Лекція 3-4.

Azure Регіони - 58 регіонів в 140 країнах

Azure global infrastructure experience (microsoft.com)

Постачальник хмарних служб та сервісів мають потужності в різних регіонах для забезпечення вимог щодо місця розташування даних користувачів. Чим ближче розташовані до користувачів хмарні сервіси/дані тим краще. Наприклад, користувачі «хмарних сервісів» з Канада, мають вимоги щоб їх дані знаходились в Канаді.
Azure включає 58 регіонів в 140 країнах.
Регіон – це група «доступних зон» (Availability Zone AZ) в яких знаходяться центри обробки даних.
Azure Availability Zone відноситься до поняття, яке використовується в хмарних сервісах Microsoft Azure для означення ізольованих локацій всередині регіону Azure. Кожна зона складається з одного або кількох дата-центрів, які оснащені незалежною електрикою, охолодженням та мережевою інфраструктурою. Це дозволяє виключити спільні точки відмови та забезпечує високий рівень доступності та надійності сервісів, розміщених в хмарі. Availability Zone застосовуються для реалізації стратегій відновлення після збоїв та забезпечення високої доступності критичних додатків.
Категорії регіонів

1. Рекомендовані регіони –регіони, в яких доступні майже всі сервіси Azure (підтримують 3 доступні зони)
2. Альтернативні – регіони з функціями «аварійного відновлення» (не підтримують різні доступні зони).

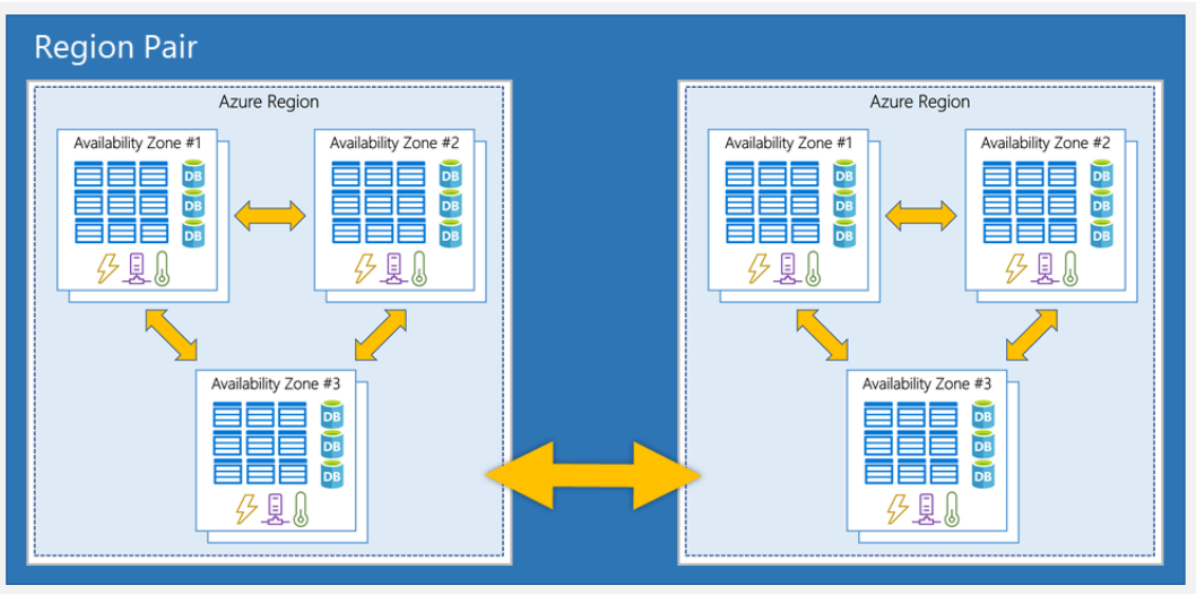
Кожен регіон «дублюється» (дзеркальна копія) іншим регіоном, який знаходиться на відстані 1287.48 км (800 miles). Таким чином, у випадку необхідності аварійного відновленні – використовуються регіон – «дублер».

Region Pairs

- At least 300 miles of separation between region pairs.
- Automatic replication for some services.
- Prioritized region recovery in the event of outage.
- Updates are rollout sequentially to minimize downtime.

Web Link: https://aka.ms/PairedRegions

Region	Region
North Central US	South Central US
East US	West US
West US 2	West Central US
US East 2	Central US
Canada Central	Canada East
North Europe	West Europe
UK West	UK South
Germany Central	Germany Northeast
South East Asia	East Asia
East China	North China
Japan East	Japan West
Australia Southeast	Australia East
India South	India Central
Brazil South (Primary)	South Central US



Azure Sovereign Regions (US Government services)

Meets the security and compliance needs of US federal agencies, state and local governments, and their solution providers.

Azure Government:

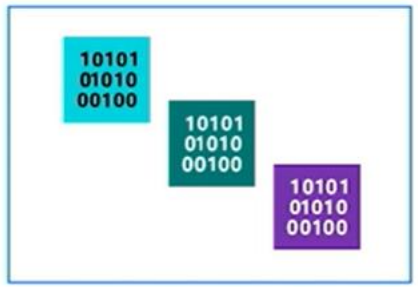
- Separate instance of Azure
- Physically isolated from non-US government deployments
- Accessible only to screened, authorized personnel

Azure Sovereign region - для US Government services, також відомий як Azure Government, - це окремий регіон Microsoft Azure, спеціально розроблений для задоволення вимог урядових організацій Сполучених Штатів. Цей регіон хмарних сервісів має покращені заходи безпеки та відповідність федеральним стандартам, серед яких:

- Фізична та логічна ізоляція даних: Azure Government забезпечує окремі центри даних, що не є доступними для загального хмарного сервісу Azure.
- Операції у Azure Government відповідають таким стандартам як FedRAMP High, CJIS, IRS 1075, DoD L4 (та частково L5) та інші. Це забезпечує високий рівень захисту даних, який вимагають урядові організації.
- Доступ до Azure Government можуть мати тільки американські громадяни, які пройшли перевірку особи, та експлуатація даного хмарного сервісу знаходиться повністю на території США.

Azure Sovereign Regions (Azure China)

Microsoft is China's first foreign public cloud service provider, in compliance with government regulations.

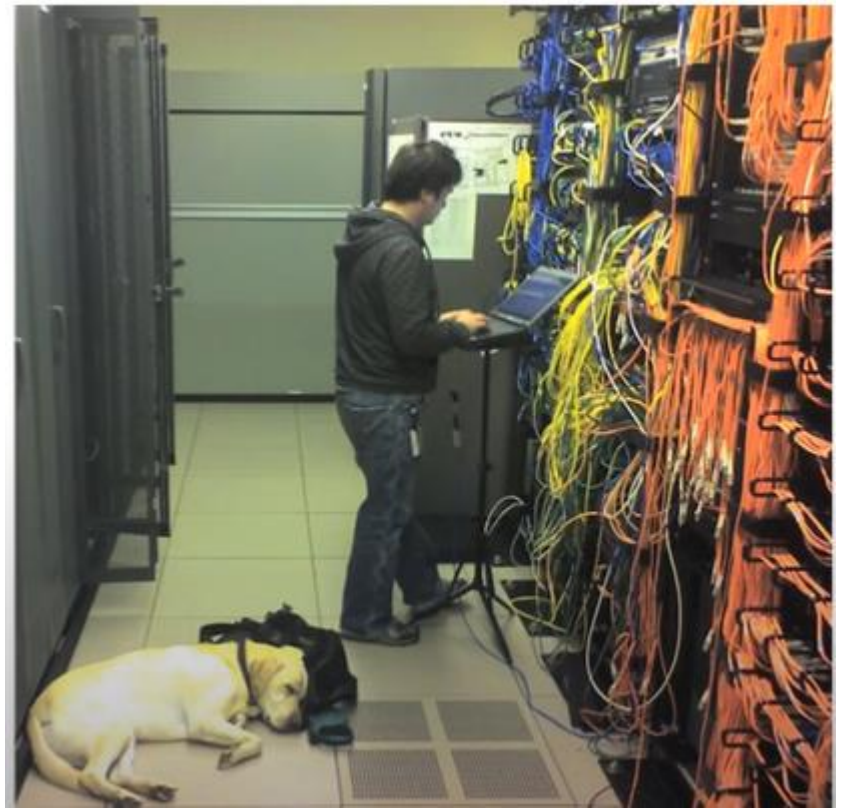


Azure China features:

- Physically separated instance of Azure cloud services operated by 21Vianet
- All data stays within China to ensure compliance

Azure China Region - це спеціальний регіон Microsoft Azure, який відповідає специфічним вимогам Китайських законів про кібербезпеку та захист даних. Цей регіон керується місцевим оператором 21Vianet, який є єдиним повноцінним постачальником сервісів від Microsoft Azure в Китаї. Це забезпечує, що дані зберігаються на території Китаю, що є вимогою місцевого законодавства.

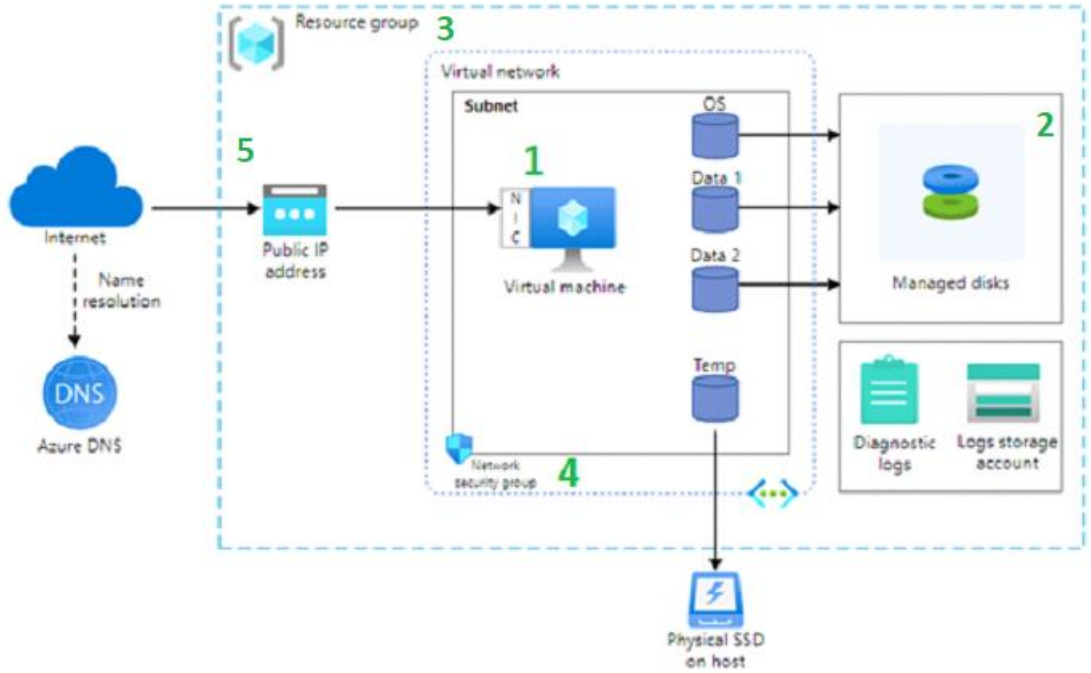
Служби Azure – базові, основні, стратегічні



«Доступна зона» - місце розташування будівлі де знаходяться центри обробки даних – 100 серверів та комп. В рекомендовану регіоні доступні до 3-х «зон».

- *Базові служби:* доступні у всіх рекомендованих та альтернативних регіонах, коли регіон стане загальнодоступним або протягом 90 днів після того, як нова базова служба стане загальнодоступною. Приклад, Azure Backup, Azure Cosmos DB, Azure DNS, Azure ExpressRoute, бази даних Azure, ВМ.
- *Основні служби:* доступні у всіх регіонах, що рекомендуються, протягом 90 днів після загальної доступності регіону. На основі попиту, деякі основі служби можуть бути розгорнуті в альтернативних регіонах. Приклад, Служба керування Azure API, Пакетна служба Azure, База даних Azure для MySQL, База даних Azure для PostgreSQL, Брандмауер Azure, Реєстр контейнерів Azure, Примірники контейнерів Azure, т.п.
- *Стратегічні служби*: Доступність на основі попиту в різних регіонах, приклад База даних Azure для MariaDB, Машинне навчання Azure, Рішення Azure VMware, Azure Analysis Services

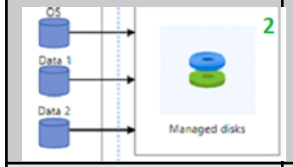
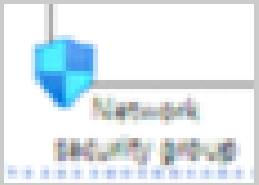
Віртуальні машини Azure



Віртуальна машина (1), віртуальні жорсткі диски (2), Віртуальна мережа (3), групи безпеки мережі (4), загальнодоступна IP-адреса (5)

- Віртуальні машини (ВМ) Azure - це масштабовані хмарні обчислювальні ресурси на вимогу. Вони аналогічні ВМ, розміщеним у Windows Hyper-V. У них є процесор, пам'ять, сховище та мережеві ресурси. ВМ - призначені для полегшення процесу міграції існуючих Windows Server додатків в "хмару" структуру. ***На відміну від перенесення сервісів і окремих компонентів, ВМ дозволяє перенести додаток цілком (lift and shift)***, і бере на себе відповідальність за надання сервісів автоматичного управління, оновлення та відмовостійкості.

Створення віртуальної машини Azure

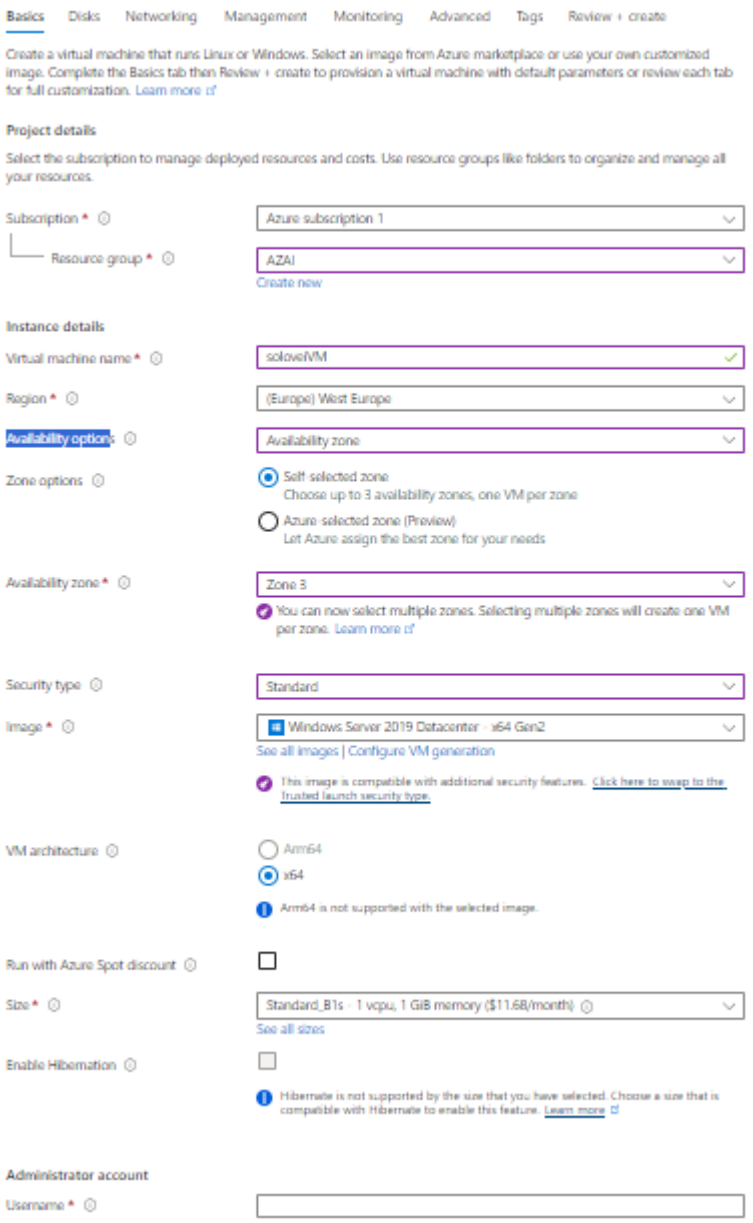
	При створенні ВМ необхідно визначити її регіон; розмір; архітектуру; базову операційну систему (Windows, Linux та інші); вибрати варіанти сховища.
	Вибрати варіант сховища, для зберігання операційної системи, додатків та даних.
	Налаштувати віртуальну мережу для забезпечення ізоляції.
	Налаштувати групи безпеки - основний інструмент, призначений для застосування та контролю правил мережевого трафіку на рівні мережі. Групи безпеки мережі — це додатковий рівень безпеки, який виступає як програмний брандмауер, який фільтрує вхідний та вихідний трафік у віртуальній мережі.

Розміри ВМ

- Розміри віртуальних машин згруповані за категоріями, починаючи із серії B для найпростішого тестування та закінчуючи серією H для складних обчислювальних завдань.
- Розмір віртуальної машини слід вибирати відповідно до необхідного робочого навантаження.
- Розмір віртуальної машини можна змінити після створення, але для цього необхідно спочатку завершити її роботу, тому краще відразу вибрати правильний розмір, якщо це можливо.

Задачі	Можливий розмір
Загальне використання обчислень або веб-сайтів: тестування та розробка, невеликі та середні бази даних або веб-сервери з низьким та середнім трафіком.	B, Dsv3, Dv3, DSv2, Dv2
Складні обчислювальні завдання: веб-сервери із середнім трафіком, мережні пристрої, пакетні процеси та сервери програм.	Fsv2 Fs, F
Використання великого обсягу пам'яті. Сервери реляційних баз даних, кеші середнього та великого обсягу, а також аналітика, що виконується в пам'яті.	Esv3, Ev3, M, GS, G, DSv2, Dv2
Зберігання та обробка даних: бази даних SQL та NoSQL, яким потрібна висока пропускна спроможність диска та операції вводу-виводу.	Ls
Ресурсоємне малювання зображень або редагування відео, а також навчання моделей та формування висновків за допомогою глибокого навчання	NV, NC, NCv2, NCv3 та ND
Високопродуктивні обчислення (HPC): якщо вам потрібні найшвидші та найпотужніші віртуальні машини ЦП з додатковими мережевими інтерфейсами з високою пропускною здатністю	H

ВМ – ***основні*** налаштування



Група, ім'я, Регіон

- Availability options – опція для управління рівнем доступності ВМ.

1) Availability zone – надається фізично відокремлена зона в межах регіону. Доступні 3 зони, кожна зона має окреме джерело живлення, мережу та охолодження.
2) VM Scale sets – дозволяє створювати групи ВМ із збалансованим навантаженням.

3) Availability sets – дозволяє групувати ВМ для забезпечення збалансованого навантаження.

Рекомендовано створювати завжди 2 ВМ

- Security type – тип безпеки, за замовчення визначено Trusted Launch VM – забезпечую захист від атак. Основою TL є Secure Boot – для всіх компонентів ВМ запитує сертифікат видавця, у разі не отримання – зупиняє інсталяцію ВМ.

2) Confidential VM - забезпечує додатковий захист на рівні обладнання.

- Image – дозволяє вибрати операційну систему
- Size - обчислювальна потужність, пам’ять і ємність зберігання.
- Administrator account – username/user password для ВМ.
- Public inbound ports – визначає порти ВМ, які доступні з Інтернету.

ВМ – ***основні*** налаштування

OS disk size - розмір диску в ГБ
OS disk type - Доступні варіанти включають жорсткі диски (HDD) або сучасні твердотільні накопичувачі (SSD).
За умовчанням для віртуальної машини Windows створюються два віртуальні жорсткі диски:
Диск операційної системи. Це основний диск або C, максимальна ємність якого становить 2048 ГБ.
Тимчасовий диск. Він призначений для тимчасового зберігання ОС чи додатків. Він має букву D: за замовчуванням, а його розмір залежить від розміру віртуальної машини, тому це ідеальне розташування для файлу підкачки Windows.

	Ultra Disk	Premium SSD v2	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	SSD	HDD
Рекомендовано для умов:	інтенсивні навантаження вводу виводу. Важкі транзакції.	низької затримки та високої пропускної здатності	Навантаження з високою продуктивністю	Веб - сервери	підтримка резервного копіювання
Max disk size	65,536 GiB	65,536 GiB	32,767 GiB	32,767 GiB	32,767 GiB

Key management – визначити набір ключів шифрування диска. За замовченням - Platform-managed keys – ключі шифрування керовані платформою.
Customer-managed keys - шифрування диску на основі власних ключів.

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

The configuration of this virtual machine and its attached disk(s) does not allow for the disk(s) to utilize their full throughput performance. The current virtual machine size supports 23 MBps. The total for disk(s) attached to virtual machine 'soloveiVM' is 100 MBps. You can change the virtual machine size to support additional disk(s) throughput. Learn more

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ☐

Encryption at host is not registered for the selected subscription.
Learn more about enabling this feature

OS disk

OS disk size: Image default (127 GiB)

OS disk type *: Standard SSD (locally-redundant storage)

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Delete with VM ☑

Key management: Platform-managed key

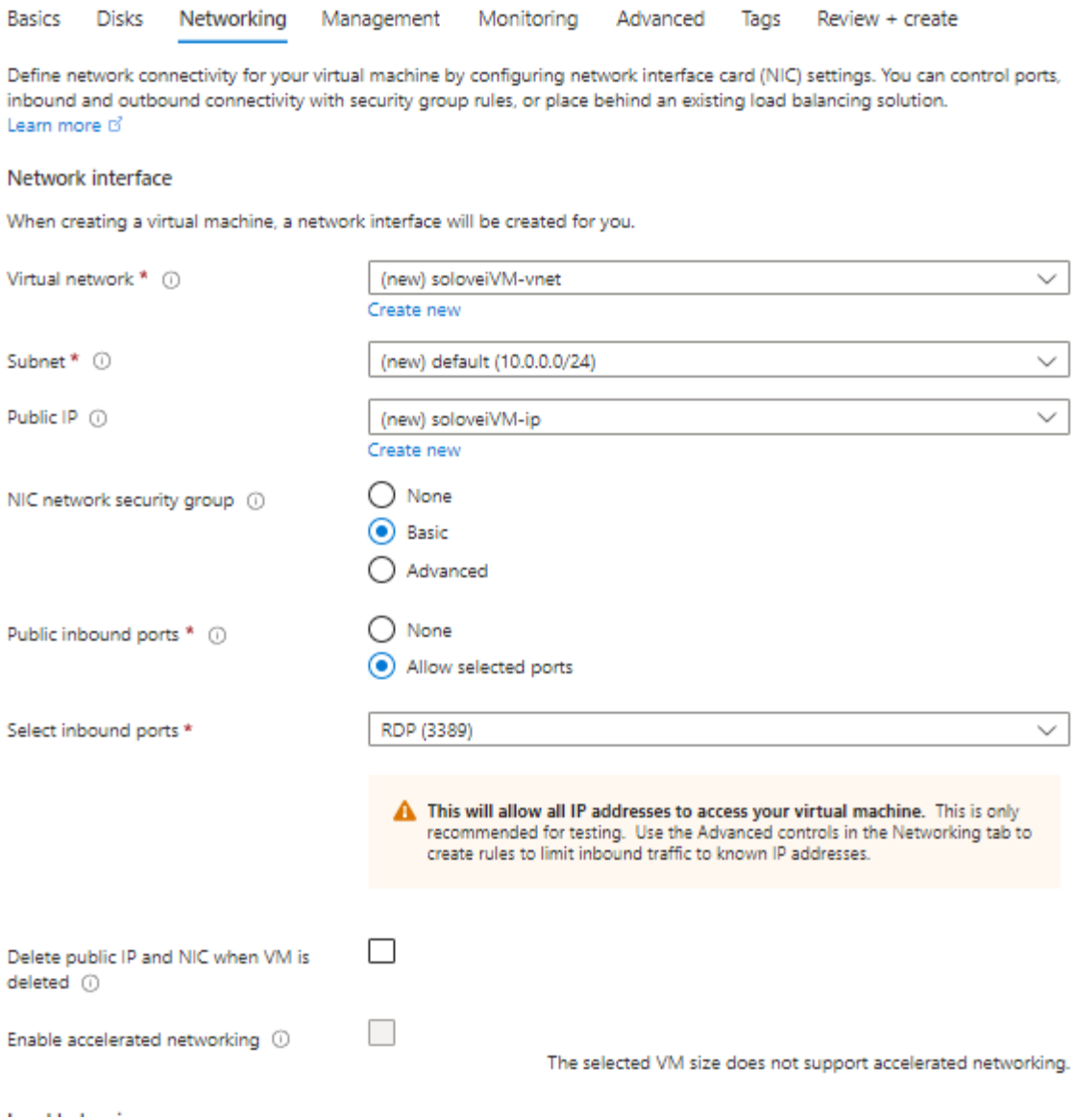
Enable Ultra Disk compatibility ☐

Data disks for soloveiVM

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM

Віртуальна мережа (Virtual network)



Віртуальна мережа Azure — це служба, яка дозволяє багатьом типам ресурсів Azure (в тому числі віртуальній машині) безпечно взаємодіяти з іншими, Інтернетом і локальними сетями.

