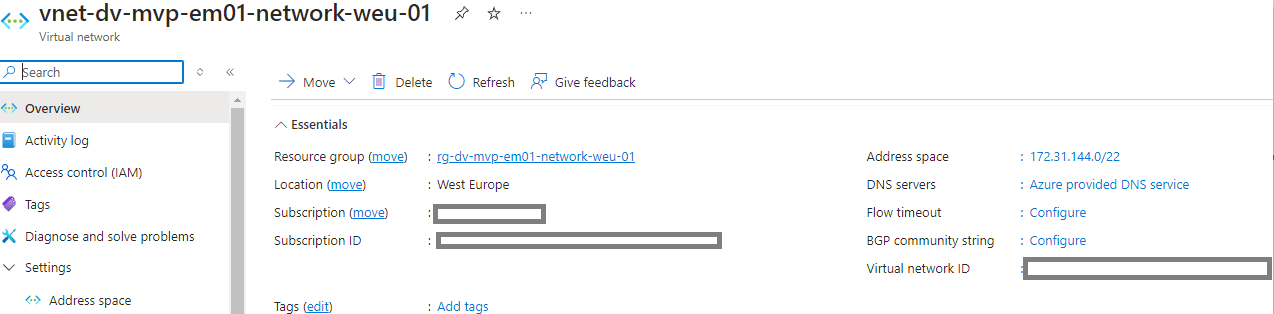
Każda z tych podsieci jest przypisana do tej samej grupy zasobów i wirtualnej sieci, ale ma unikalną przestrzeń adresową. To pozwala na izolację ruchu sieciowego między różnymi typami zasobów w Azure1.



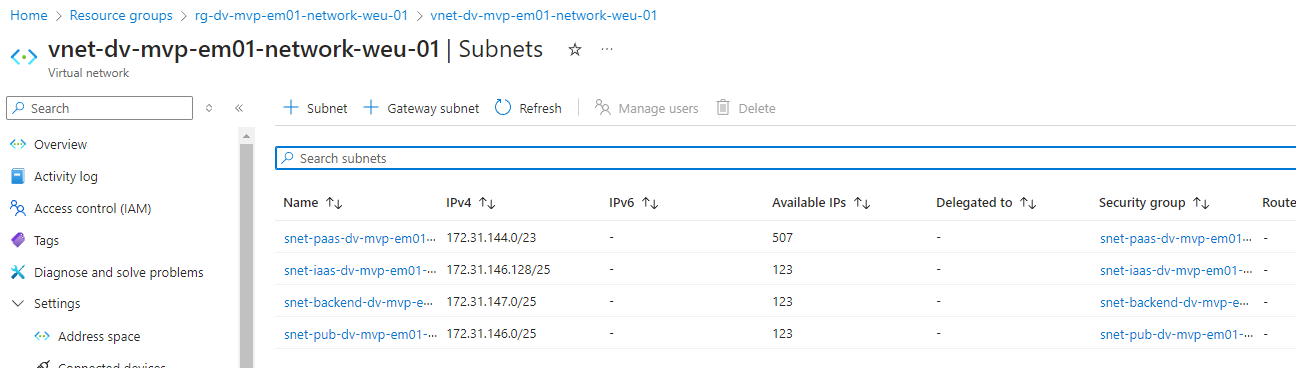
Rysunek 1 Widok modelu samochodu ze specyficznymi zagęszczeniami [1]



Rysunek 1 Widok modelu samochodu ze specyficznymi zagęszczeniami [1]

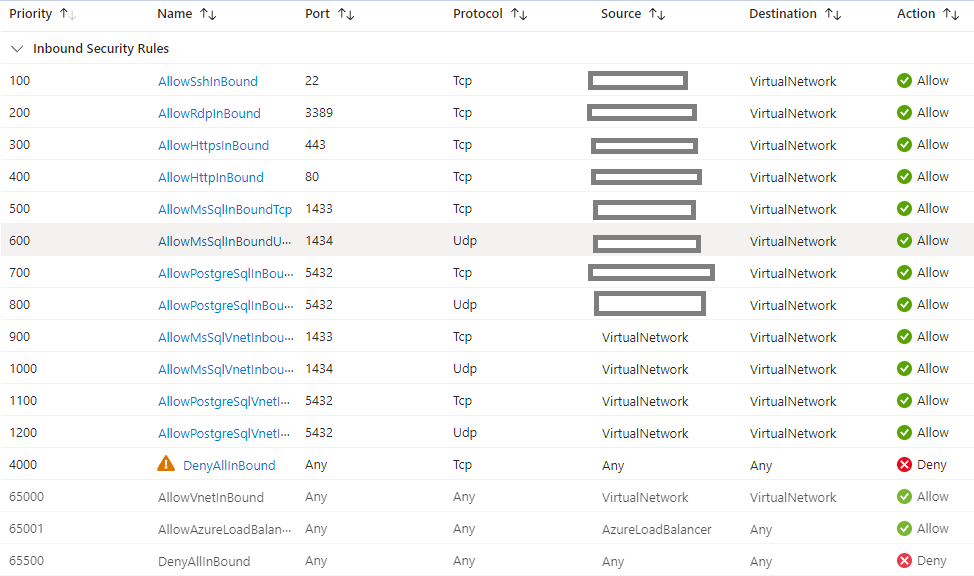


Rysunek 1 Widok modelu samochodu ze specyficznymi zagęszczeniami [1]