Основні сценарії, які можна виконати за допомогою віртуальної мережі.

- Обмін даних через Інтернет – можливо за допомогою Public IP.
- Взаємодія з локальними ресурсами - – за протоколами Point-to-site virtual private network (VPN), Site-to-site VPN, Azure ExpressRoute
- Фільтрація мережевого трафіку – через створення груп безпеки. Група безпеки мережі містить правила безпеки, які дозволяють або забороняють вхідний мережевий трафік до віртуальної машини або вихідний мережевий трафік від віртуальної машини. рекомендується пов’язувати групу безпеки мережі з окремими підмережами (Subnet), а не з окремими мережевими інтерфейсами в підмережі, коли це можливо.
- Маршрутизация сетевого трафика.

Віртуальна мережа – Мережа основні налаштування

- Virtual networks - віртуальні мережі логічно ізольовані одна від одної. Для їх налаштувати необхідно визначити діапазони IP-адрес, підмережі, таблиці маршрутів, шлюзи та параметри безпеки
- Subnet - це діапазон IP-адрес у вашій віртуальній мережі, який можна використовувати для ізоляції віртуальних машин одна від одної.
- Network Interface (NIC) network security group - складається з правил, які забороняють чи дозволяють вхідний мережевий трафік до ВМ або вихідний мережевий трафік від ВМ.
- Public inbound ports - За замовчуванням доступ до віртуальної машини обмежено. Якщо вибрати "Allow selected ports" - тоді вхідний трафік стане можливим.
- Load balancing - механізм балансування навантажень для ВМ, які включені в поол.

Загальнодоступні та приватні IP-адреси

- Загальнодоступні та приватні IP-адреси використовуються в Azure для обміну даними між ресурсами. Обмін даними між ресурсами може відбуватися у приватній віртуальній мережі Azure та в загальнодоступний Інтернет.
- Префікси загальнодоступної IP-адреси — це резервовані діапазони IP-адрес в Azure. Префікси загальнодоступних IP-адрес складаються з адрес IPv4 і
- IPv6.
- Доступні такі розміри префіксів загальнодоступних IP-адрес:
- /28 (IPv4) або /124 (IPv6) = 16 адрес
- /29 (IPv4) або /125 (IPv6) = 8 адрес
- /30 (IPv4) або /126 (IPv6) = 4 адреси
- /31 (IPv4) або /127 (IPv6) = 2 адреси
- Розмір префікса визначається як розмір маски безкласової міждоменної.
- маршрутизації (CIDR).

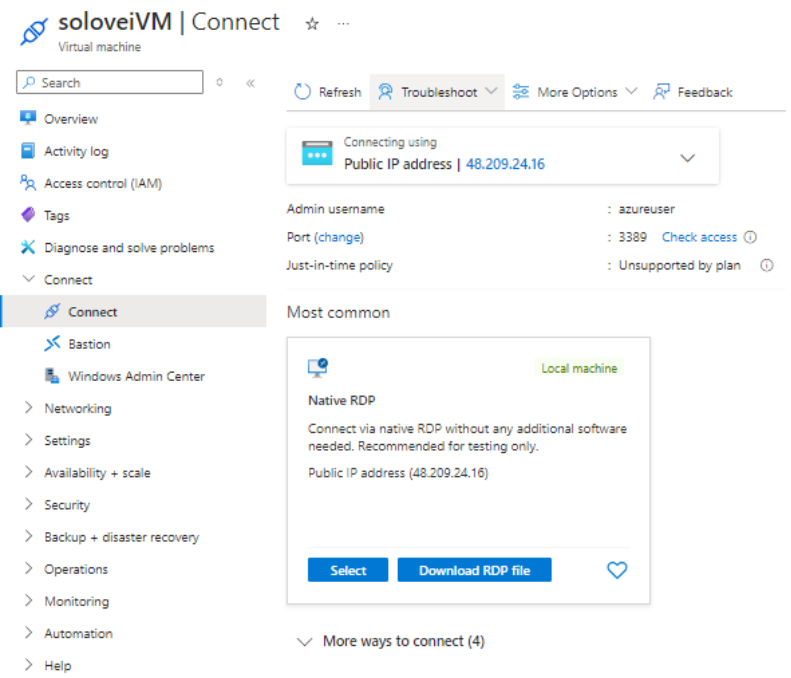
Пріоритети правил

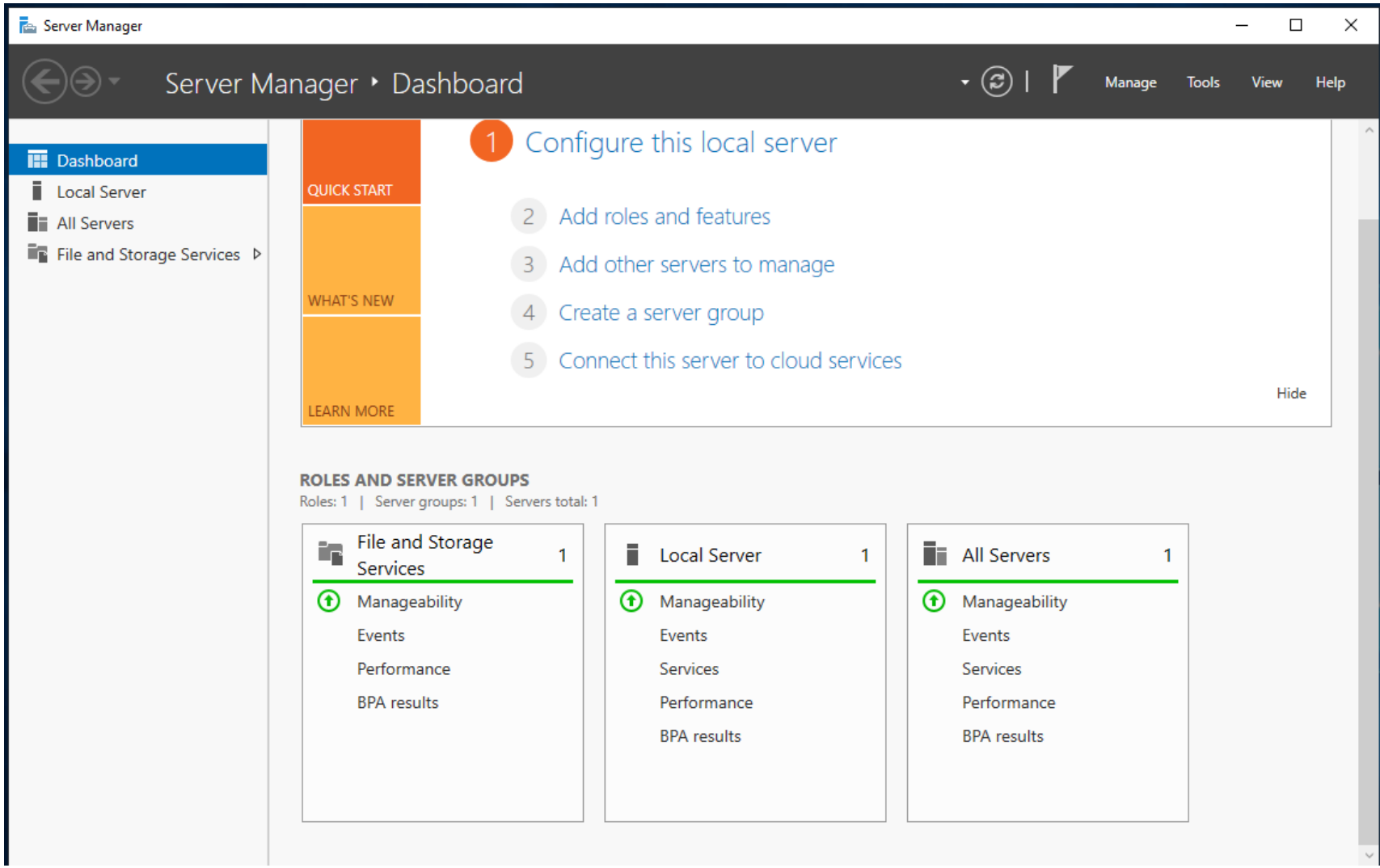
- Правила оцінюються в порядку пріоритету, починаючи з найнижчого пріоритетного правила. Забороняюче правило завжди зупиняє оцінку. Наприклад, якщо вихідний запит заблоковано правилом інтерфейсу мережі, правила для підмережі не перевіряються. Щоб проходження трафіку через групу безпеки було дозволено, він повинен проходити через усі застосовні групи.
- ***Останнє правило - це завжди правило Заборонити все. Це правило за умовчанням, додане до кожної групи безпеки для вхідного та вихідного трафіку з пріоритетом 65500***

Підключення до ВМ Azure

- Після створення ВМ – до неї необхідно підключитись. Існує кілька варіантів вибору.
  - Протокол віддаленого робочого столу (RDP)
  - Користувальницькі скрипти;
  - Користувальницькі образи віртуальних машин (з встановленим програмним забезпеченням).
- Протокол віддаленого робочого стола (RDP) забезпечує віддалене підключення до інтерфейсу користувача комп'ютерів Windows. RDP дозволяє увійти на віддалений фізичний або віртуальний комп'ютер Windows і керувати цим комп'ютером.
- Для підключення протоколу RDP потрібен клієнт RDP. Корпорація Майкрософт надає клієнтам RDP такі операційні системи:
  - Windows (вбудований);
  - macOS;
  - iOS
  - Android.
- Щоб підключитися до віртуальної машини Azure за допомогою клієнта RDP, вам знадобиться:
  - загальнодоступна IP-адреса віртуальної машини (або приватна адреса, якщо налаштовано підключення віртуальної машини до вашої мережі);
  - Номер порту
- Ви можете ввести ці відомості в клієнт RDP або завантажити попередньо налаштований файл RDP.
- Файл RDP - це текстовий файл, який містить набір пар "ім'я-значення", які визначають параметри з'єднання для клієнта RDP для підключення до віддаленого комп'ютера за допомогою протоколу віддаленого робочого столу.

Для підключення до *створеної* ВМ необхідно отримати RDP file. При вдалому підключенні ви зможете відкрити Server Manager, який треба налаштувати





Web-Internet Information Services (IIS) — це веб-сервер від компанії Microsoft, який входить до складу операційних систем Windows. IIS забезпечує платформу для розміщення та управління веб-сайтами, веб-додатками та послугами.

Основні компоненти IIS:
Веб-сервер: Основна функція IIS — це обробка запитів HTTP і HTTPS. Веб-сервер приймає запити від клієнтів (наприклад, веб-браузерів) і повертає відповідний контент, такий як HTML-сторінки, зображення або інші дані.

FTP-сервер: IIS може також функціонувати як FTP-сервер, забезпечуючи передачу файлів через протокол FTP.

Служби безпеки: IIS підтримує різні методи автентифікації та авторизації для захисту ресурсів веб-сайту. Це включає Windows-аутентифікацію, базову автентифікацію, сертифікати SSL/TLS для захищеного з'єднання тощо.

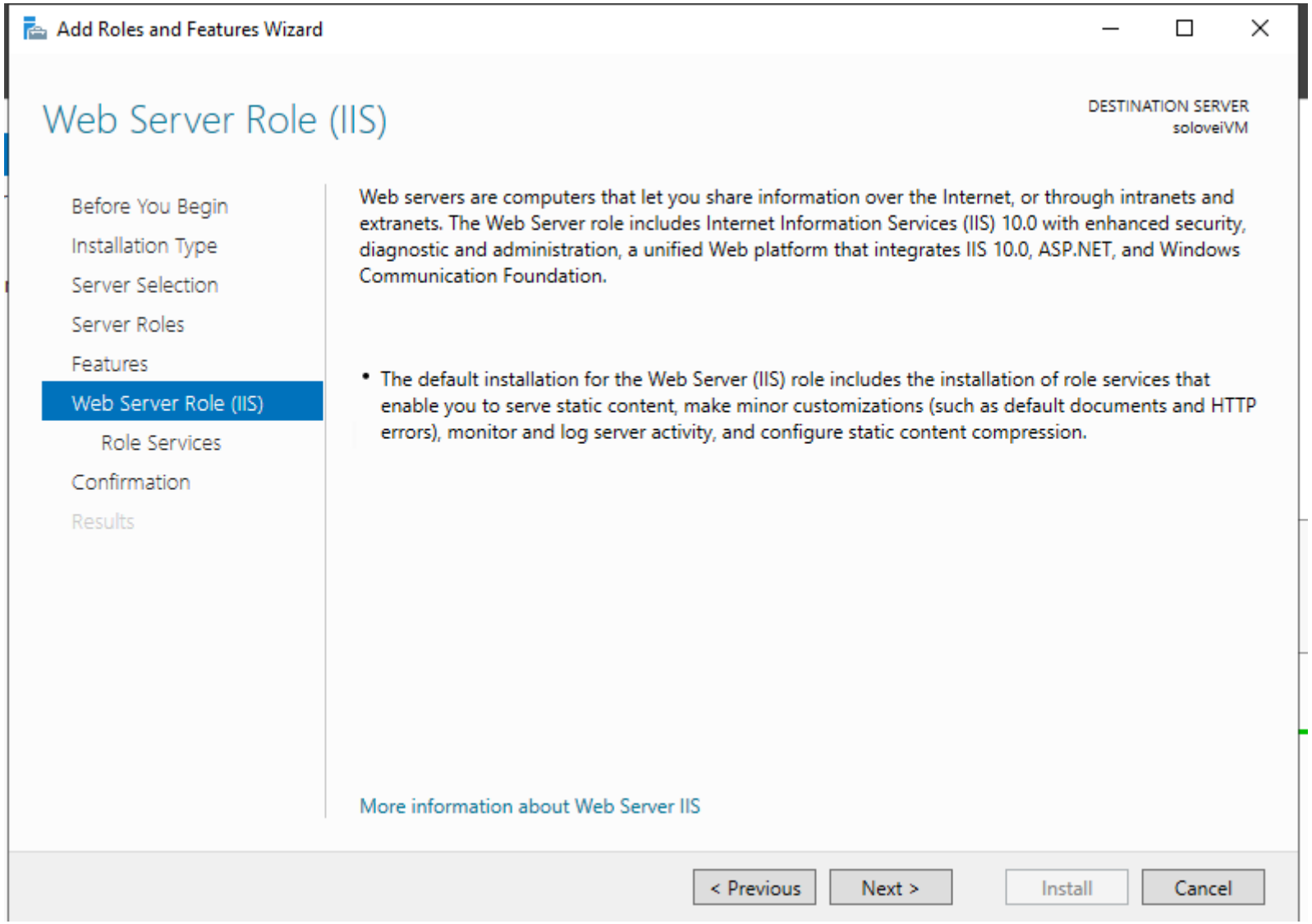
Розширюваність: IIS підтримує модулі, які дозволяють розширювати функціональні можливості сервера. Наприклад, це можуть бути модулі для обробки запитів ASP.NET, PHP, CGI, і інші.

Управління сайтами: IIS надає інтерфейс для управління веб-сайтами та додатками, де можна створювати нові сайти, налаштовувати зони видимості, обмеження доступу, налаштовувати обробку помилок і так далі.

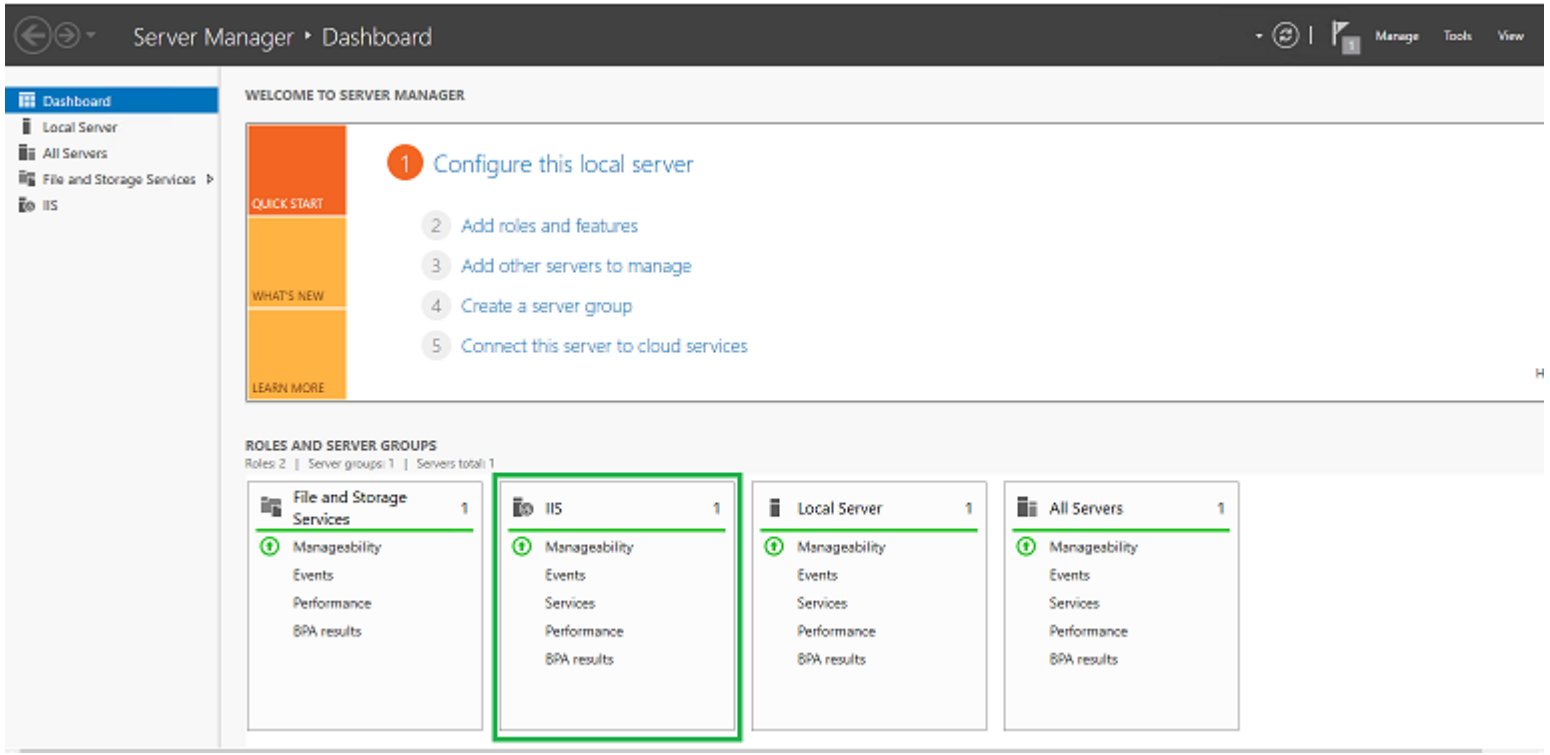
Логи та моніторинг: IIS надає інструменти для ведення логів і моніторингу активності на сервері. Це дозволяє адміністраторам відстежувати доступ до ресурсів, виявляти та усувати можливі проблеми.

Налаштування Web-Internet Information Services (IIS) на ВМ

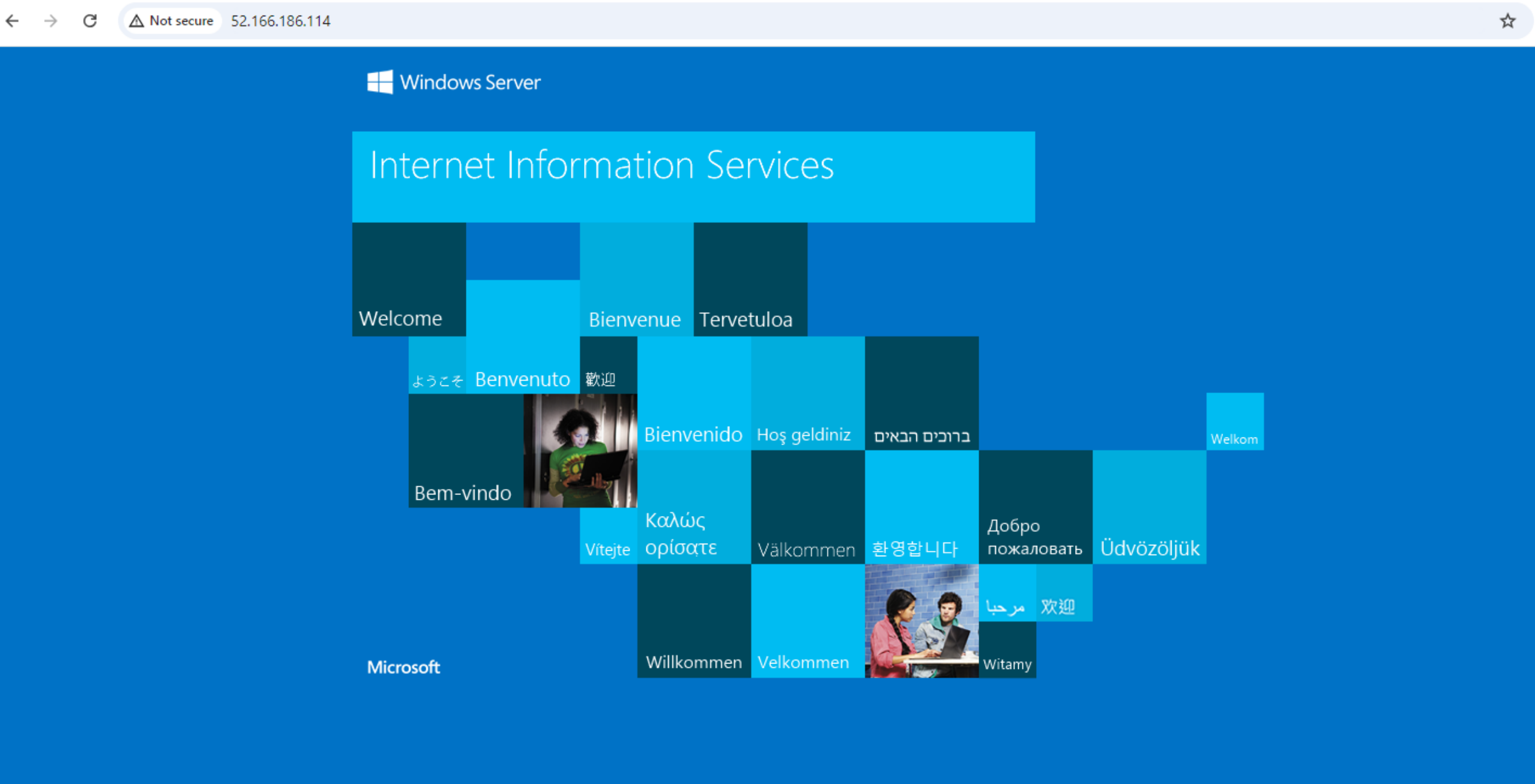
Server Manager/Add Roles and Features/Web Server Role



Після вдалого розгортання серверу, його буде додано до списку серверів.



Відкриємо Default Web site page



Відкриття портів у віртуальних машинах Azure

Нові віртуальні машини заблоковано за замовчуванням.

Програми можуть виконувати вихідні запити, але дозволено лише вхідний трафік із віртуальної мережі (наприклад, інші ресурси у тій самій локальній мережі) та Azure Load Balancer (перевірка проб).

Щоб налаштувати конфігурацію для підтримки FTP, потрібно виконати два кроки.

При створенні віртуальної машини можна відкрити кілька поширених портів (RDP, HTTP, HTTPS і SSH). Проте, якщо потрібно внести інші зміни до брандмауера, необхідно внести їх самостійно.

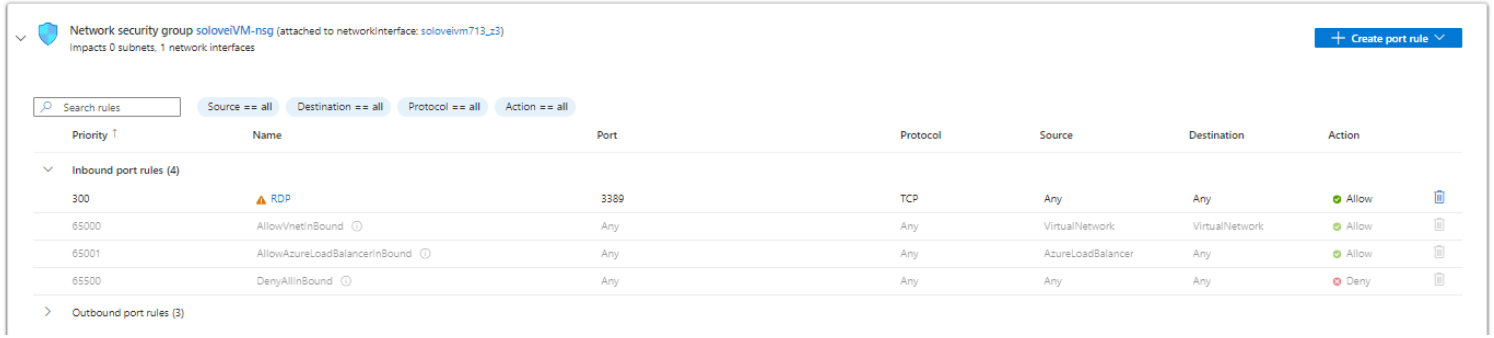
Ця процедура складається з двох етапів:

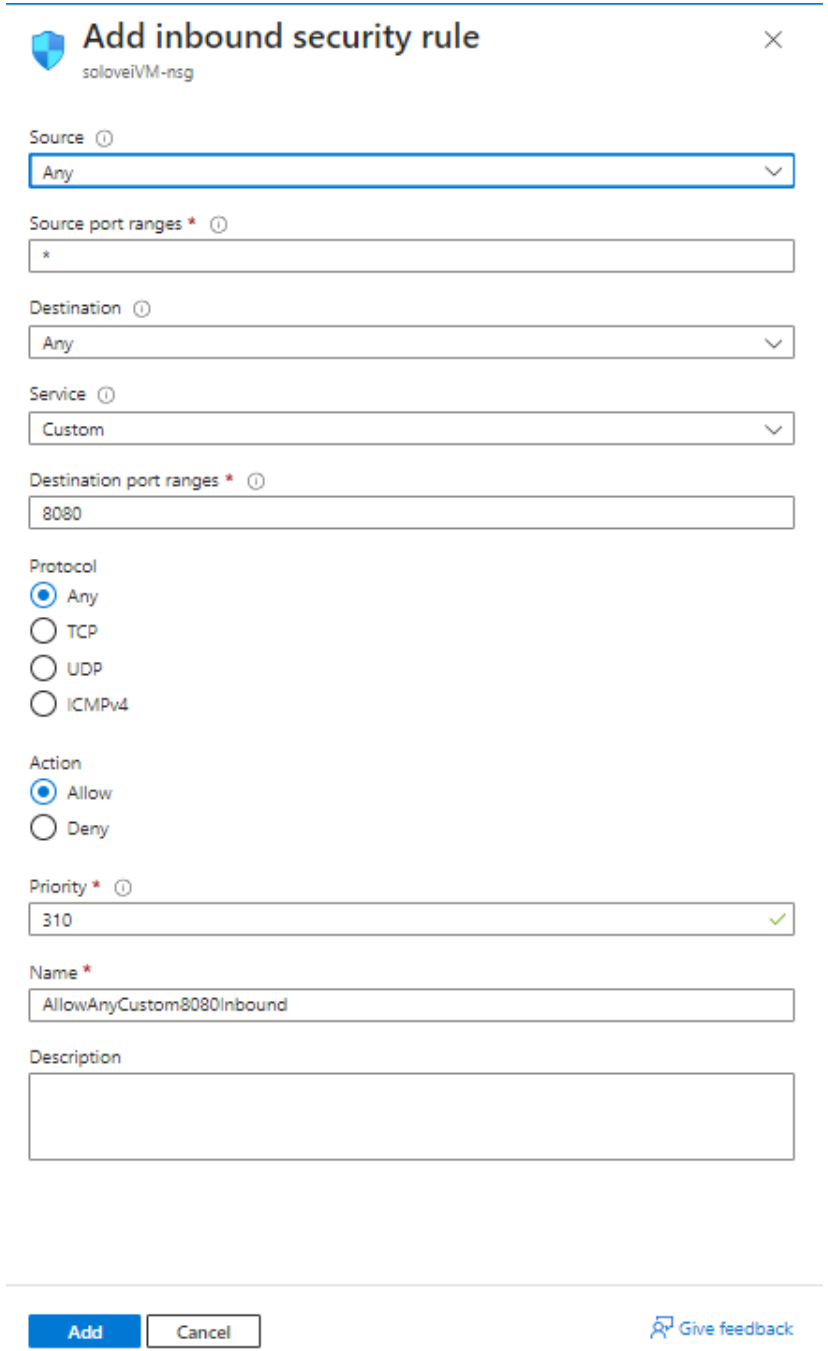
- ✓ Створіть групу безпеки мережі.
- ✓ Створіть правило вхідного трафіку, яке дозволяє трафік через порт 20 та 21 для активної підтримки FTP.

Відкриємо Default Web site page

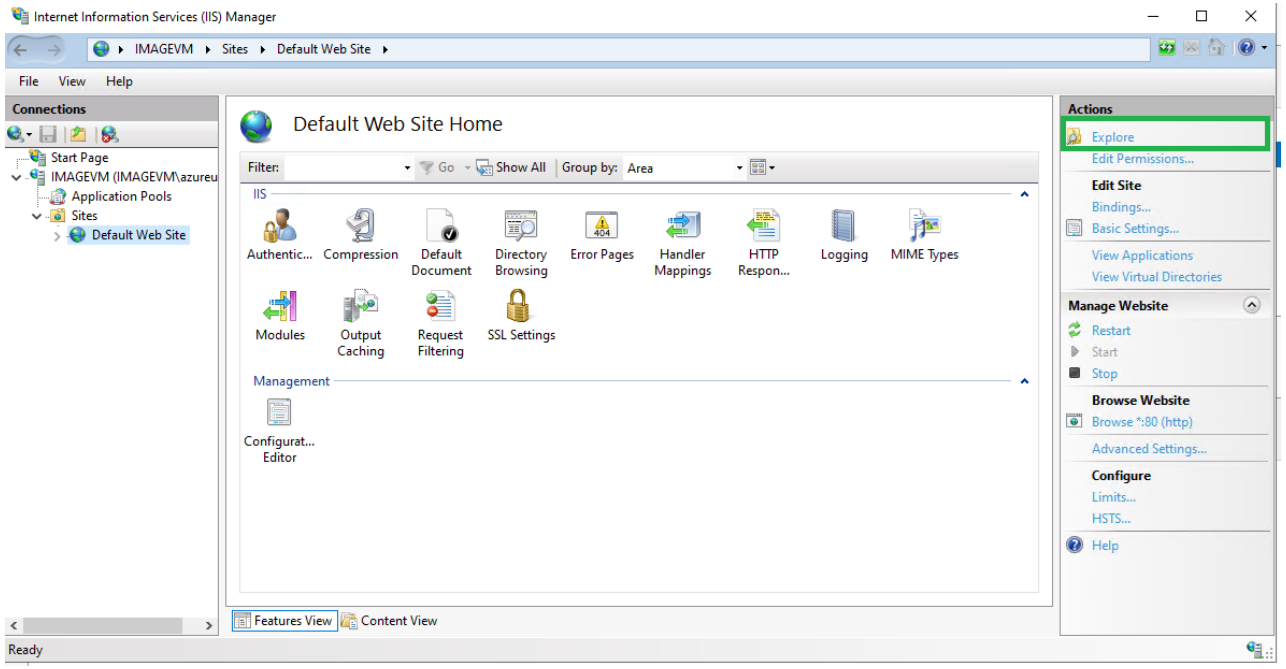
Для *створеної* ВМ група безпеки закриває всі порти.

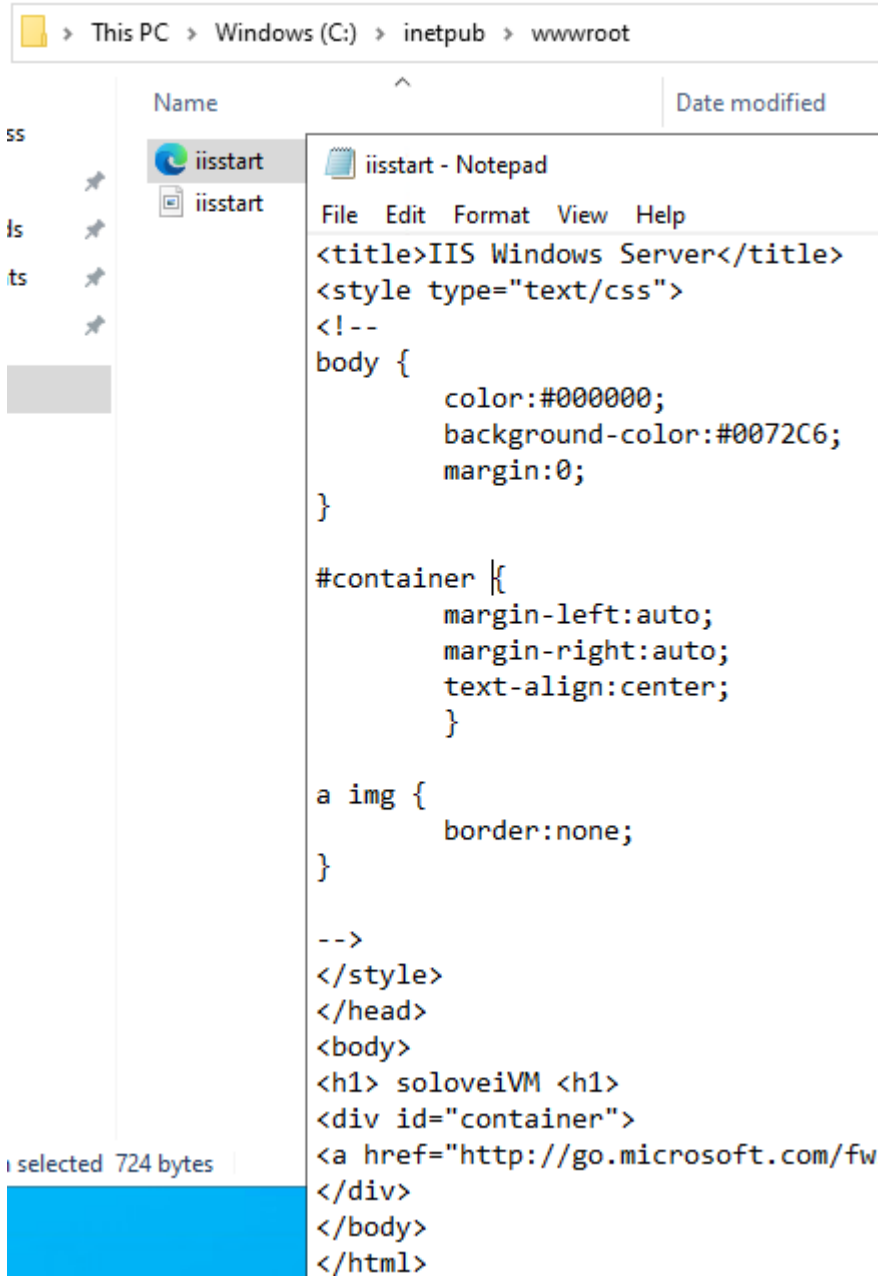
Для отримання трафіку – відкриємо порти – 8080.





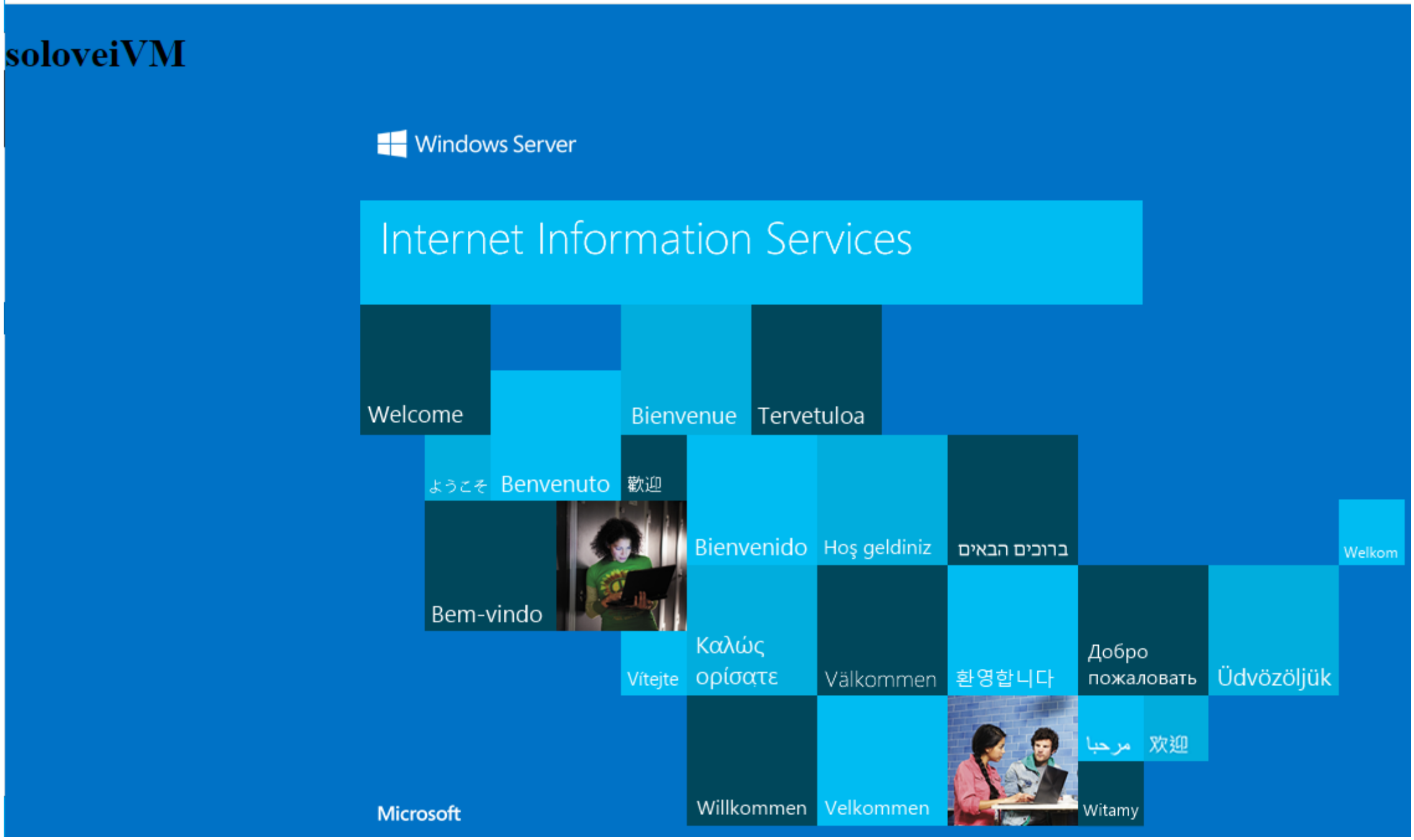
Додамо ім'я ВМ на default web site home page виконаємо кроки – IIS Manager, Explore.





Not secure 52.166.186.114

soloveiVM



Лабораторна робота №2

Azure Cloud Shell – Azure CLI

Azure Cloud Shell - це браузерна оболонка, призначена для розробки та адміністрування ресурсів Azure. Azure CLI використовується для створення ресурсів Azure та керування ними з командного рядка або за допомогою скриптів.

Оскільки Cloud Shell створена для інтерактивних сеансів, оболонки автоматично завершують роботу після 20 хвилин бездіяльності.

Azure Cloud Shell виконується в Azure Linux, дистрибутиві Linux корпорації Майкрософт для продуктів та служб на межі хмарної інфраструктури.

Корпорація Майкрософт внутрішньо компілює всі пакети, що входять до репозиторій Azure Linux, щоб захиститися від атак ланцюжка поставок.

Azure Cloud Shell дозволяє створити та розгорнути ВМ за допомогою низки команд.

Azure Cloud Shell – команди для створення ВМ

1. Робота починається зі створення групи ресурсів за допомогою команди ***az group create***.

```
resourcegroup="myResourceGroupCLI"
location="westus3"
az group create --name $resourcegroup --location $location
```

У прикладі створюється група ресурсів з ім'ям myResourceGroup в розташуванні "Західна частина США 3".

1. Командою az vm create – створюється ВМ.

```
vmname="myVM"
username="azureuser"
az vm create \
    --resource-group $resourcegroup \
    --name $vmname \
    --image Win2022AzureEditionCore \
    --public-ip-sku Standard \
    --admin-username $username
```

У прикладі створюємо ВМ з ім’ям myVM та ім'ям адміністратора – azureuser. Якщо ВМ - ну створено, то про це з’явиться повідомлення та publicIpAddress.

Створення ВМ – cloud shell

```
$grp="VMdemo"
$location="westeurope"
$vnetName="VNET"
$subnetName="SUBNET_1"
$vmName="Demo_VM1"
$vmName="Demo_VM2"
$avset ="AVSET"

# CREATE RESOURCE GROUP
az group create --name $grp --location $location

# CREATE VIRTUAL NETWORK
az network vnet create --address-prefixes 10.0.0.0/16 --name $vnetName --resource-group $grp

# CREATING SUBNET
az network vnet subnet create -g $grp --vnet-name $vnetName -n $subnetName --address-
prefixes 10.0.0.0/24

# CREATING VMs
az vm create --resource-group $grp --name $vmName --vnet-name $vnetName --subnet
$subnetName --admin-username azureuser --admin-password Hello@12345#

#open ports
az vm open-port --port 80 --resource-group $grp --name $vmName

#install web server IIS
az vm run-command invoke -g $grp -n $vmName --command-id RunPowerShellScript --scripts
"Install-WindowsFeature -name Web-Server -IncludeManagementTools"

#az group delete --name $grp
```

Azure Marketplace містить багато образів, які можна використовувати для створення віртуальних машин. На попередніх кроках віртуальна машина створювалася за допомогою Windows Server 2016 Datacenter. На цьому кроці модуль PowerShell використовується для пошуку інших образів Windows на сайті Marketplace, які можна використовувати для створення віртуальних машин. Цей процес полягає в пошуку відомостей про видавця, пропозицію, номер SKU та (необов'язково) номер версії для ідентифікації образу.
Get-AzVMImagePublisher -Location "westeurope"

Список пропозицій образів, використовуючи команду Get-AzVMImageOffer. Ця команда повертає список, відфільтрований за вказаним видавцем Microsoft Windows Server.

```
Get-AzVMImageOffer `
   -Location "westeurope" `
   -PublisherName "MicrosoftWindowsServer"
```

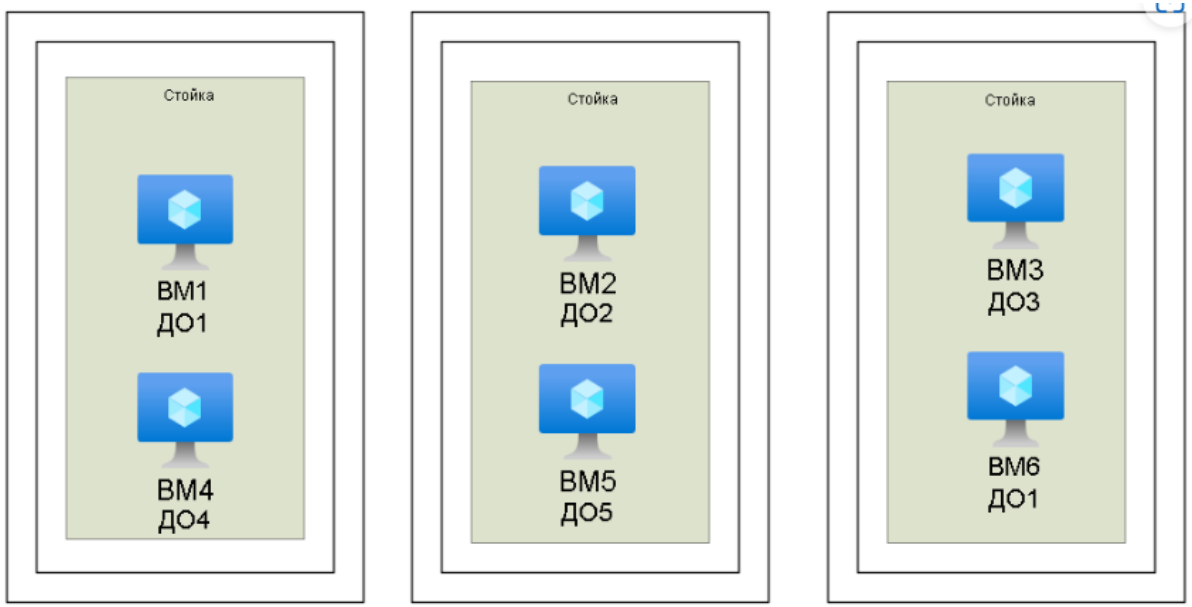
Команда Get-AzVMImageSku відфільтрує список на ім'я видавця та назву пропозиції, відобразивши список імен образів.

```
Get-AzVMImageSku -Location "westeurope" -PublisherName "MicrosoftWindowsServer" -Offer "WindowsServer"
```

Ці відомості можна використовувати для розгортання віртуальної машини з урахуванням конкретного образу

```
az vm create --resource-group VMdemo --name MyVM --image Win2019Datacenter --admin-username azureuser --admin-password
Hello@12345# --size Standard_DS1_v2

$grp = "VMdemo"
$vmname = "MyVM“

#open ports
az vm open-port --port 80 --resource-group $grp --name $vmName

az vm run-command invoke -g $grp -n $vmName --command-id RunPowerShellScript --scripts "Install-WindowsFeature -name Web-Server -
IncludeManagementTools“
```