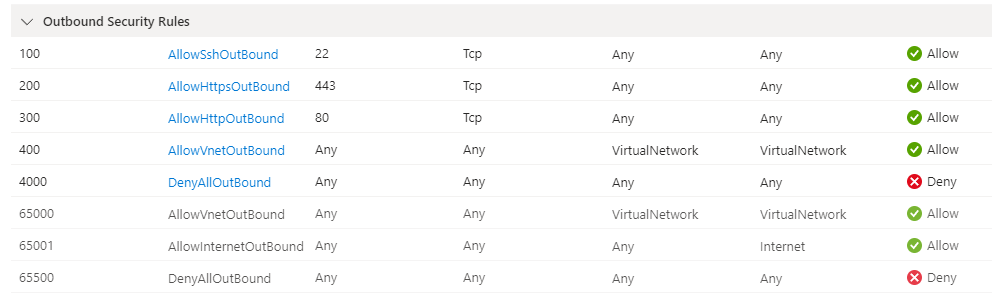


Rysunek 1 Widok modelu samochodu ze specyficznymi zagęszczeniami [1]

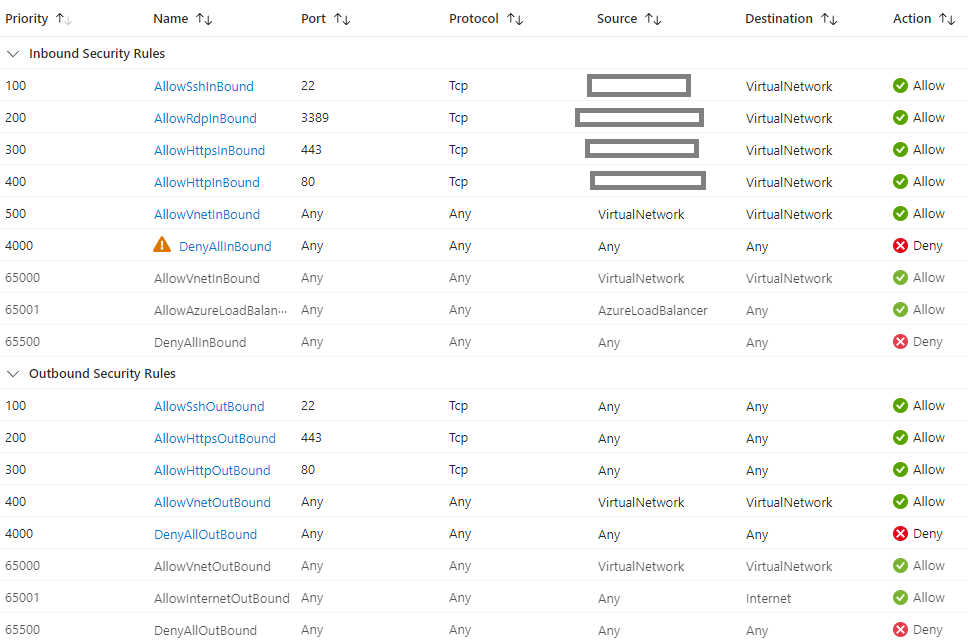
technologii motoryzacyjnych. Jest to nie tylko narzędzie wspierające decyzje podczas wyścigów, ale także duży krok w kierunku postępu w dziedzinie inżynierii samochodowej.