Azure *«Availability sets»* **- *«домени збою» і «домени оновлення»***

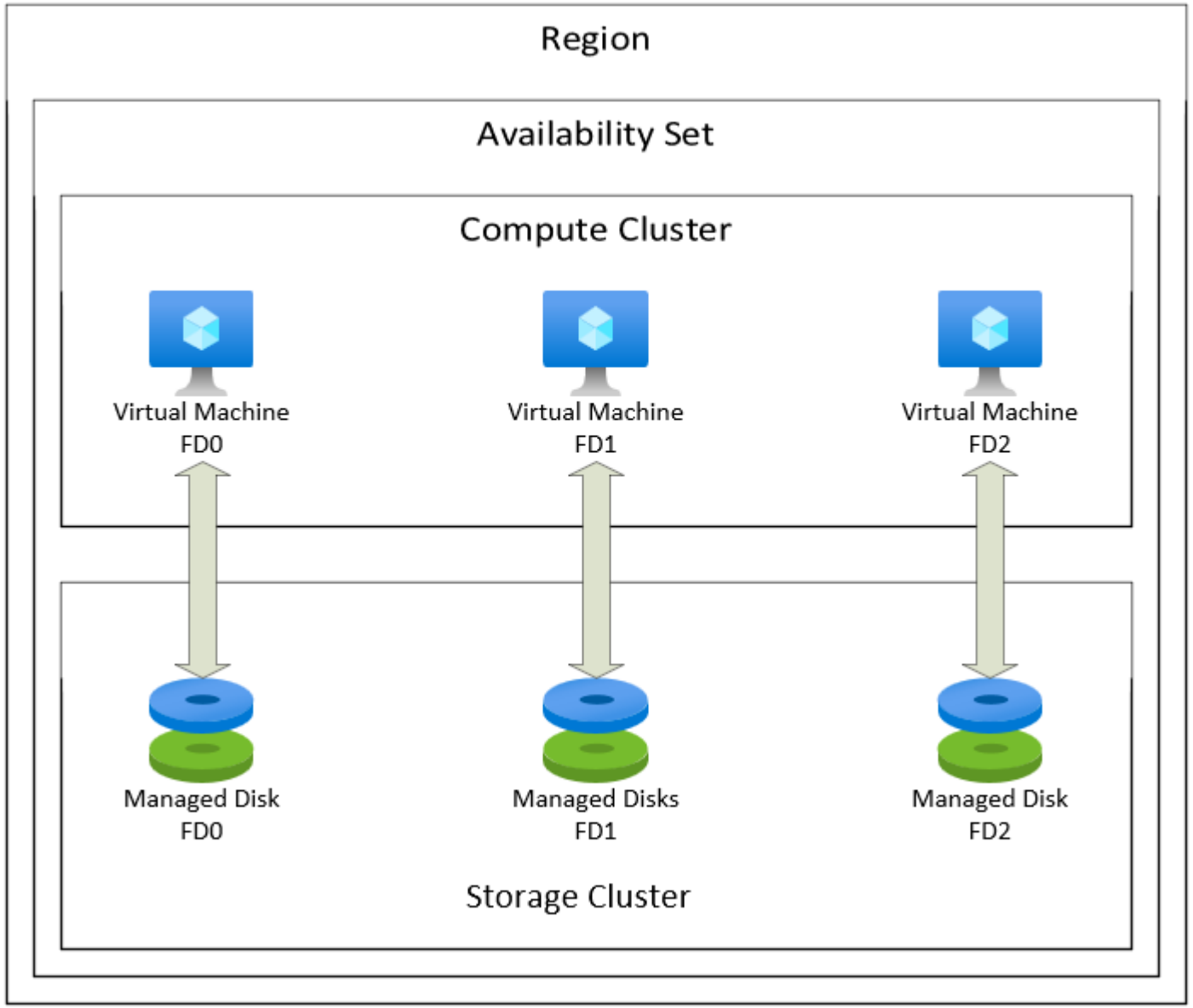


Наприклад, для 6 ВМ з 5 доменами оновлення шоста віртуальна машина поміщається в той же домен оновлення, що й перша віртуальна машина, таким чином, коли ДО1 – перезавантажується, то ВМ1 та ВМ2 не доступні, але ВМ3, ВМ4, ВМ5 – працюють, відповідно при завантаженні ДО2 – не доступна тільки ВМ2.
Це рішення забезпечує високу доступність ВМ в хмарі Azure.

- «Доступна зона» є комбінацією «доменів збою» і «доменів оновлення». Для кожної зони доступності можна настроїти до 3 доменів збою та 20 доменів оновлення. Ці конфігурації не можна змінити після створення групи доступності.
- Домени збою визначають групу віртуальних машин, які спільно використовують спільне джерело живлення та мережний комутатор.
- Домени оновлення – це групи віртуальних машин та базове фізичне обладнання, яке може бути перезавантажено одночасно.

Availability sets— це логічне групування віртуальних машин, яке дозволяє Azure зрозуміти, як ваша програма створена для забезпечення резервування та доступності. Рекомендовано створювати дві або більше віртуальних машин у межах набору доступності, щоб забезпечити високу доступність програми та відповідати 99,95% Azure SLA.
За певних обставин дві віртуальні машини в одному наборі доступності можуть спільно використовувати домен помилки.
Спільний домен помилки може бути спричинений виконанням наступної послідовності під час розгортання віртуальних машин:

Розгорніть першу віртуальну машину.
Зупинити/звільнити першу віртуальну машину.
Розгорніть другу віртуальну машину.
За цих обставин диск ОС другої віртуальної машини може бути створений у тому самому домені помилки, що й перша віртуальна машина, тому дві віртуальні машини будуть у тому самому домені помилки. Щоб уникнути цієї проблеми, не треба зупиняти/звільняти віртуальні машини між розгортаннями.



Availability sets

```
az vm availability-set create --name
                              --resource-group
                              [--location]
                              [--no-wait]
                              [--platform-fault-domain-count]
                              [--platform-update-domain-count]
                              [--ppg]
                              [--tags]
                              [--unmanaged]
                              [--validate]
```

az vm availability-set create -n MyAvSet -g $grp --platform-fault-domain-count 2 --platform-update-domain-count 2

```
az vm availability-set delete [--availability-set-name]
                              [--ids]
                              [--resource-group]
                              [--subscription]
```

Конфігурація віртуальна мережа з двома і більше віртуальними машинами

Коли дві віртуальні машини (VM) підключені до однієї віртуальної мережі, можуть виникати кілька проблем, пов'язаних з навантаженням, які варто враховувати:

1. Мережева затримка (Latency)

•Якщо одна або обидві машини генерують великий трафік, можуть виникати затримки в передачі даних між віртуальними машинами через перевантаження мережевої інфраструктури. Це особливо важливо, коли одна з машин виконує багато операцій вводу-виводу або вимагає обробки великих обсягів даних в реальному часі.

2. Обмежена пропускна здатність

•Віртуальна мережа має обмежену пропускну здатність, яка розподіляється між віртуальними машинами. Якщо одна з VM використовує значну частину пропускної здатності, інші машини можуть відчувати нестачу ресурсів для передачі даних, що знижує продуктивність.

3. Конкуренція за мережеві ресурси

•У віртуалізованих середовищах часто є обмежені фізичні мережеві інтерфейси. Коли декілька VM використовують один і той самий фізичний мережевий інтерфейс (NIC), це може призвести до перевантаження інтерфейсу, збільшення затримок і зниження загальної пропускної здатності.

4. Перевантаження сервісів

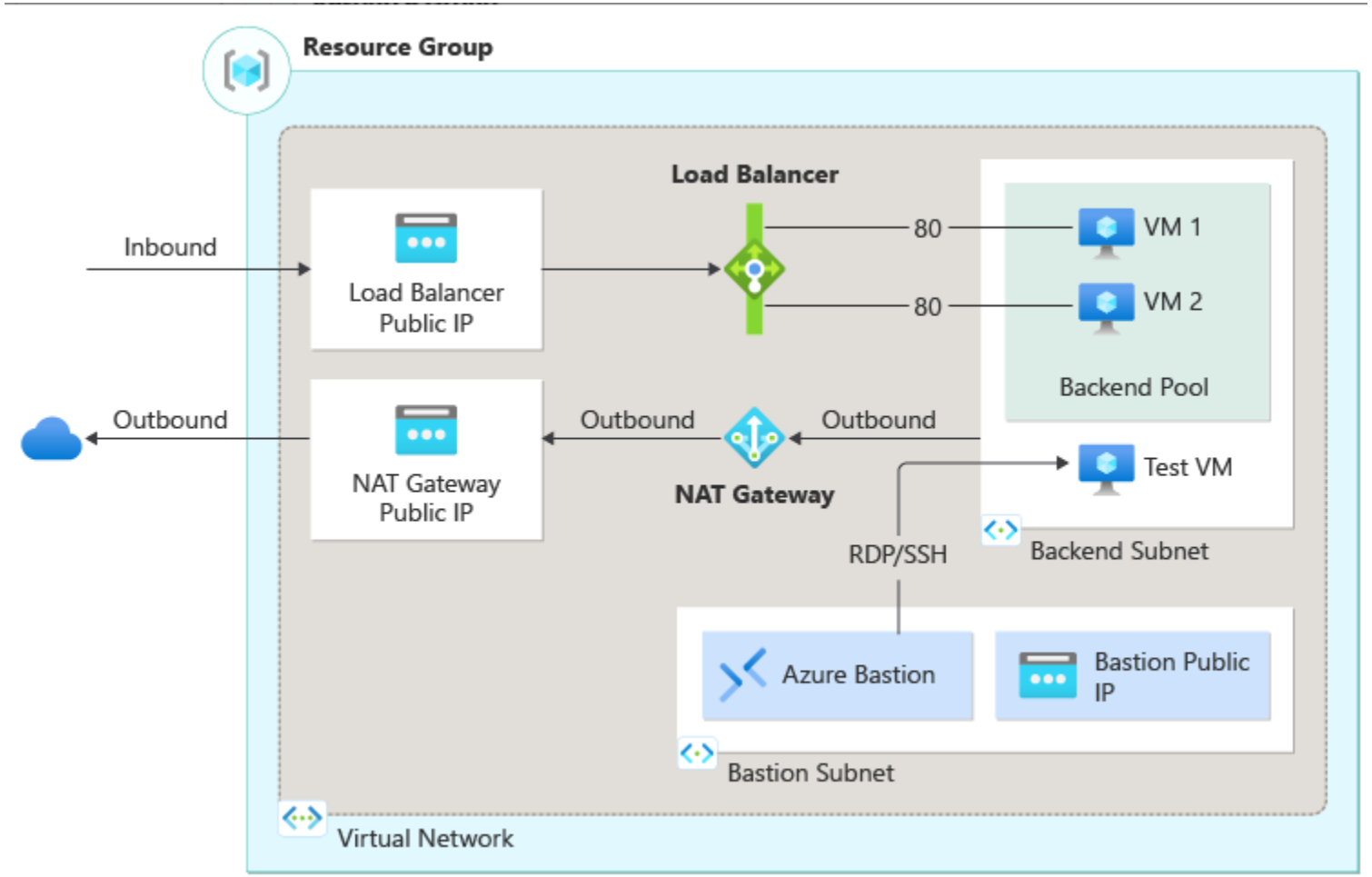
•Якщо дві машини залежать від тих самих мережевих сервісів (наприклад, DHCP, DNS або NAT), надмірне навантаження на ці сервіси може спричинити затримки або збої в обробці запитів. Наприклад, якщо обидві VM одночасно намагаються отримати IP-адресу через DHCP або вирішити доменне ім'я через DNS, можуть виникати затримки.

Віртуальні машини

```
$grp="VMdemo"
$location="westeurope"
$vnetName="VNET"
$subnetName="SUBNET_1"
$vmName1=“Demo_VM1”
$vmName2=“Demo_VM2”
$avset =“AVSET”

# CREATE RESOURCE GROUP
az group create --name $grp --location $location

# CREATE VIRTUAL NETWORK
az network vnet create --address-prefixes 10.0.0.0/16 --name $vnetName --resource-group $grp

# CREATING SUBNET
az network vnet subnet create -g $grp --vnet-name $vnetName -n $subnetName --address-prefixes 10.0.0.0/24

# CREATING AVAILABILITY SET
az vm availability-set create -n $avset -g $grp --platform-fault-domain-count 2 --platform-update-domain-count 2

# CREATING VM1
az vm create --resource-group $grp --name $vmName1 --image Win2019Datacenter --vnet-name $vnetName --subnet $subnetName --availability-set $avset --admin-username
azureuser --admin-password Hello@12345# --size Standard_DS1_v2

# CREATING VM2
az vm create --resource-group $grp --name $vmName2 --image Win2019Datacenter --vnet-name $vnetName --subnet $subnetName --availability-set $avset --admin-username
azureuser --admin-password Hello@12345# --size Standard_DS1_v2


#open ports
az vm open-port --port 80 --resource-group $grp --name $vmName1
az vm open-port --port 80 --resource-group $grp --name $vmName2

az vm run-command invoke -g $grp -n $vmName1 --command-id RunPowerShellScript --scripts "Install-WindowsFeature -name Web-Server -IncludeManagementTools
az vm run-command invoke -g $grp -n $vmName2 --command-id RunPowerShellScript --scripts "Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

Azure Load Balancer

Балансування навантаження відноситься до ефективного розподілу вхідного мережного трафіку між групою внутрішніх серверів або ресурсів.
Load Balancer використовуються для балансування трафіку, надісланого з Інтернету до віртуальних машин.

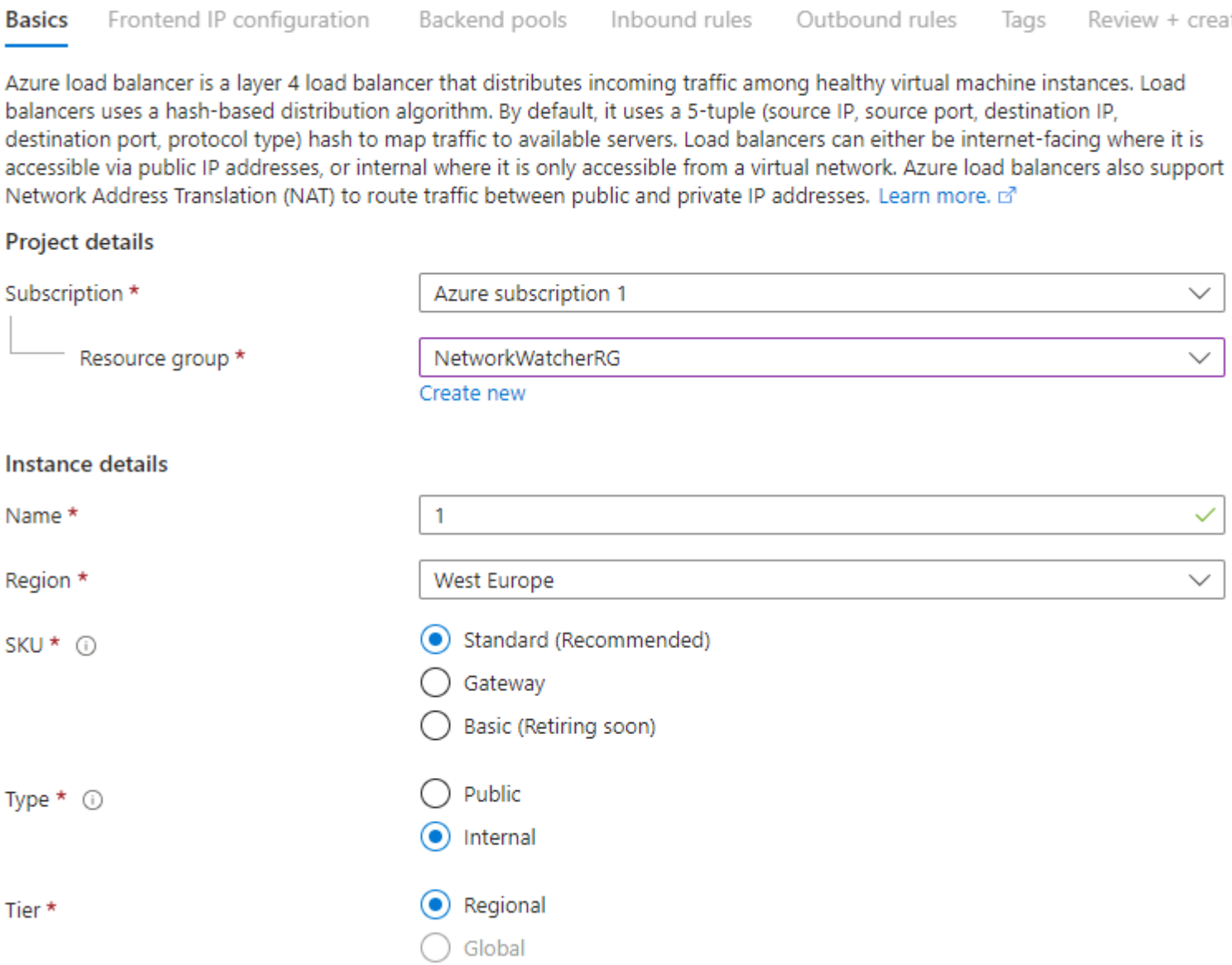


Під час створення підсистеми балансування навантаження необхідно налаштувати:

1. Інтерфейсна IP-адреса
2. Внутрішній пул
3. Правила балансування навантаження для вхідного трафіку
4. Проба працездатності

Основні сценарії, які можна виконати за допомогою Azure Standard Load Balancer, включають:

- Баланс внутрішнього та зовнішнього трафіку для віртуальних машин Azure.
- Підвищуйте доступність, розподіляючи ресурси всередині та між зонами.
- Моніторинг збалансованих ресурсів.
- Переадресація портів для доступу до віртуальних машин у віртуальній мережі за загальнодоступною IP-адресою та портом.
- Стандартний балансувальник навантаження надає багатовимірні показники через Azure Monitor. Ці показники можна фільтрувати, групувати та розбивати за певним параметром. Вони надають поточну та історичну інформацію про продуктивність і здоров’я вашого сервісу.
- Insights for Azure Load Balancer пропонує попередньо налаштовану інформаційну панель із корисними візуалізаціями для цих показників.



Azure Load Balancer має три одиниці (SKU) — Basic, Standard, and Gateway. Кожен SKU призначений для певного сценарію та має відмінності в масштабі, функціях і ціні.

Standard - коли потрібна висока продуктивність і наднизька затримка. Маршрутизує трафік усередині та між регіонами, а також до зон доступності для високої стійкості.

Basic - для невеликих додатків, яким не потрібна висока доступність або резервування. Несумісний із зонами доступності

Конфігурація IP зовнішнього інтерфейсу

IP-адреса Azure Load Balancer. Це точка взаємодії з клієнтами. Ці IP-адреси можна віднести до наступних категорій:

1. Загальнодоступний IP-адрес
2. Приватний IP-адрес

Тип IP-адреси визначає тип створюваної підсистеми балансування навантаження. Якщо вибрати приватну IP-адресу, створюється внутрішня підсистема балансування навантаження. Якщо вибрати загальнодоступний IP-адресу, створюється загальнодоступна підсистема балансування навантаження.

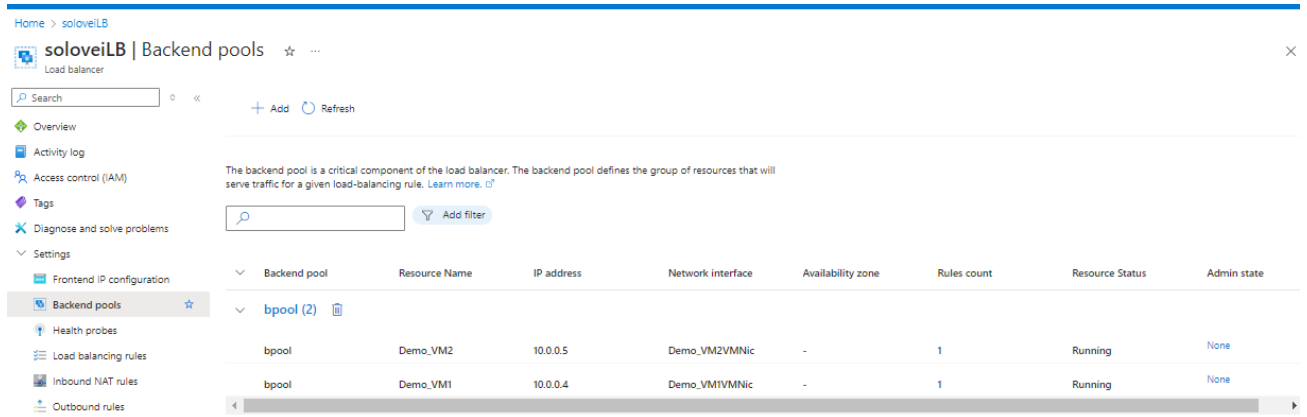
Загальнодоступна підсистема балансування навантаження містить загальнодоступний IP-адресу та порт вхідного трафіку з частним IP-адресою та портом віртуальної машини. Відповідний трафік від віртуальної машини містить підсистему балансування навантаження зворотним способом. Змінюючи правила балансування навантаження, можна розподілити певні типи трафіку між кількома різними віртуальними машинами або службами. Наприклад, можна розподілити навантаження від трафіку веб-запитів на кілька веб-серверів.

Внутрішня підсистема балансування навантаження розподіляє трафік між ресурсами, що знаходяться в віртуальній мережі. Azure обмежує доступ до інтерфейсних IP-адрес віртуальної мережі, до якої застосовується балансування навантаження. Зовнішні IP-адреси та віртуальні мережі ніколи не надаються безпосередньо в кінцевій точці Інтернету, що означає, що внутрішня підсистема балансування навантаження не може приймати вхідний трафік з Інтернету. Внутрішні бізнес-додатки виконуються в Azure і доступні з Azure або з локальних ресурсів.

Backend pool

Група віртуальних машин або примірників ***у масштабованому наборі віртуальних машин***, яка обслуговує вхідний запит.

Бекенд-пули підтримують додавання примірників через мережевий інтерфейс або IP-адреси. Віртуальним машинам не потрібна загальнодоступна IP-адреса, щоб бути приєднаними до фонового пулу загальнодоступного балансувальника навантаження. Віртуальні машини можна приєднувати до фонового пулу балансувальника навантаження, навіть якщо вони перебувають у стані зупинки. Ви також можете налаштувати кілька внутрішніх пулів з різними групами екземплярів для одного балансувальника навантаження. Створивши кілька правил балансування навантаження, кожне з яких націлено на окремий серверний пул, ви можете налаштувати трафік для розподілу між різними наборами внутрішніх ресурсів на основі зовнішнього порту та протоколу балансувальника навантаження.



Health probes

Зонд справності використовується для визначення стану справності екземплярів у фоновому пулі. Цей тест працездатності визначає, чи може він отримувати трафік.

Ви можете визначити нездоровий поріг для ваших зондів здоров’я. Коли зонд не відповідає, балансувальник навантаження припиняє надсилати нові підключення до непрацездатних примірників. Помилка зонду не впливає на існуючі з’єднання. З’єднання триває, доки програма:

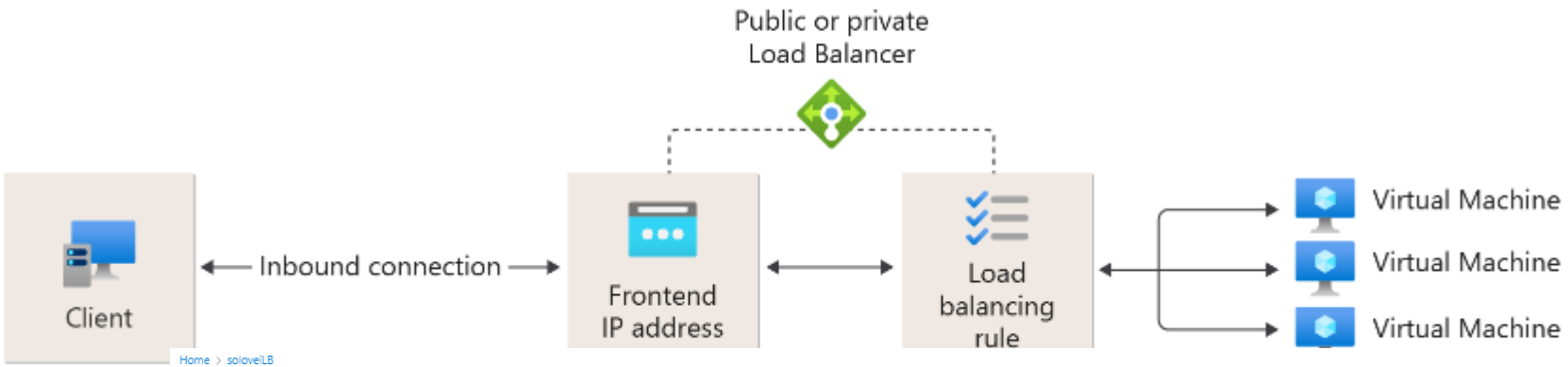
Закінчує потік
Виникає тайм-аут простою
Віртуальна машина вимикається
Балансувальник навантаження надає різні типи тестів справності для кінцевих точок: TCP, HTTP і HTTPS.
Базовий балансувальник навантаження не підтримує перевірки HTTPS. Базовий балансувальник навантаження закриває всі TCP-з’єднання (включаючи встановлені з’єднання).

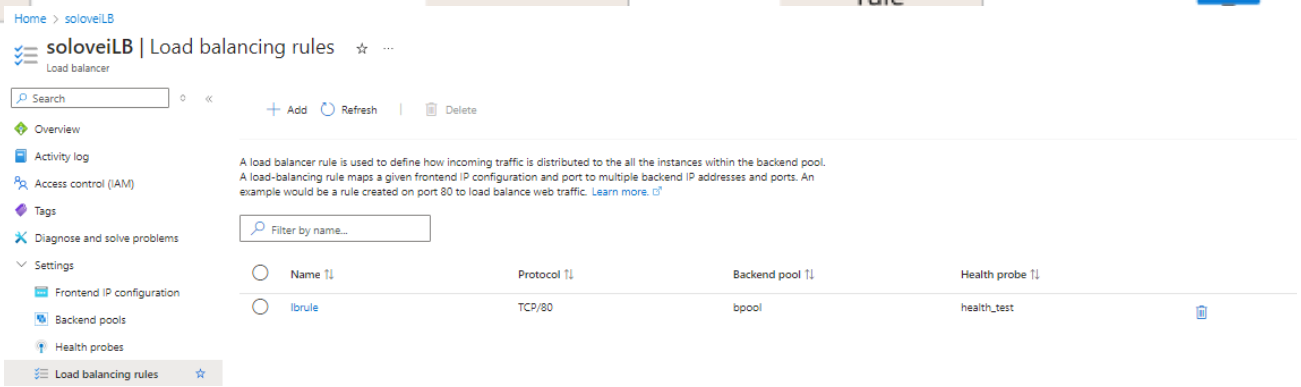
Властивості
Ім'я Назва зонда спавності.
Протокол Варіанти: TCP, HTTP, HTTPS
Порт Порт датчика працездатності. Порт призначення, який би використовував зонд справності під час підключення до віртуальної машини для перевірки її справності
Інтервал (секунди) Інтервал перевірки працездатності. Час (у секундах) між різними зондами під час двох послідовних спроб перевірки справності віртуальної машини
Використовується Список правил балансування навантаження, які використовують цей конкретний тест справності.

Load Balancer rules

Правило балансування навантаження використовується для визначення того, як вхідний трафік розподіляється між усіма екземплярами всередині резервного пулу. Правило балансування навантаження відображає певну конфігурацію IP-адреси та порт інтерфейсу на кілька внутрішніх IP-адрес і портів. Правила балансування навантаження призначені лише для вхідного трафіку.

Наприклад, правило балансування навантаження для порту 80, щоб спрямувати трафік із IP-адреси зовнішньої сторони на порт 80 серверної частини.





Порти високої доступності

Правило балансування навантаження, налаштоване за допомогою «протокол — усі та порт — 0», відоме як правило порту високої доступності (HA). Це правило дає змогу одним правилом балансувати навантаження для всіх потоків TCP і UDP, які надходять на всі порти внутрішнього стандартного балансувальника навантаження.

Рішення про балансування навантаження приймається для кожного потоку. Ця дія заснована на наступному зв'язку з п'яти кортежів:

IP-адреса джерела
вихідний порт
IP-адреса призначення
порт призначення
протокол

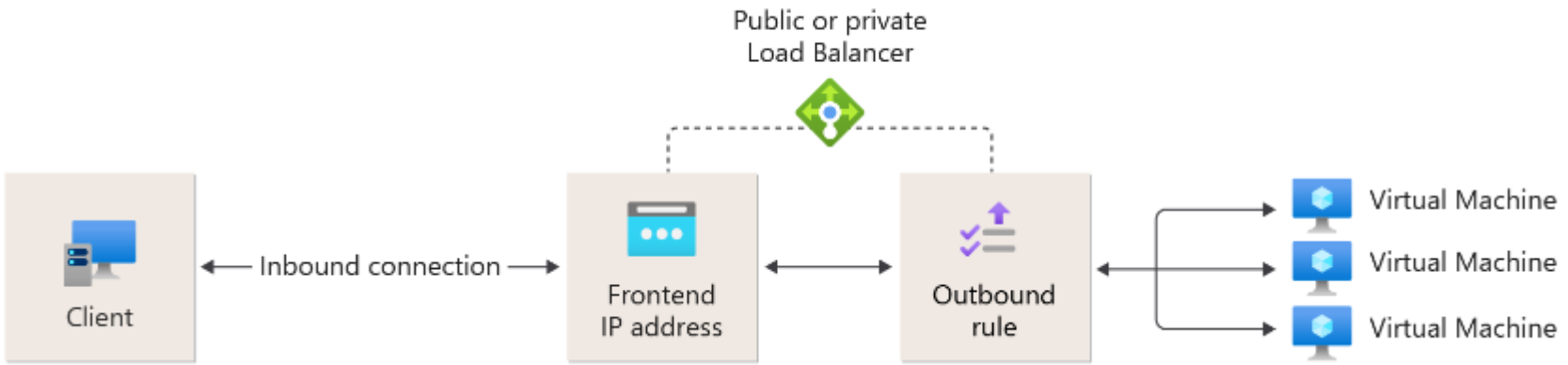
Правила балансування навантаження портів високої доступності допомагають у критичних сценаріях, таких як висока доступність і масштабування мережевих віртуальних пристроїв (NVA) у віртуальних мережах. Ця функція може допомогти, коли потрібно збалансувати навантаження великої кількості портів.

Вхідні правила NAT

Правило вхідного NAT пересилає вхідний трафік, надісланий на зовнішню комбінацію IP-адреси та порту. Трафік надсилається на певну віртуальну машину або екземпляр у фоновому пулі. Перенаправлення портів виконується за допомогою того ж розподілу на основі хешу, що й балансування навантаження.

Вихідні правила

Вихідне правило виводить вихідну трансляцію мережевих адрес (NAT) для всіх віртуальних машин або екземплярів, визначених серверним пулом. Це правило дозволяє примірникам у серверній частині обмінюватися даними (вихідними) з Інтернету або іншими кінцевими точками.



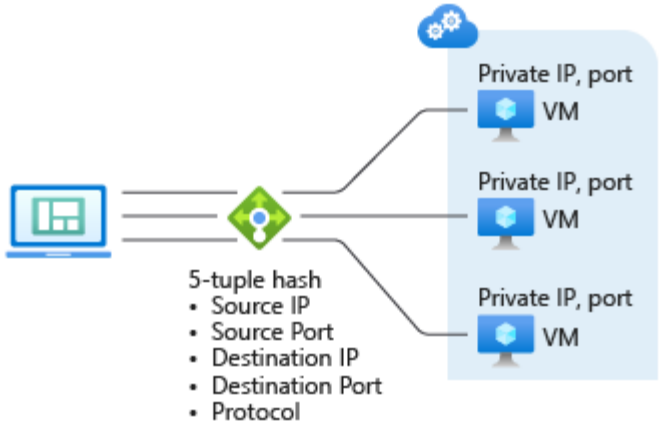
Алгоритм балансування навантаження

Створивши правило балансувальника навантаження, ви можете розподілити потоки вхідного трафіку від інтерфейсу балансувальника навантаження до його фонових пулів. Azure Load Balancer використовує п’ятикратний алгоритм хешування для розподілу вхідних потоків (не байтів). Балансувальник навантаження переписує заголовки потоків заголовків TCP/UDP під час спрямування трафіку до екземплярів внутрішнього пулу (балансувальник навантаження не переписує заголовки HTTP/HTTPS). Коли тест справності балансувальника навантаження вказує на справну кінцеву точку серверної частини, екземпляри серверної частини доступні для отримання нових потоків трафіку.

За замовчуванням Azure Load Balancer використовує хеш із п’яти кортежів.

П'ятірка включає:

1. IP-адреса джерела
2. Порт джерела
3. IP-адреса призначення
4. Порт призначення
5. Номер IP-протоколу для відображення потоків на доступні сервери



При використанні протоколу RDP (Remote Desktop Protocol) для доступу до віртуальної машини в Azure можуть виникати наступні проблеми:

Неавторизований доступ: Відкриття порту RDP (звичайно 3389) може зробити віртуальну машину вразливою для атак типу brute-force, що можуть призвести до несанкціонованого доступу.

Відсутність шифрування: Якщо з'єднання RDP не налаштоване належним чином, можуть виникати проблеми з недостатнім рівнем шифрування, що робить дані вразливими до перехоплення.

VPN обмеження: Деякі організації рекомендують використовувати RDP через VPN, щоб додатково захистити машину від зовнішніх атак.

Обмеження мережевого трафіку: RDP вимагає наявності відкритого порту на віртуальній машині, і цей порт може бути заблокований фаєрволами або налаштуваннями мережі.

Недостатня пропускна здатність: Якщо інтернет-з'єднання користувача є нестабільним або має низьку пропускну здатність, це може спричиняти затримки або розриви з'єднання RDP.

3. ***Обмеження продуктивності***
Висока вимога до графічних ресурсів може викликати уповільнення в роботі, оскільки RDP не завжди ефективно передає дані, особливо якщо використовуються ресурсоємні програми.
Високе навантаження на мережу: Погане налаштування або недостатня ширина каналу інтернет-з'єднання може викликати затримки в передачі даних та уповільнення роботи віртуальної машини.

5. Використання публічних IP-адрес
Використання публічного IP для підключення через RDP підвищує ризик атак з боку інтернету, тому рекомендується використовувати приватні мережі або рішення на основі VPN.

Проблема: встановлення звязку з ВМ через приватну IP адресу заборонено

Віртуальна приватна мережа (VPN) типу «точка – мережа»,
підключення типу “Vnet-peering”,
підключення типу «мережа – мережа», Azure ExpressRoute

IPv4 (Інтернет-протокол версії 4)

IPv4 (Інтернет-протокол версії 4) — це основний протокол, який використовується на рівні Інтернету моделі TCP/IP. Він забезпечує унікальну адресацію для пристроїв, підключених до мережі
Формат адреси: адреси IPv4 — це 32-розрядні числові значення, записані в десятковій системі у вигляді чотирьох 8-розрядних чисел, розділених крапками, наприклад 192.168.0.1. Кожне число становить від 0 до 255, тобто адреси IPv4 варіюються від 0.0.0.0 до 255.255.255.255.
Класи адрес:
Клас A: для великих мереж від 1 до 126.
Клас B: для мереж середнього розміру 128 до 191.
Клас C: для невеликих мереж 192 до 223.
Клас D: зарезервовано для багатоадресних груп.
Клас E: зарезервовано для експериментального використання.
Підмережі: поділ IP-мережі на менші сегменти (підмережі) шляхом маніпулювання маскою підмережі. Це допомагає керувати мережевим трафіком і оптимізувати розподіл IP-адрес.
Обмеження: IPv4 підтримує приблизно 4,3 мільярда унікальних адрес, що призвело до розвитку IPv6 через вичерпання доступних адрес IPv4.
Нотації CIDR (Classless Inter-Domain Routing) дозволяє визначати підмережі за допомогою позначення, наприклад, 192.168.10.0/24, де /24 означає, що перші 24 біти використовуються для мережі, а залишкові — для хостів.