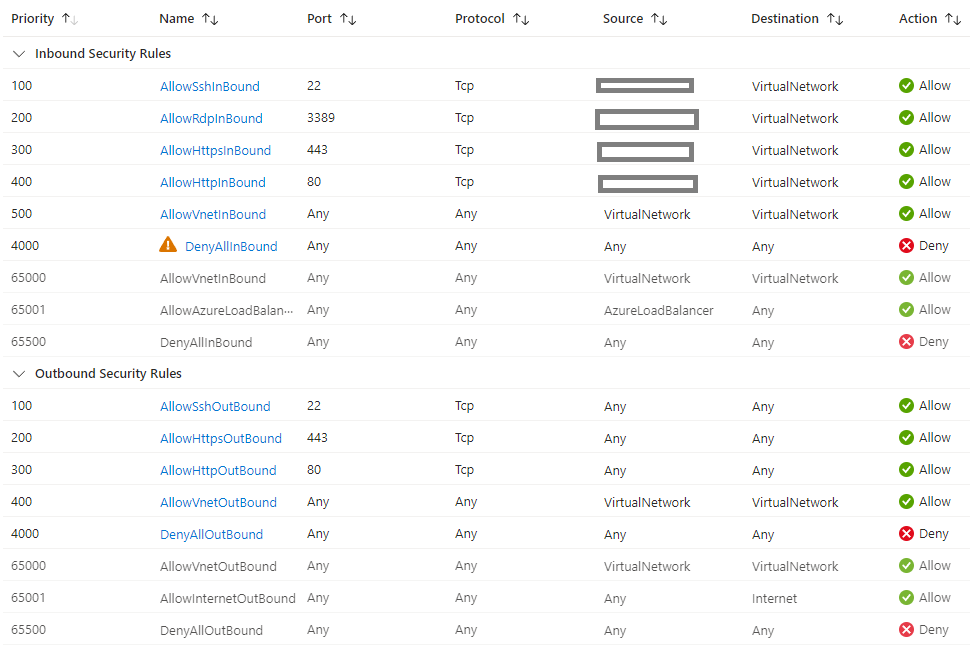
Rysunek 1 backend [1]



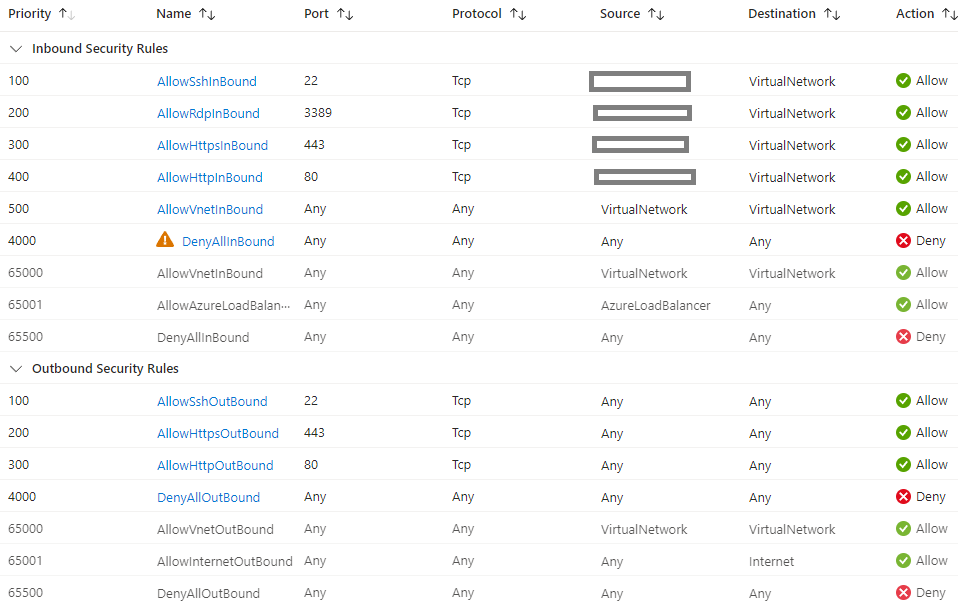
Rysunek 1 backend [1]



Rysunek 1 iaas [1]



Rysunek 1 paas [1]



Rysunek 1 public [1]

1. Wpływ n

Zastosowanierasie. Elastyczność w reagowaniu na zmiany warunków przekłada się na konkurencyjność mediów, sponsorów i kibiców, co dodatkowo podkreśla pozycję lidera w świecie motor sportu. Wpływ symulacji na działalność operacyjną Formuły 1 jest złożony i wieloaspektowy, obejmując różne sfery działalności związane zarówno z przygotowaniami przedwyścigowymi, jak i działaniami podczas samych wyścigów. To narzędzie staje się kluczowym elementem, umożliwiającym skuteczne zarządzanie zmieniającym się i wymagającym środowiskiem wyścigowym.

1. Bibliografia

[1].<https://mesco.com.pl/praktyczne-wskazowki-symulacji-aerodynamiki-zewnetrznej-na-przykladzie-konceptu-bolidu-f1-2022/>

[2]. <https://www.formula1.com/en/toolbar/partners.html>

[3]. <https://www.fia.com/>

[4]. <https://www.mercedesamgf1.com/news/how-does-f1-simulation-work>

[5].<https://www.formula1.com/en/latest/article.formula-why-how-do-f1-simulators-work-and-why-do-teams-need-them.3UjYyfeFMumTpkge6BZrwA.html>

[6]. https://www.catapult.com/blog/formula-1-race-strategy-analysis