Діапазон приватних IP-адрес

Є три діапазони IP-адрес, які спеціально зарезервовані для приватного використання:

1.Діапазон класу A:

- •Приватні адреси: 10.0.0.0 – 10.255.255.255
- •Загалом містить 16,777,216 адрес.
- •Використовується для великих мереж.

2.Діапазон класу B:

- •Приватні адреси: 172.16.0.0 – 172.31.255.255
- •Загалом містить 1,048,576 адрес.
- •Часто використовується для середніх мереж.

3.Діапазон класу C:

- •Приватні адреси: 192.168.0.0 – 192.168.255.255
- •Загалом містить 65,536 адрес.
- •Найпоширеніший для домашніх та малих мереж.

Як працюють приватні IP-адреси:

•**Приватні адреси** працюють тільки всередині локальної мережі, наприклад, у домашньому або офісному середовищі.

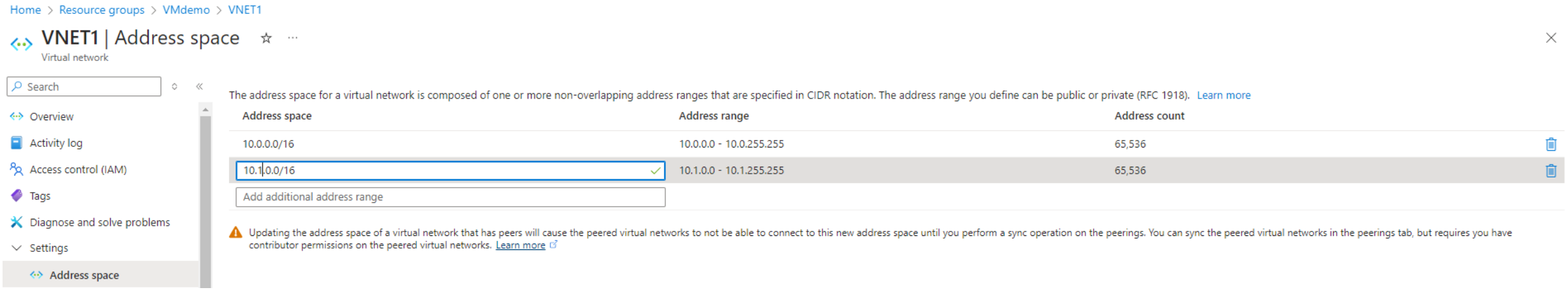
•Якщо пристрій із приватною IP-адресою хоче отримати доступ до Інтернету, маршрутизатор використовує NAT для перетворення приватної IP-адреси на публічну IP-адресу, яку бачить зовнішній світ.

Ознаки приватних IP-адрес:

•Приватні IP-адреси **ніколи не використовуються безпосередньо в Інтернеті**.

•Вони використовуються для мережевих пристроїв, таких як комп'ютери, принтери, телефони всередині організацій чи домівок.

Додати або видаляти діапазони адрес для віртуальної мережі.
Діапазон адрес має бути вказаний у нотації CIDR і не може перетинатися з іншими діапазонами адрес у тій самій віртуальній мережі.

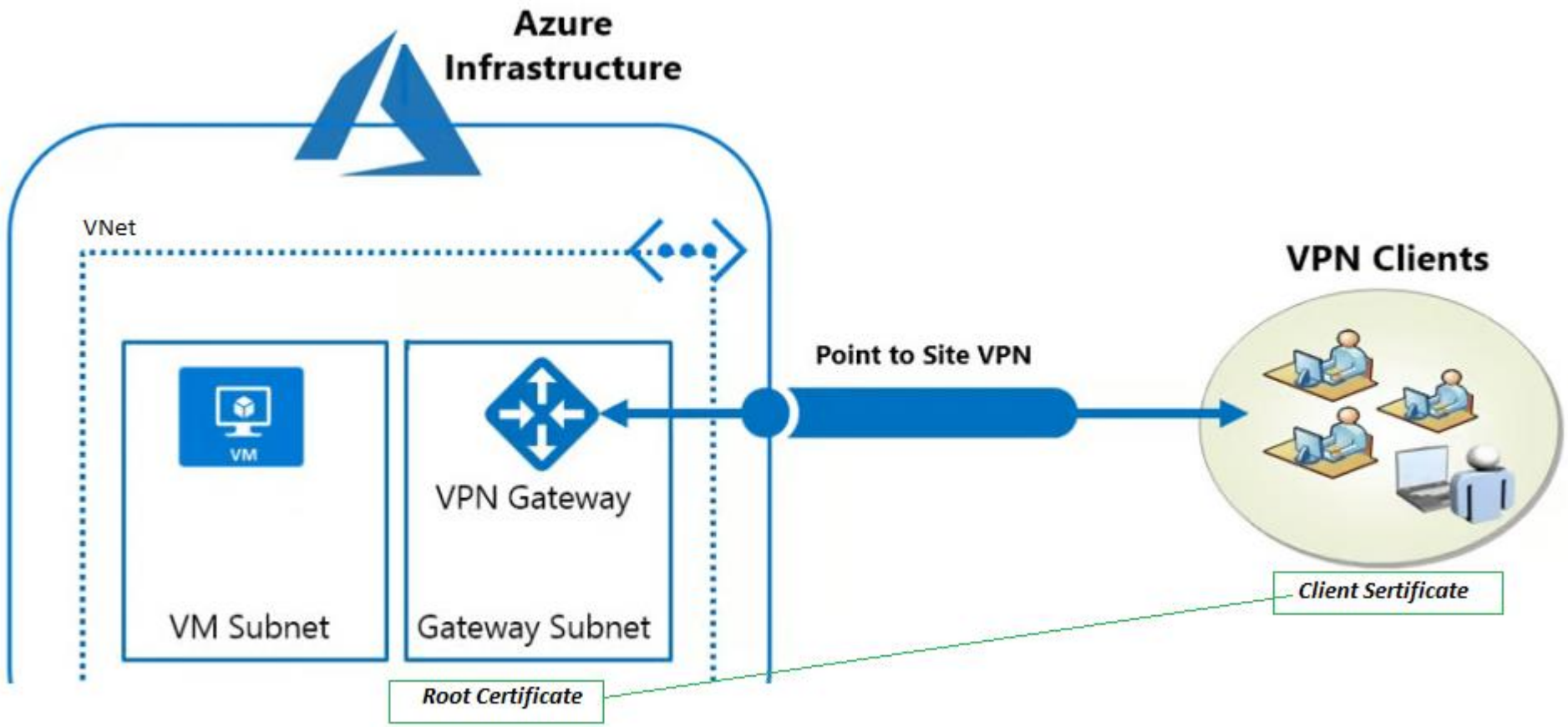


Конфігурація підключення до віртуальної мережі Azure

Комп'ютери та мережі можна підключити до віртуальної мережі за допомогою будь-якого з наступних варіантів:

1. Віртуальна приватна мережа (VPN) типу «точка – мережа» - встановлюється між віртуальною мережею та одним комп'ютером у мережі. Обмін даними між комп'ютером та віртуальною мережею здійснюється через Інтернет за допомогою зашифрованого тунелю.
2. Віртуальна приватна мережа (VPN) типу “VNet peering” – піринг віртуальної мережі дає змогу легко з’єднати дві або більше віртуальних мереж у Azure.
3. Віртуальна приватна мережа (VPN) типу “VNet-to-VNet” -
4. Віртуальна приватна мережа (VPN) типу «мережа – мережа» - встановлюється між локальним VPN-пристроєм та VPN-шлюзом Azure, розгорнутим у віртуальній мережі. Використовуючи такий тип з'єднання, авторизовані локальні ресурси можуть отримати доступ до віртуальної мережі. Обмін даними між локальним VPN-пристроєм та VPN-шлюзом Azure здійснюється через Інтернет за допомогою зашифрованого тунелю.
5. Azure ExpressRoute: встановлюється між мережею та Azure через партнера ExpressRoute. Це підключення закрите. Трафік не передається через Інтернет.

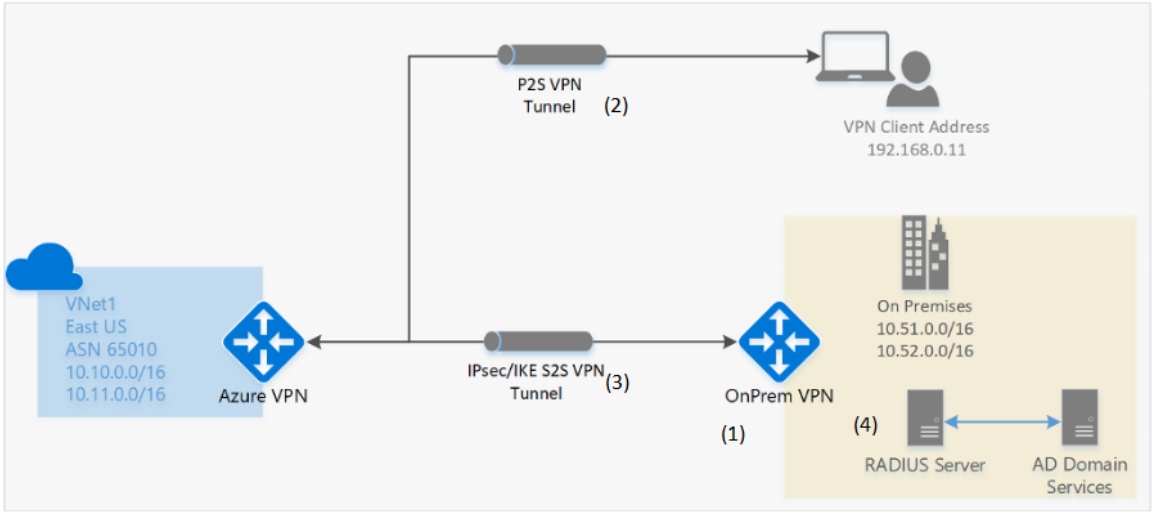
Віртуальна приватна мережа (VPN) типу «точка – мережа»



При умові, коли локальна машина має сертифікат клієнтаVPN Gateway – Root Certificate, тоді між локальною машиною і VPN Gateway встановлюється з'єднання, шляхом якого локальна машина отримує з'єднання з ВМ, тому, що VPN Gateway включено в одну віртуальну мережу з ВМ.

Конфігурація підключення типу «точка – мережа»

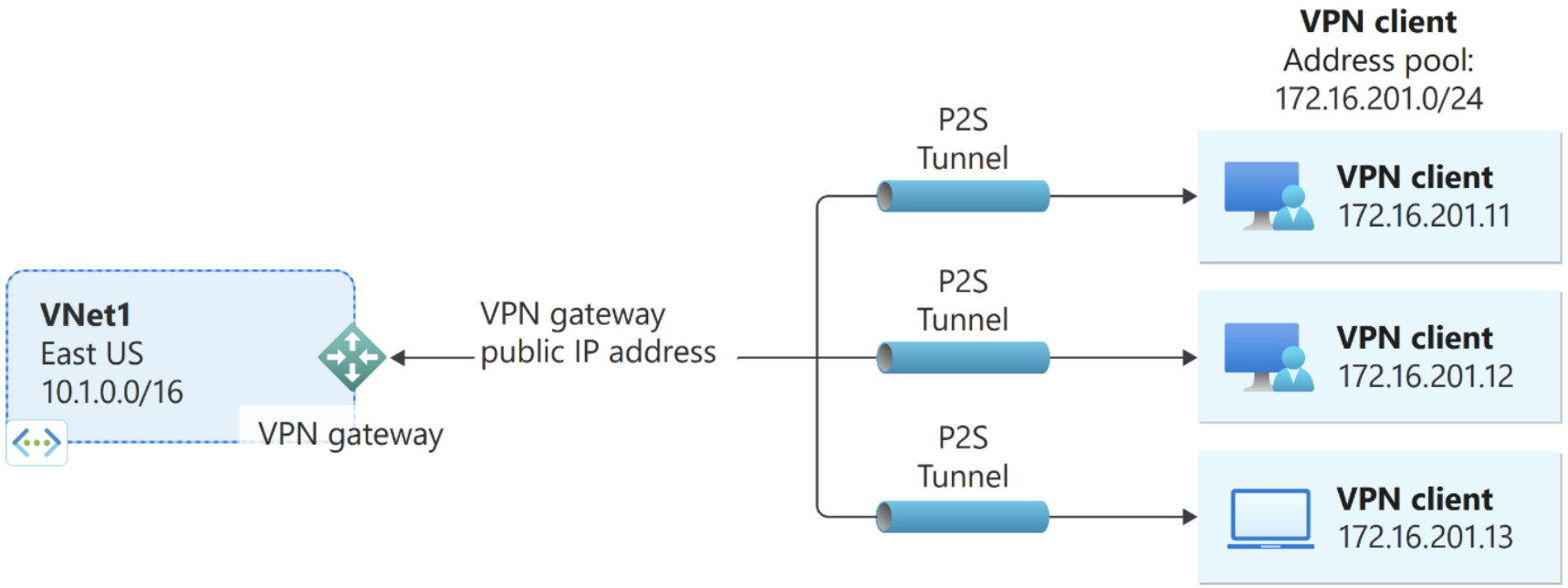
- Підключення типу «точка – мережа» можливе за одним з протоколів:
  - Протокол OpenVPN- на основі SSL/TLS, підключення дозволяє трафіку проходити через брандмауер - порт 443. OpenVPN можна використовують для пристроїв на платформі Android, iOS, Windows, Linux и Mac.
  - SSTP (Secure Socket Tunneling Protocol) - підключення за протоколом TLS (*Transport Layer Security)*, підходить тільки для пристроїів Windows.
  - IPSec/IKEv2 VPN — рішення VPN на основі стандартів Ipsec (IP Security - а відміну від SSL та TLS, працюють на мережевому рівні; IKE (Internet Key Exchange) - стандартний протокол набору протоколів IPsec, який використовується для забезпечення безпеки взаємодії в віртуальних приватних мережах). IKEv2 VPN можна використовують для пристроїв - на платформі Mac.
- Аутентифікація клієнтів можлива способами: 1) перевірка сертифікатів; 2) перевірка дійсного обликового запису клієнта Azure; 3) перевірка облікового домену організації.
- Перевірка виконується шлюзами (2,3) на момент встановлення підключення.
- Для перевірки облікового запису домену організації – додатково використовується сервер RADIUS (4) , який інтегрований з обліковими записами Azure.



Спосіб аутентифікації	Тип тунелю	Платформа
Сертифікат Azure	IKEv2, OpenVPN, SSTP	Windows
Сертифікат Azure	IKEv2, OpenVPN	Linux, macOS-iOS
Обліковий запис Azure	OpenVPN (SSL)	Windows, macOS

Конфігурація підключення типу «точка – мережа»

Підключення "точка - мережа" (P2S) до VPN-шлюзу дозволяє встановити безпечне з'єднання з віртуальною мережею на індивідуальному клієнтському комп'ютері. Підключення типу "точка - мережа" спочатку встановлюється на клієнтському комп'ютері. Таку конфігурацію також зручно використовувати замість VPN-підключення типу "мережа-мережа" за наявності невеликої кількості клієнтів, яким потрібне підключення до віртуальної мережі.



Azure VPN Gateway - ключові сценаріїв для шлюзу VPN

- Надсилає зашифрований трафік між віртуальною мережею Azure і локальними розташуваннями через загальнодоступний Інтернет.

З’єднання «сайт-сайт»: міжлокальне тунельне з’єднання IPsec/IKE VPN між шлюзом VPN і локальним пристроєм VPN.

З’єднання «точка-сайт»: VPN через OpenVPN, IKEv2 або SSTP. Цей тип підключення дає змогу підключитися до віртуальної мережі з віддаленого місця, наприклад із конференції чи з дому.

- Надсилає зашифрований трафік між віртуальними мережами.

VNet-to-VNet: тунельне з’єднання IPsec/IKE VPN між шлюзом VPN та іншим шлюзом VPN Azure, який використовує тип з’єднання VNet-to-VNet. Цей тип підключення розроблено спеціально для підключень VNet-to-VNet.

З’єднання «сайт-сайт»: тунельне з’єднання IPsec/IKE VPN між шлюзом VPN та іншим шлюзом VPN Azure. Цей тип з’єднання, якщо він використовується в архітектурі VNet-to-VNet, використовує тип з’єднання Site-to-site (IPsec), який дозволяє підключатися між приміщеннями до шлюзу на додаток до з’єднань між шлюзами VPN.

ExpressRoute + шлюз VPN: комбінація з’єднань ExpressRoute + шлюз VPN (сумісні з’єднання).
Використовуйте мережі VPN типу "сайт-сайт", щоб підключатися до сайтів, які не підключені через ExpressRoute. Ви можете зробити це за допомогою:

ExpressRoute + шлюз VPN: комбінація з’єднань ExpressRoute + шлюз VPN (сумісні з’єднання).

Віртуальний мережевий шлюз складається з двох або більше віртуальних машин, керованих Azure. Коли ви створюєте шлюз віртуальної мережі, віртуальні машини шлюзу автоматично розгортаються в підмережі шлюзу (завжди під назвою GatewaySubnet) і налаштовуються з указаними параметрами. Процес може тривати 45 хвилин або більше, залежно від вибраного SKU шлюзу.

Одним із параметрів, які ви вказуєте під час створення шлюзу віртуальної мережі, є тип шлюзу. Тип шлюзу визначає спосіб використання шлюзу віртуальної мережі та дії, які виконує шлюз. Віртуальна мережа може мати два віртуальні мережеві шлюзи; один шлюз VPN і один шлюз ExpressRoute.

Azure підтримує два різні типи VPN для шлюзів VPN: на основі політики та на основі маршруту. VPN-шлюзи на основі маршрутів створені на іншій платформі, ніж VPN-шлюзи на основі політики. Це призводить до різних специфікацій шлюзу. У наведеній нижче таблиці показано артикули шлюзу, які підтримують кожен тип VPN, і пов’язані підтримувані версії IKE.

Gateway VPN type	Gateway SKU	IKE versions supported
Policy-based gateway	Basic	IKEv1
Route-based gateway	Basic	IKEv2
Route-based gateway	VpnGw1, VpnGw2, VpnGw3, VpnGw4, VpnGw5	IKEv1 and IKEv2
Route-based gateway	VpnGw1AZ, VpnGw2AZ, VpnGw3AZ, VpnGw4AZ, VpnGw5AZ	IKEv1 and IKEv2

Режим Active-Active — це конфігураційний варіант для віртуальних мережевих шлюзів Azure, який дозволяє одночасно працювати двом екземплярам шлюзу.
Резервування та висока доступність: У режимі Active-Active розгортаються два екземпляри VPN-шлюзу. Кожен екземпляр має власну публічну IP-адресу. Ця конфігурація забезпечує резервування та високу доступність, тому що у випадку відмови одного з екземплярів шлюзу трафік може автоматично перенаправлятися через другий екземпляр без перерв.
•**Балансування навантаження**: Обидва екземпляри шлюзу активні одночасно, тобто вони можуть ділити між собою навантаження трафіку. Це корисно в ситуаціях, коли потрібно обробляти великий обсяг трафіку або забезпечити безперервну доступність.
•**Подвійні з'єднання**: Завдяки двом активним шлюзам можна встановити два одночасні VPN-з'єднання між локальною мережею та Azure. Це дозволяє краще розподіляти навантаження та забезпечувати більшу надійність.
Шлюзові SKU, що підтримують режим Active-Active
VpnGw1, VpnGw2, VpnGw3: Це різні рівні продуктивності для віртуальних мережевих шлюзів Azure, кожен з яких пропонує різні рівні пропускної здатності, кількість з'єднань і ціну.

VpnGw1: Базовий рівень шлюзу, який підходить для малих та середніх навантажень. Підтримує режим Active-Active та забезпечує збалансовану продуктивність за нижчою вартістю.
VpnGw2: Середній рівень шлюзу з вищою пропускною здатністю та більшою кількістю з'єднань у порівнянні з VpnGw1. Підходить для більш вимогливих завдань.
VpnGw3: Високопродуктивний шлюз для масштабних навантажень, що потребують максимальної пропускної здатності та максимальної кількості з'єднань. Ідеально підходить для критичних додатків, які потребують високої продуктивності та надійності.

SKU шлюзи – SKU конфігурація
покоління 1 і 2, крім VPN на основі базового маршруту: до 100 тунелів (*), P2S, BGP, активний-активний, настроювана політика IPsec/IKE, співіснування ExpressRoute/VPN

VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP	Zone-redundant	Supported Number of VMs in the Virtual Network
Generation1	Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported	No	200
Generation1	VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	No	450
Generation1	VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	No	1300
Generation1	VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	No	4000
Generation1	VpnGw1AZ	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	Yes	1000
Generation1	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	Yes	2000
Generation1	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	Yes	5000
Generation2	VpnGw2	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported	No	685
Generation2	VpnGw3	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported	No	2240
Generation2	VpnGw4	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported	No	5300
Generation2	VpnGw5	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported	No	6700
Generation2	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported	Yes	2000
Generation2	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported	Yes	3300
Generation2	VpnGw4AZ	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported	Yes	4400
Generation2	VpnGw5AZ	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported	Yes	9000

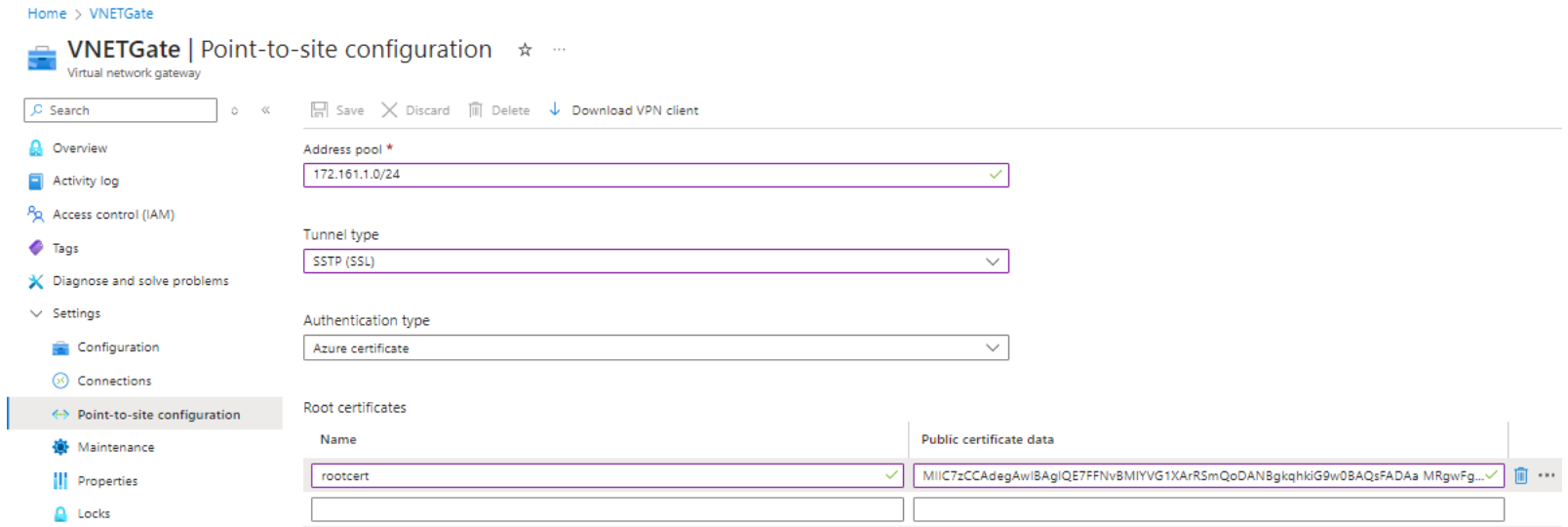
SKU шлюзи – SKU продуктивність

Generation	SKU	Algorithms used	Throughput observed per tunnel
Generation1	VpnGw1	GCMAES256 AES256 & SHA256 DES3 & SHA256	650 Mbps 500 Mbps 130 Mbps
Generation1	VpnGw2	GCMAES256 AES256 & SHA256 DES3 & SHA256	1.2 Gbps 650 Mbps 140 Mbps
Generation1	VpnGw3	GCMAES256 AES256 & SHA256 DES3 & SHA256	1.25 Gbps 700 Mbps 140 Mbps
Generation1	VpnGw1AZ	GCMAES256 AES256 & SHA256 DES3 & SHA256	650 Mbps 500 Mbps 130 Mbps
Generation1	VpnGw2AZ	GCMAES256 AES256 & SHA256 DES3 & SHA256	1.2 Gbps 650 Mbps 140 Mbps
Generation1	VpnGw3AZ	GCMAES256 AES256 & SHA256 DES3 & SHA256	1.25 Gbps 700 Mbps 140 Mbps
Generation2	VpnGw2	GCMAES256 AES256 & SHA256 DES3 & SHA256	1.25 Gbps 550 Mbps 130 Mbps

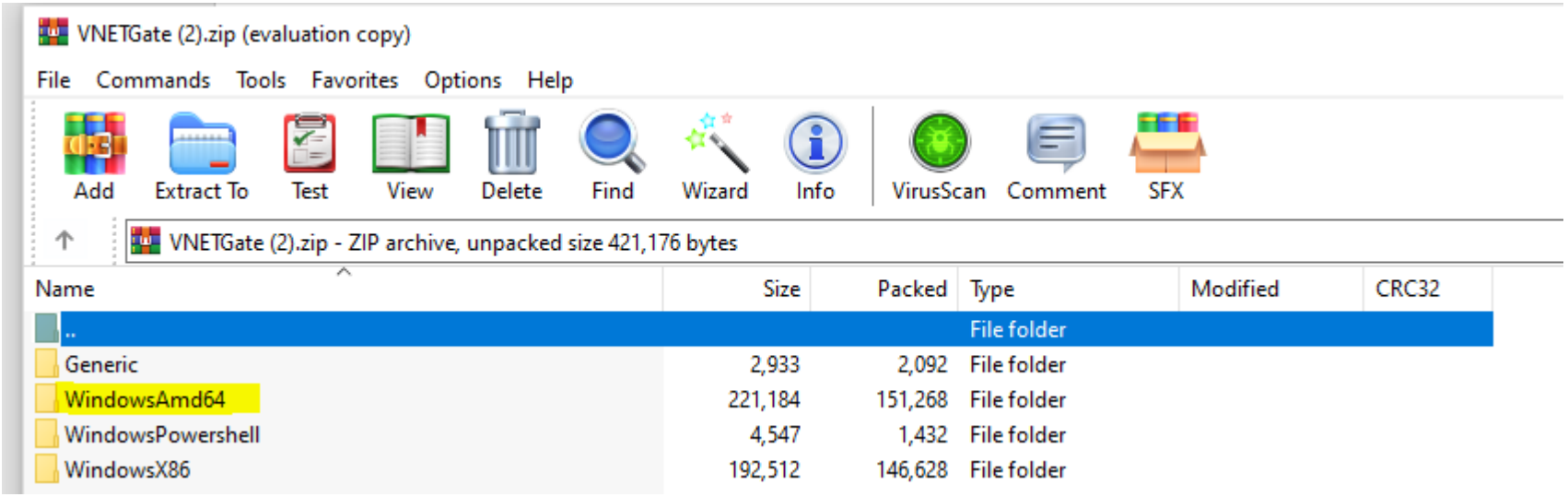
SKU шлюзу за продуктивністю
У таблиці в цьому розділі наведено результати тестування продуктивності для SKU VpnGw. Тунель VPN підключається до екземпляра шлюзу VPN. Пропускна здатність кожного екземпляра згадується в таблиці пропускної спроможності в попередньому розділі та доступна в сукупності для всіх тунелів, що підключаються до цього екземпляра. У таблиці показано спостережувану пропускну здатність і пропускну здатність пакетів за секунду на тунель для різних SKU шлюзу. Усе тестування проводилося між шлюзами (кінцевими точками) в Azure у різних регіонах зі 100 підключеннями та за стандартних умов навантаження. Ми використовували загальнодоступні інструменти iPerf і CTSTraffic для вимірювання продуктивності з’єднань між сайтами

Найкращу продуктивність було досягнуто, коли ми використовували алгоритм GCMAES256 як для шифрування IPsec, так і для цілісності.
Середня продуктивність була отримана при використанні AES256 для шифрування IPsec і SHA256 для цілісності.
Найнижча продуктивність була отримана, коли ми використовували DES3 для шифрування IPsec і SHA256 для цілісності.

Розглянемо приклад

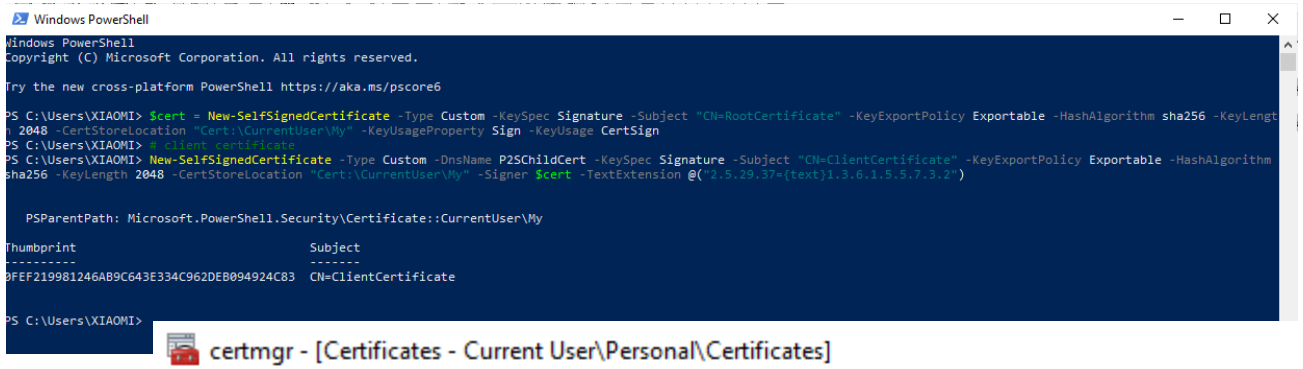


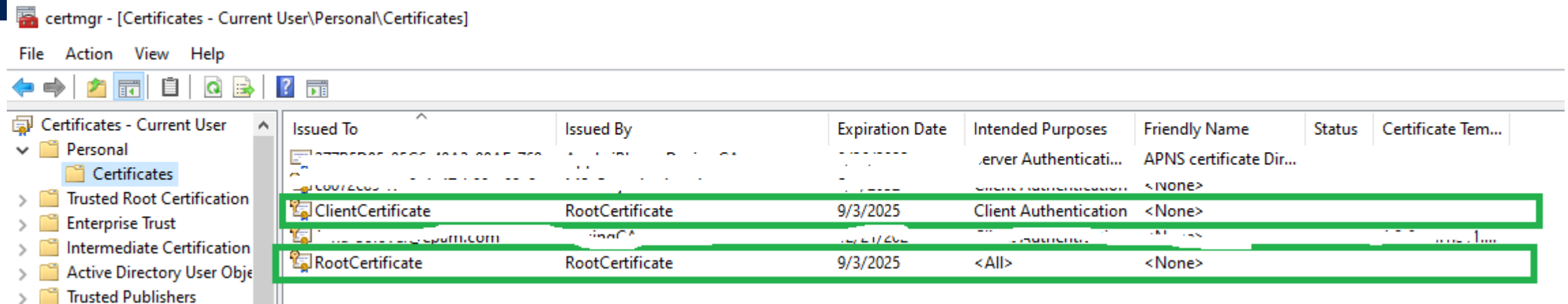
1. Перейдіть до Virtual network Gateway, визначте та збережіть Point-to-site конфігурацію – вкажіть Address pool, скопіюйте Root certificate, визначте Тип тунелю – SSTP (SSL).
2. Завантажте архів з файлами конфігурації.
3. Виконайте файл з WindowsAmd64



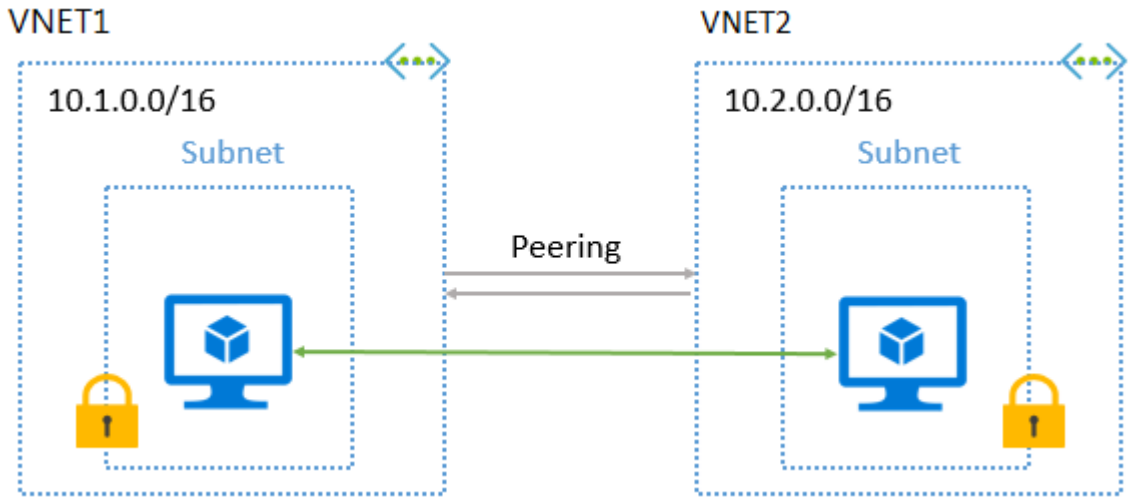
Додати сертифікати

```
# GENERATE CERTIFICATES WITH POWERSHELL
# root certificate
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject "CN=RootCertificate" -KeyExportPolicy
Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -
KeyUsage CertSign
# client certificate
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature -Subject "CN=ClientCertificate" -
KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -Signer
$cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

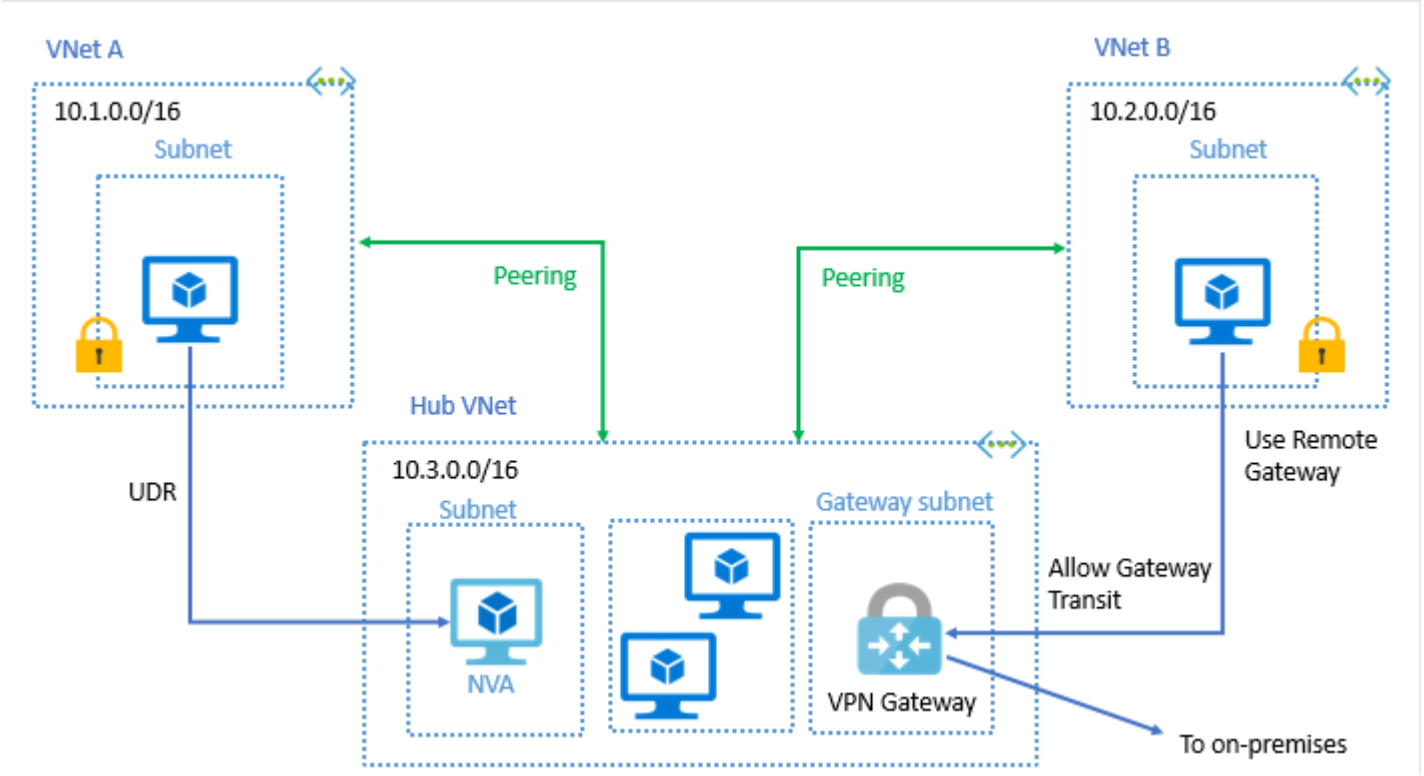




Vnet Peering- з’єднати дві або більше віртуальних мереж у Azure

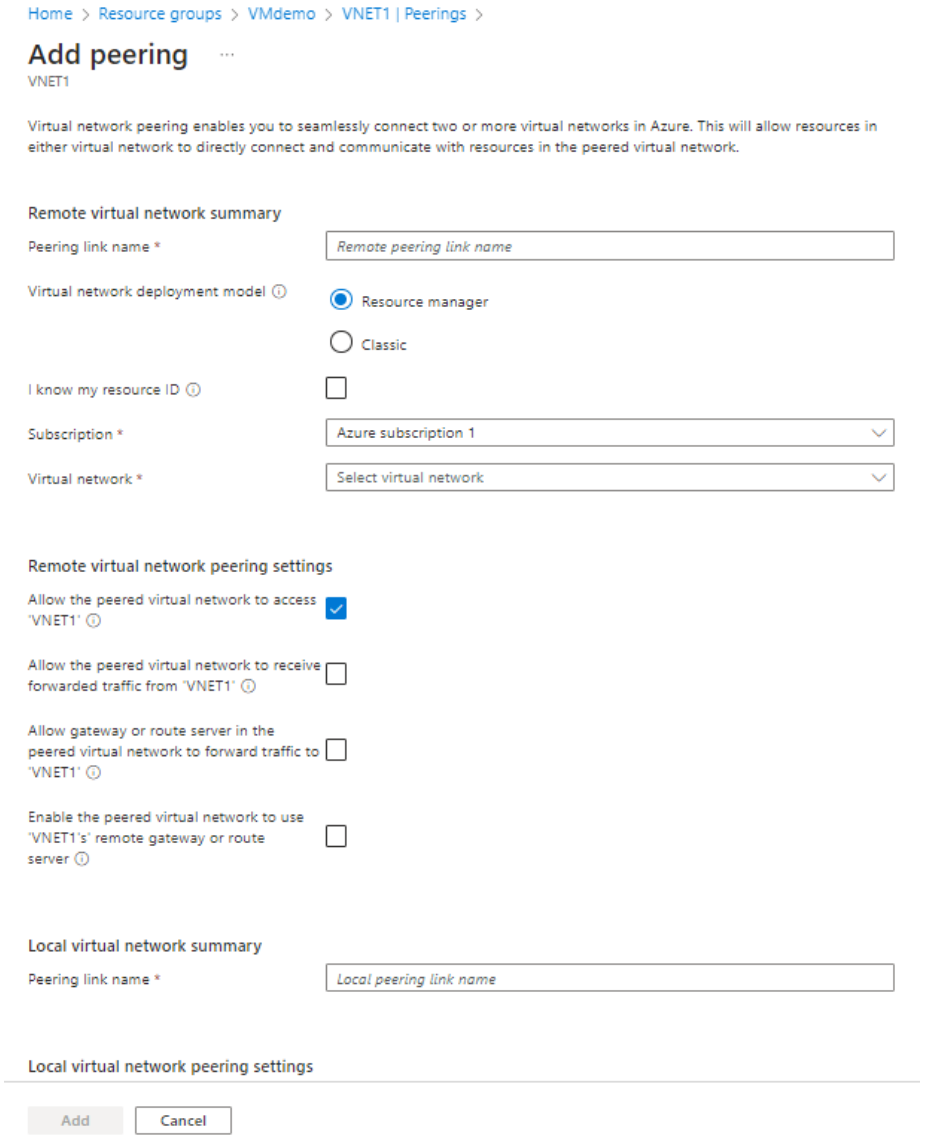


Трафік між віртуальними машинами в одноранговых віртуальних мережах використовує приватну інфраструктуру Azure. Як і трафік між віртуальними машинами в одній мережі, трафік направляється лише через приватну мережу Microsoft.



Віртуальна мережа може використовувати свій шлюз шлюз (VPN Gateway) для підключення до локальної мережі.
При цьому, також мати підключення до іншої віртуальної мережі типу VNET peering.

Vnet Peering-створення конфігурації



Peering link name – визначає імя зєднання, має бути визначено для 2-х напрямків 'vnet-1' -> 'vnet-2' і 'vnet-2' -> 'vnet-1'

Модель розгортання віртуальної мережі - Resource manager (визначає, модель розгортання якої було розгорнуто віртуальну мережу)

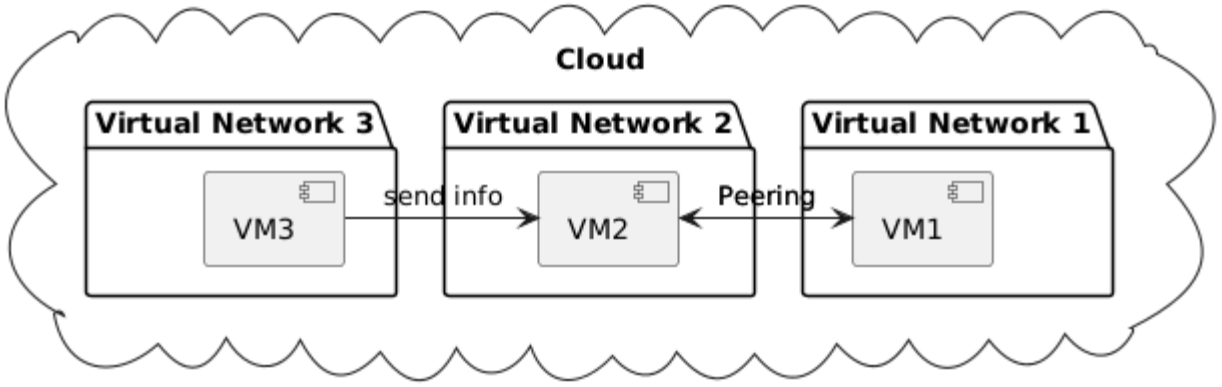
Я знаю свій ідентифікатор ресурсу - Якщо немає доступу на читання до віртуальної мережі або підписки, з якою втановлюється з'єднатися, тоді цей прапорець потрібен.

Віртуальна мережа – вказується та, з якою встановлюється з'єднання.

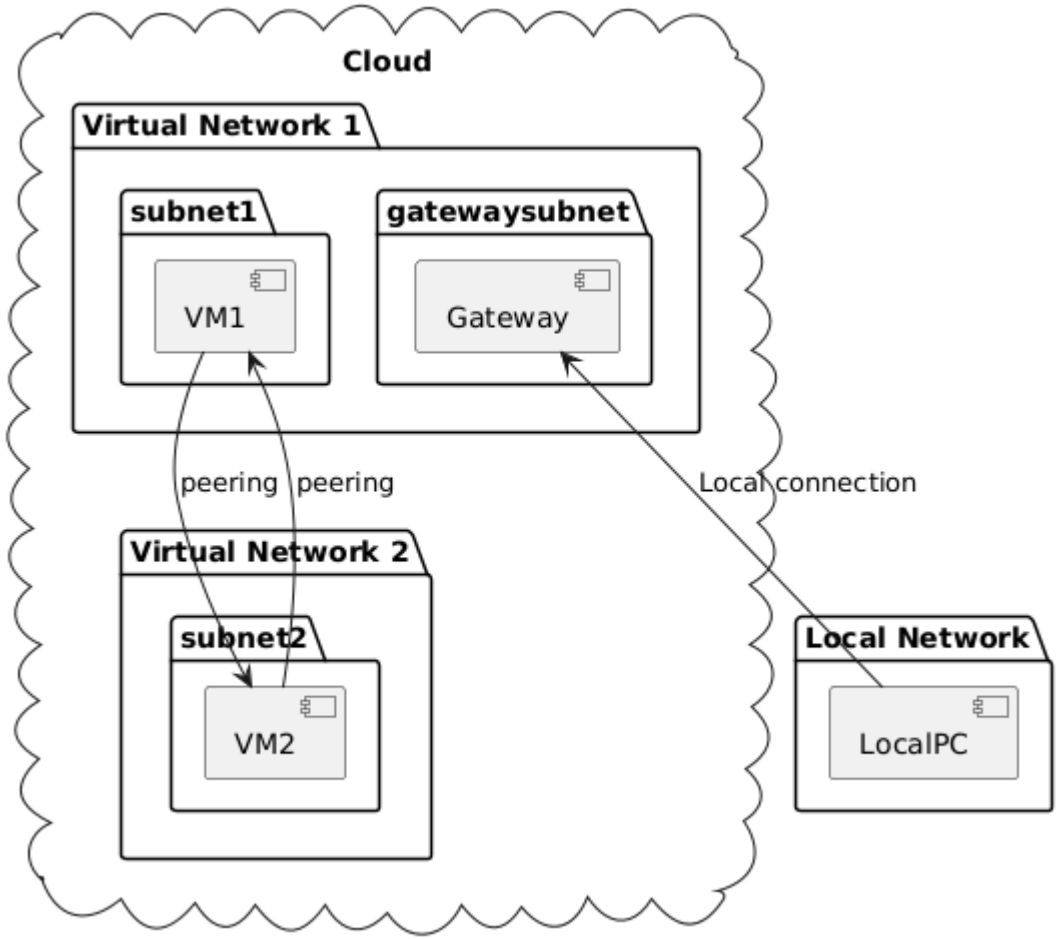
1. Allow the peered virtual network to access 'vnet-1' (Дозволити одноранговій віртуальній мережі доступ до «vnet-1») - параметр умикає зв'язок між концентратором і роз'ємом у топології мережі зі зв'язком і дозволяє віртуальній машині в одноранговій віртуальній мережі спілкуватися з віртуальною машиною у «vnet-1».
2. Allow the peered virtual network to receive forwarded traffic from 'vnet-1`

дозволить одноранговій віртуальній мережі 'vnet-2' отримувати трафік від віртуальних мереж, підключених до «vnet-1»

Наприклад, дані з Vnet3 введені в веб-сайт Vnet2 і передані на збереження Vnet1.



Vnet Peering-створення конфігурації



3. Allow gateway or route server in the peered virtual network to forward traffic to 'vnet-1' (Дозволити шлюзу або серверу маршрутизації у одноранговій віртуальній мережі «vnet-2» пересилати трафік до «vnet-1») - дозволить «vnet-1» отримувати трафік від шлюзу або сервера маршрутизації однорангових віртуальних мереж. Щоб увімкнути цей параметр, однорангова віртуальна мережа «vnet-2» повинна містити шлюз або сервер маршрутизації.

4. Enable the peered virtual network to use 'vnet-1's' remote gateway or route server (Увімкнути однорангову віртуальну мережу для використання віддаленого шлюзу або сервера маршрутизації «vnet-1») - Дозволити шлюзу або серверу маршрутизації у одноранговій віртуальній мережі «vnet-1» пересилати трафік до «vnet-2»

Розглянемо приклад

Переваги використання пірингу віртуальної мережі

1. Для однорангових віртуальних мереж ресурси будь-якої віртуальної мережі можуть безпосередньо з’єднуватися з ресурсами однорангової віртуальної мережі. Трафік між віртуальними машинами в однорангових віртуальних мережах направляється безпосередньо через магістральну інфраструктуру Microsoft, а не через шлюз або через загальнодоступний Інтернет.
2. Пропускна здатність мережі базується на пропускній здатності, дозволеній для віртуальної машини, пропорційній її розміру. Немає жодних додаткових обмежень щодо пропускної здатності в рамках пірингу.
3. Мережевий трафік між одноранговими віртуальними мережами є приватним. Ресурси будь-якої віртуальної мережі можуть безпосередньо з’єднуватися з ресурсами однорангової віртуальної мережі.
4. Піринг віртуальних мереж можливий для однорангових віртуальних мереж в одному регіоні або в різних регіонах. Піринг віртуальних мереж у різних регіонах також називають глобальним пірингом віртуальної мережі.
5. Коли віртуальна мережа є частиною пірингу, її неможливо перемістити до іншої групи ресурсів або підписки, - спочатку необхідно видалити одноранговий зв’язок, перемістити віртуальну мережу, а потім повторно створити одноранговий зв’язок.
6. Віртуальні мережі можуть бути в одній або різних підписках.
7. Піринги самі по собі не є транзитивними.

Якщо існує піринг між:
VirtualNetwork1 і VirtualNetwork2
VirtualNetwork2 і VirtualNetwork3

Тоді Немає з’єднання між
VirtualNetwork1 і VirtualNetwork3 через VirtualNetwork2.

Обмеження використання пірингу

Піринг віртуальних мереж можливий для Одноранговых віртуальних мереж в одному регіоні або в різних регіонах. Піринг віртуальних мереж у різних регіонах також називають глобальним пірингом віртуальної мережі.
Коли віртуальна мережа є частиною пірингу, її неможливо перемістити до іншої групи ресурсів або підписки, - спочатку необхідно видалити одноранговий зв’язок, перемістити віртуальну мережу, а потім повторно створити одноранговий зв’язок.
Віртуальні мережі можуть бути в одній або різних підписках.
Піринги самі по собі не є транзитивними.

Якщо існує піринг між:
VirtualNetwork1 і VirtualNetwork2
VirtualNetwork2 і VirtualNetwork3

Тоді Немає з’єднання між
VirtualNetwork1 і VirtualNetwork3 через VirtualNetwork2.

підключення «віртуальна мережа — віртуальна мережа»

Підключення «віртуальна мережа — віртуальна мережа» використовує VPN-шлюз для створення захищеного тунелю, який використовує IPsec/IKE протокол. Дозволяє з'єднувати дві або більше віртуальні мережі в Azure за допомогою VPN Gateway. Це забезпечує зашифроване з'єднання між мережами через тунель, що працює на основі протоколу IPSec.

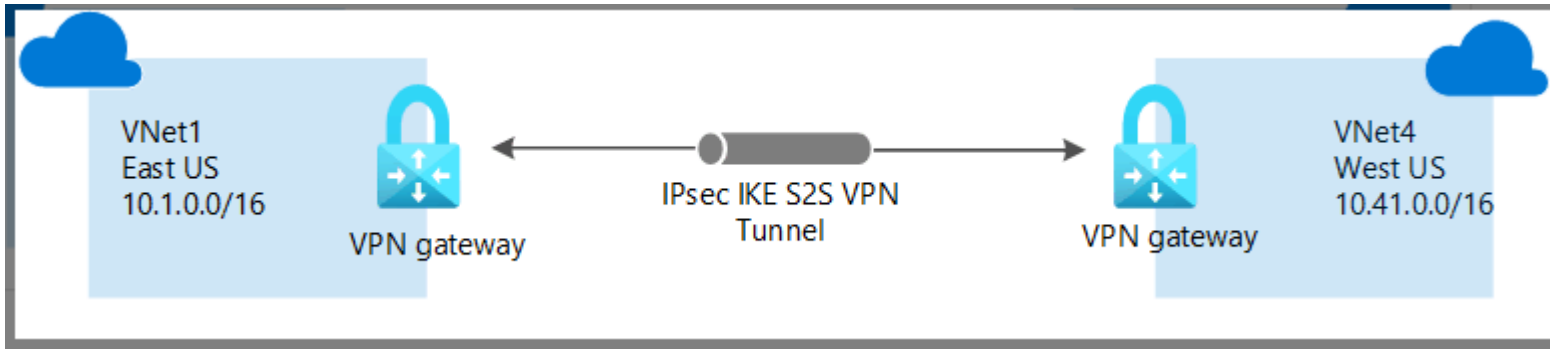
Основна відмінність від VNet Peering полягає в тому, що VNet Peering не шифрує трафік, але забезпечує швидке та безпечне з'єднання через приватну інфраструктуру Azure.

Сценарії використання

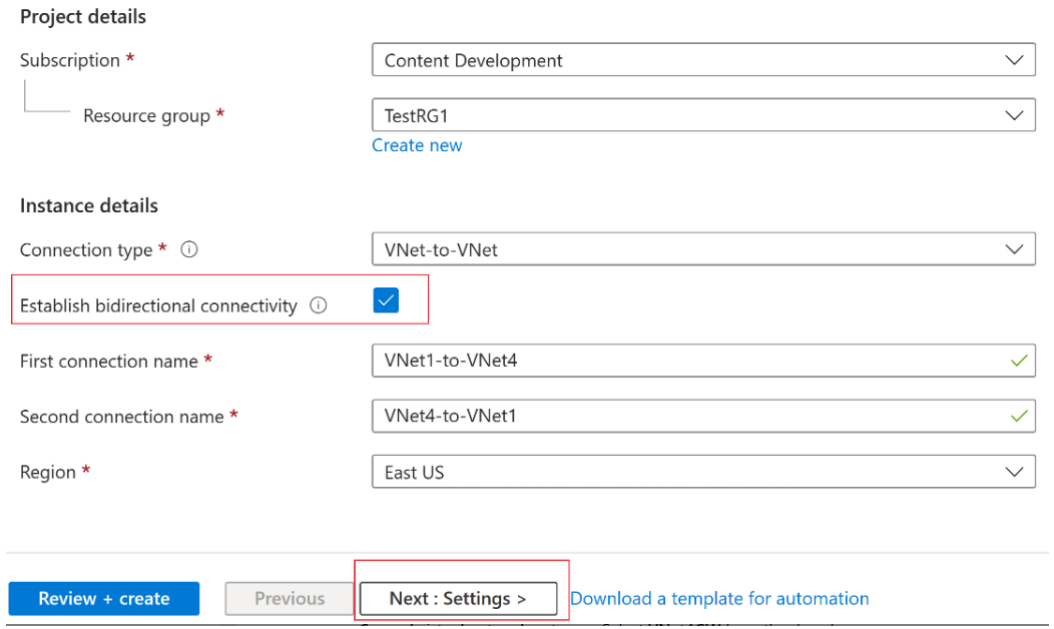
Використовується для з'єднання віртуальних мереж у різних регіонах з високим рівнем безпеки.

Використовується для розширення локальної інфраструктури в Azure через VPN-з'єднання.

Для створення резервних копій або розгортання служб у різних регіонах з безпечним з'єднанням між ними.



Розглянемо приклад



Визначне конфігурацію з’єднання типу «мережа - мережа» для Gateway

Схема з'єднання **ExpressRoute Circuit**

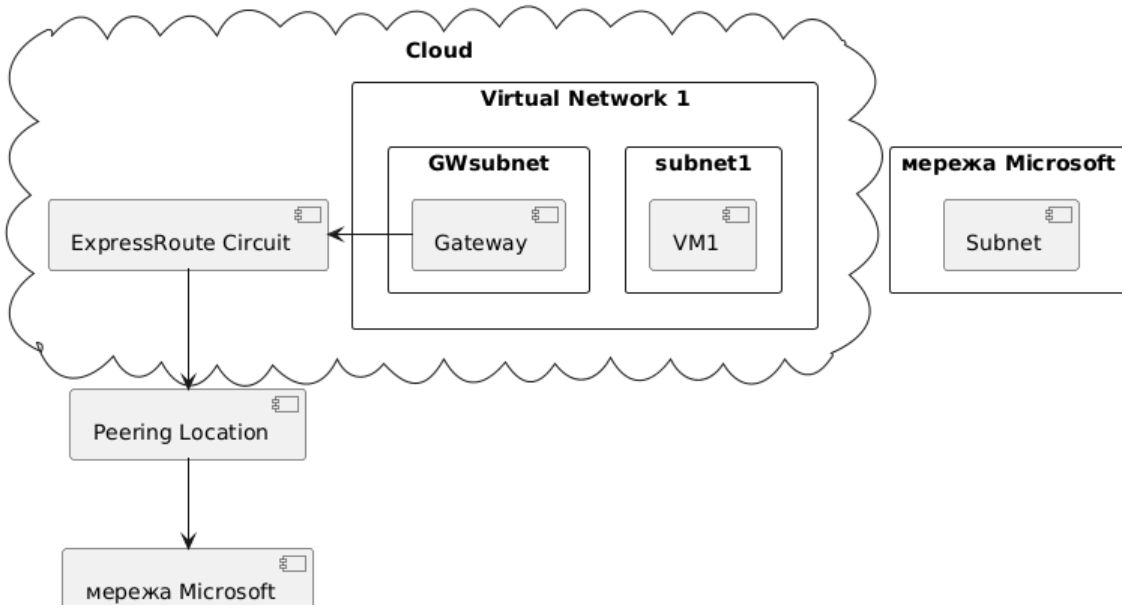
Схема з'єднання **ExpressRoute Circuit** від Microsoft Azure використовується для забезпечення приватного з'єднання між локальними мережами організації та хмарними сервісами Azure. Вона дозволяє підключатися до Azure безпосередньо, **минаючи публічний інтернет**

Основні компоненти з'єднання ExpressRoute Circuit:

1. **Локальна мережа (On-premises network)** – корпоративна інфраструктура.
2. **Мережевий провайдер (Connectivity Provider)** – ExpressRoute працює через провайдерів, які надають послуги зв'язку, такі як Ethernet або MPLS VPN.
3. **ExpressRoute Circuit** – Віртуальний канал, що забезпечує підключення між вашою локальною мережею і хмарними сервісами Azure через точки присутності (Point of Presence) вашого провайдера.

Кожен канал має фіксовану пропускну здатність (50 Мбіт/с, 100 Мбіт/с, 200 Мбіт/с, 500 Мбіт/с, 1 Гбіт/с, 2 Гбіт/с, 5 Гбіт/с, 10 Гбіт/с) і зіставляється з постачальником підключення та місцем пірингу.

Схема з'єднання



Peering location — це дата-центр або вузол телекомунікаційного провайдера, де відбувається фізичне підключення до мережі Microsoft. Це може бути інфраструктура постачальника послуг, наприклад, телеком-компанії або партнери Microsoft, які забезпечують доступ до мережі Azure через **ExpressRoute**.

Як вибрати Peering Location:

1.Місце розташування дата-центру або офісу:

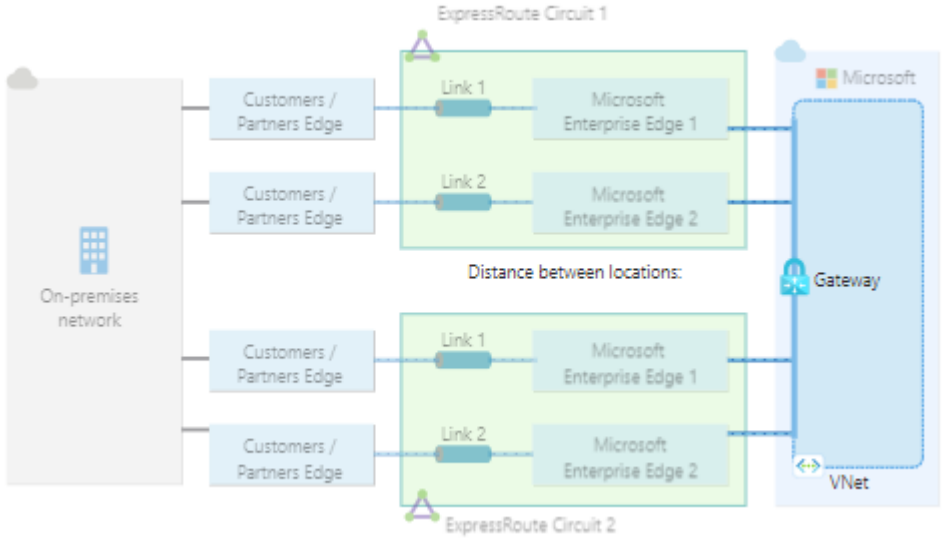
1. Виберіть найближчий **peering location**, щоб зменшити затримки між VNet1 та мережею Azure.
2. Перевірте, чи підтримує постачальник послуг потрібні вам **peering locations** і чи надає він необхідну пропускну здатність.
3. Для великих організацій з високими вимогами до продуктивності та надійності варто врахувати не лише фізичну близькість до **peering location**, а й здатність обробляти великі обсяги трафіку.

Роль постачальників послуг (Service Providers):

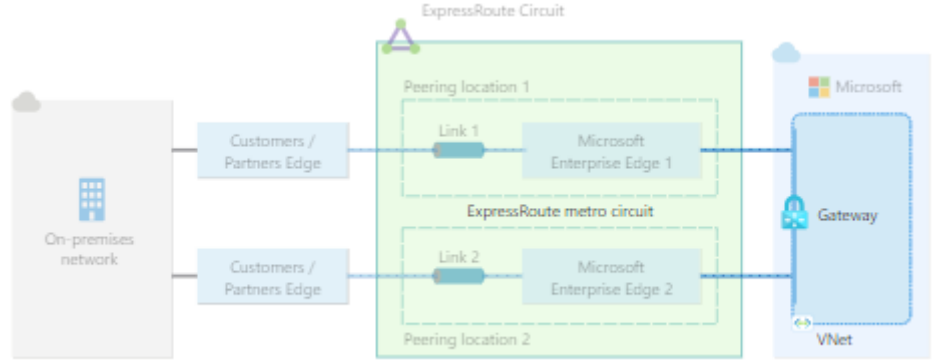
•Підключення до **peering location** через постачальника послуг (телекомунікаційну компанію, провайдера MPLS тощо), який організовує фізичне підключення до мережі Microsoft.

•Постачальники послуг мають свої точки доступу до мережі Microsoft у певних **peering locations**.

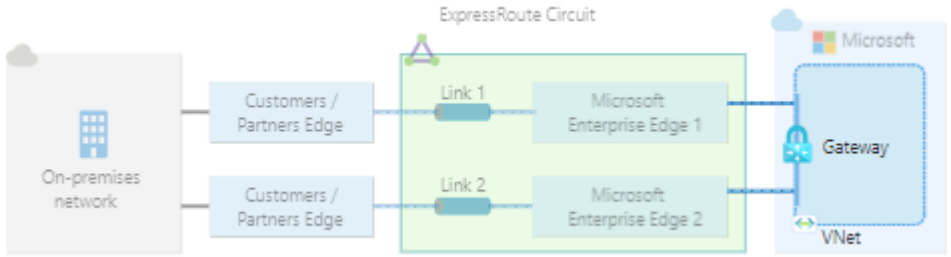
ExpressRoute Resiliency забезпечує надійність та стійкість з'єднання в інфраструктурі **Azure ExpressRoute**. Це досягається завдяки використанню резервних каналів і додаткових елементів інфраструктури, які дозволяють забезпечити безперебійність роботи



Максимальная стійкість
Geographic (2+2): Найбільш стійкий варіант, який передбачає два ExpressRoute Circuits, розміщені в різних регіонах. Це забезпечує максимальну відмовостійкість у випадку катастрофічних відмов в одному регіоні.



Висока стійкість
Два окремі ExpressRoute Circuits у двох різних точках підключення в одному регіоні для підвищення надійності



Стандартна стійкість - Один ExpressRoute Circuit з двома фізичними підключеннями в одному регіоні (локальне резервування).

Create ExpressRoute

Configuration Tags Review + create

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Establish connections to Azure at an ExpressRoute location, such as an Exchange provider facility, or directly connect to Azure from your existing WAN network, such as a multiprotocol label switching (MPLS) VPN, provided by a network service provider. Learn more about Express Route circuits

Project Details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure subscription 1

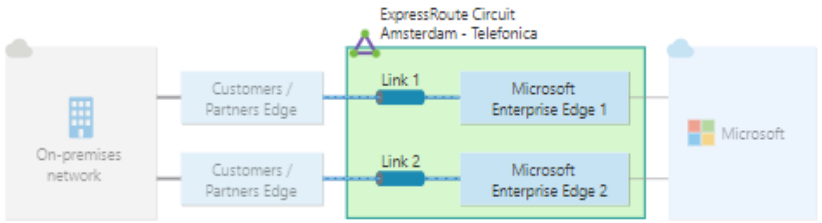
Resource group * : VMdemo

Create new

Resiliency

- ( ) Maximum Resiliency (Recommended): Resiliency across two or more distinct edge locations each with redundant physical links
- ( ) High Resiliency: Metro model offering resiliency across distinct edge locations each with single physical link
- (•) Standard Resiliency: Physical link redundancy within one edge location only

Does not protect against location-wide outages. Suitable for non-critical / non-production workloads.



Circuit Details

Region * : West Europe

Circuit name * : expressroute

Port type : (•) Provider ( ) Direct

Peering location * : Amsterdam

Provider * : Telefonica

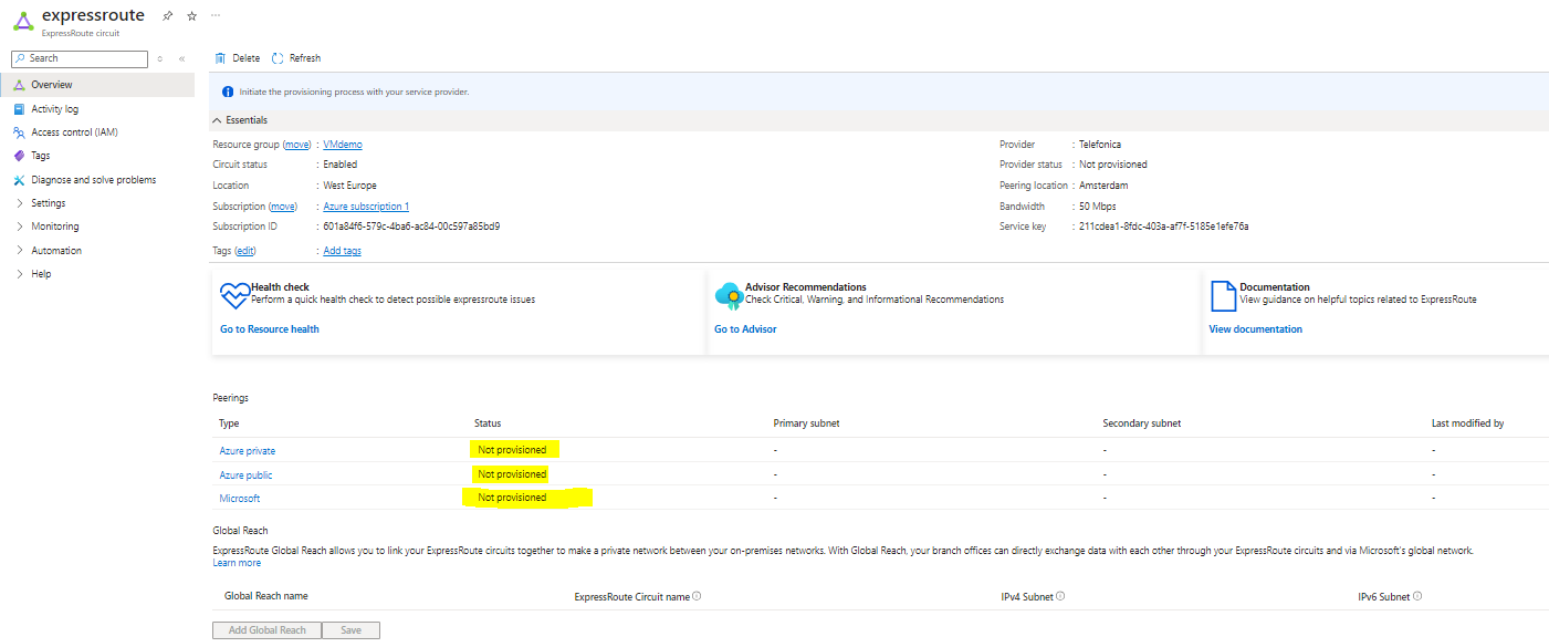
Bandwidth * : 50Mbps

SKU : ( ) Local (•) Standard ( ) Premium

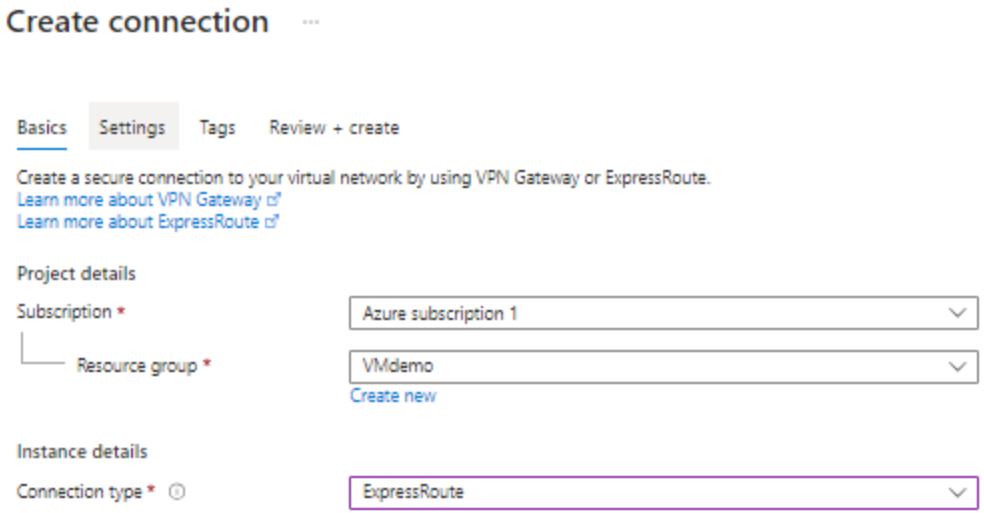
Billing model : (•) Metered ( ) Unlimited

Розглянемо приклад

Визначаємо конфігурацію з'єднання



Express



Підключення VPN-шлюзу типу "мережа - мережа" (S2S)

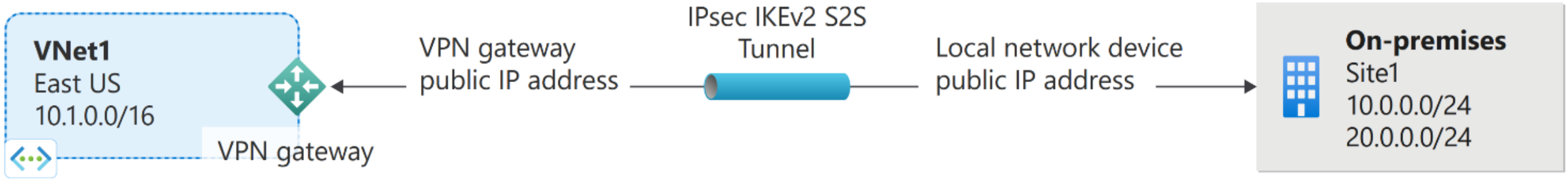
Підключення через VPN-тунель IPsec/IKE (IKEv1 або IKEv2), трафік VPN типу "мережа-мережа" проходить зашифрованим **через загальнодоступний Інтернет**. (принципова різниця між підключення “Vnet-peering”)

Підключення типу "мережа-мережа" можна використовувати для розподілених та гібридних конфігурацій.

Шлюз VPN можна налаштувати в режимі "активний - резервний" з однією загальнодоступною IP-адресою або в режимі "активний - активний" з двома загальнодоступними IP-адресами. У режимі "активний - резервний" завжди активний один тунель IPsec, а інший перебуває в режимі очікування. У цьому варіанті трафік проходить через активний тунель і перемикається на резервний лише у випадку, якщо виникла проблема з основним тунелем.

Рекомендованим є режим "активний - активний", в якому обидва тунелі IPsec одночасно активні і дані передаються через обидва тунелі. Додаткова перевага режиму "активний - активний" полягає в тому, що клієнти отримують більш високу пропускну здатність.

У шлюзі віртуальної мережі можна створити кілька VPN-підключень, як правило, до різних локальних сайтів. Під час роботи з кількома підключеннями слід використовувати тип VPN "RouteBased" (динамічний шлюз для роботи з класичними віртуальними мережами).



Конфігурація підключення типу «мережа – мережа»

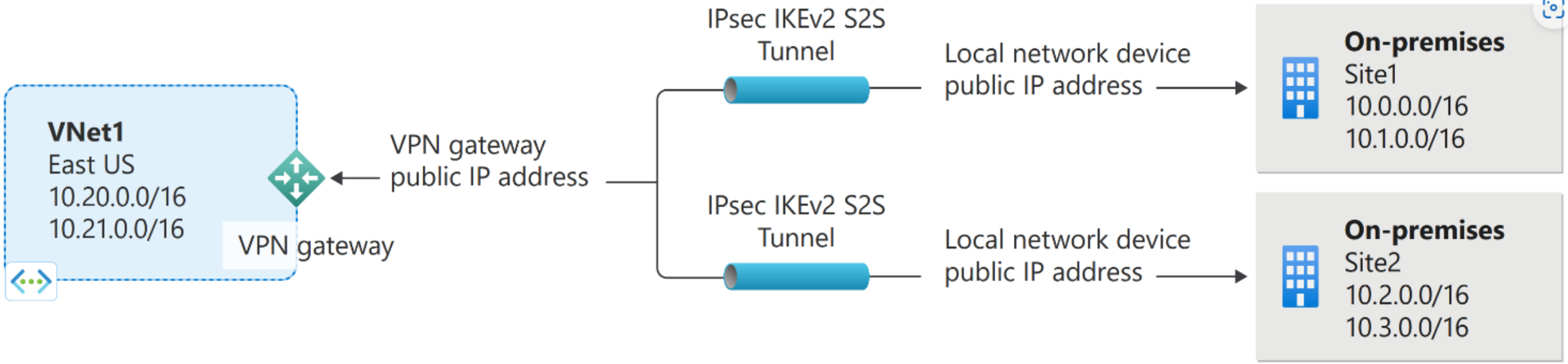
Підключення VPN-шлюзу типу "мережа - мережа" (S2S) - це підключення через VPN-тунель IPsec/IKE (IKEv1 або IKEv2). Підключення типу "мережа-мережа" можна використовувати для розподілених та гібридних конфігурацій.

Шлюз VPN можна налаштувати в режимі "активний - резервний" з однією загальнодоступною IP-адресою або в режимі "активний - активний" з двома загальнодоступними IP-адресами. У режимі "активний - резервний" завжди активний один тунель IPsec, а інший перебуває в режимі очікування. У цьому варіанті трафік проходить через активний тунель і перемикається на резервний лише у випадку, якщо виникла проблема з основним тунелем.

Рекомендованим є режим "активний - активний", в якому обидва тунелі IPsec одночасно активні і дані передаються через обидва тунелі. Додаткова перевага режиму "активний - активний" полягає в тому, що клієнти отримують більш високу пропускну здатність.

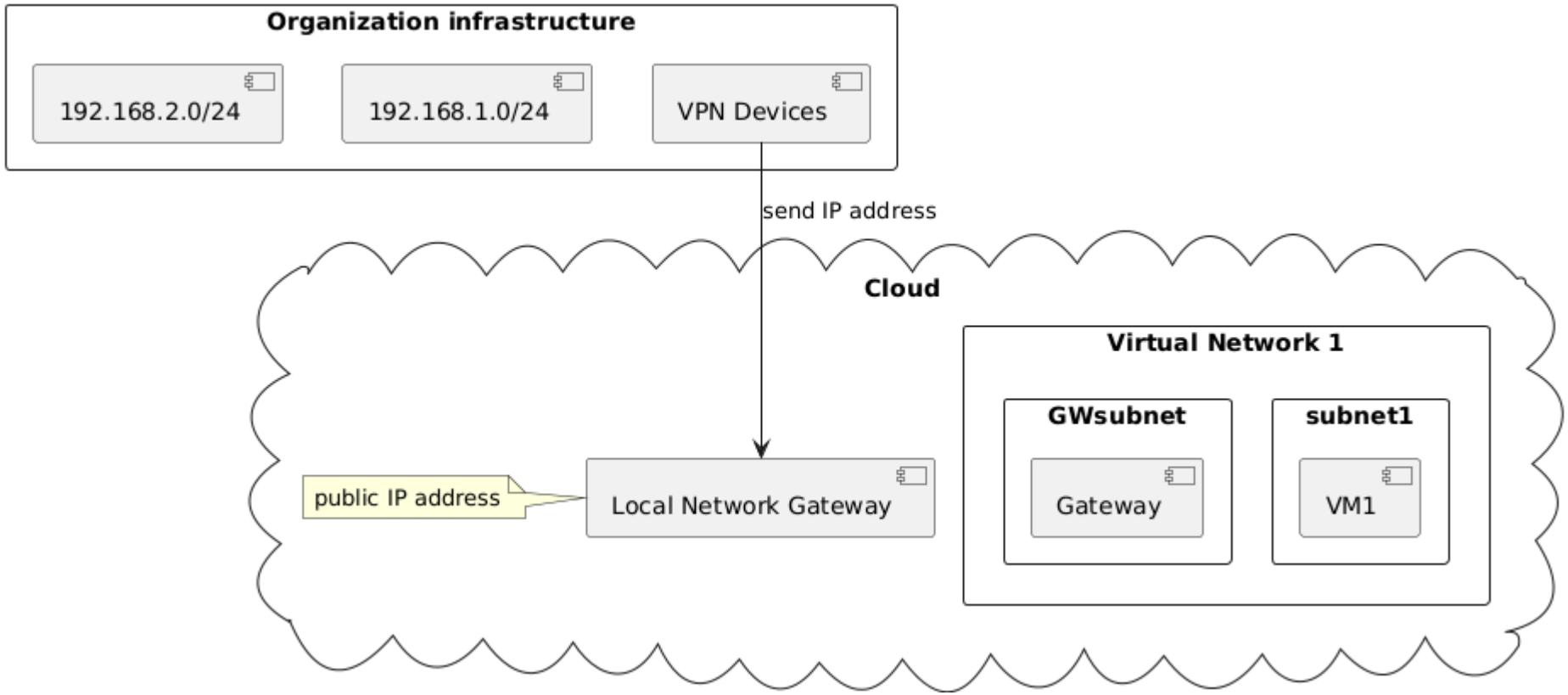
У шлюзі віртуальної мережі можна створити кілька VPN-підключень, як правило, до різних локальних сайтів. Під час роботи з кількома підключеннями слід використовувати тип VPN "RouteBased" (динамічний шлюз для роботи з класичними віртуальними мережами).

Трафік VPN типу "мережа-мережа" проходить зашифрованим через загальнодоступний Інтернет

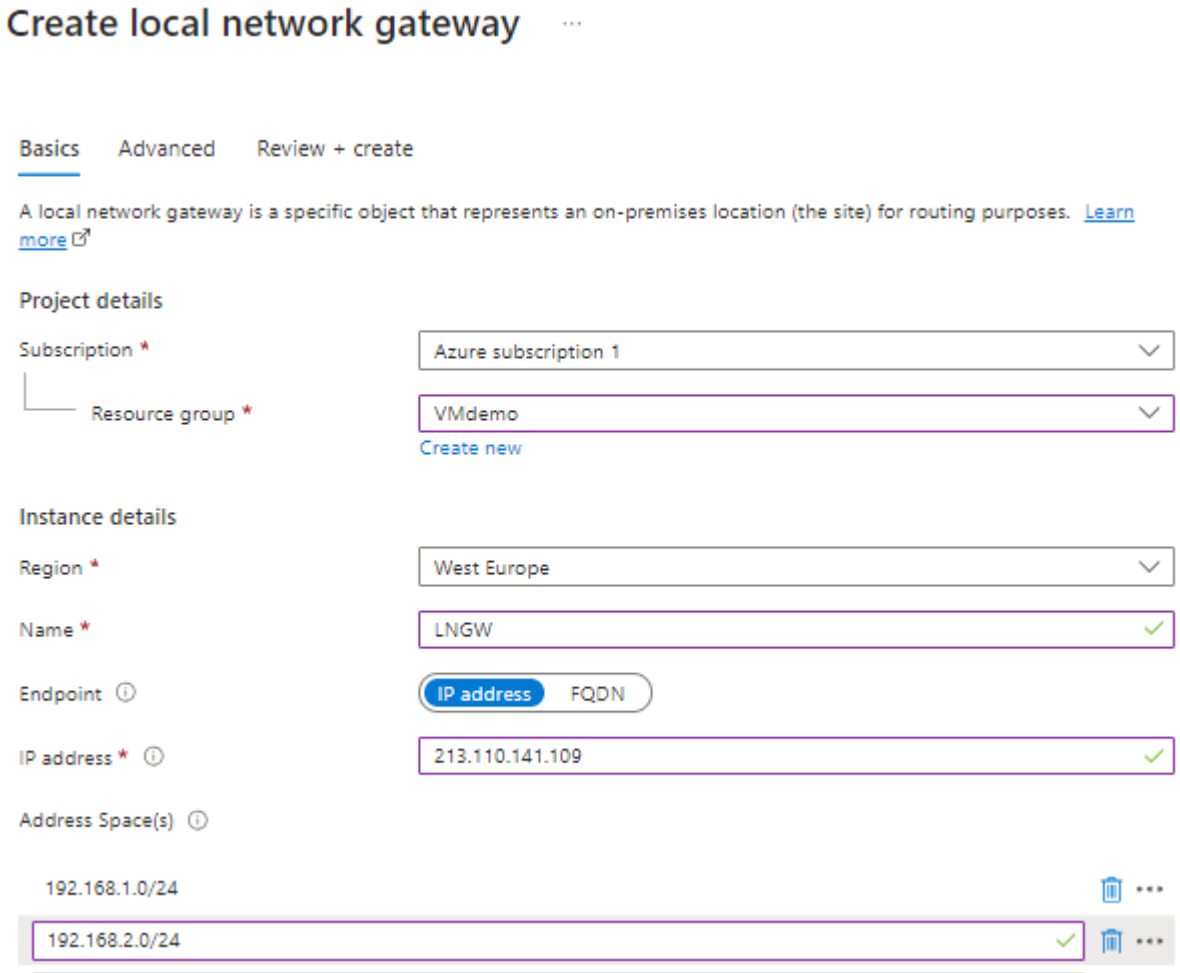


Підключення типу «мережа – мережа»

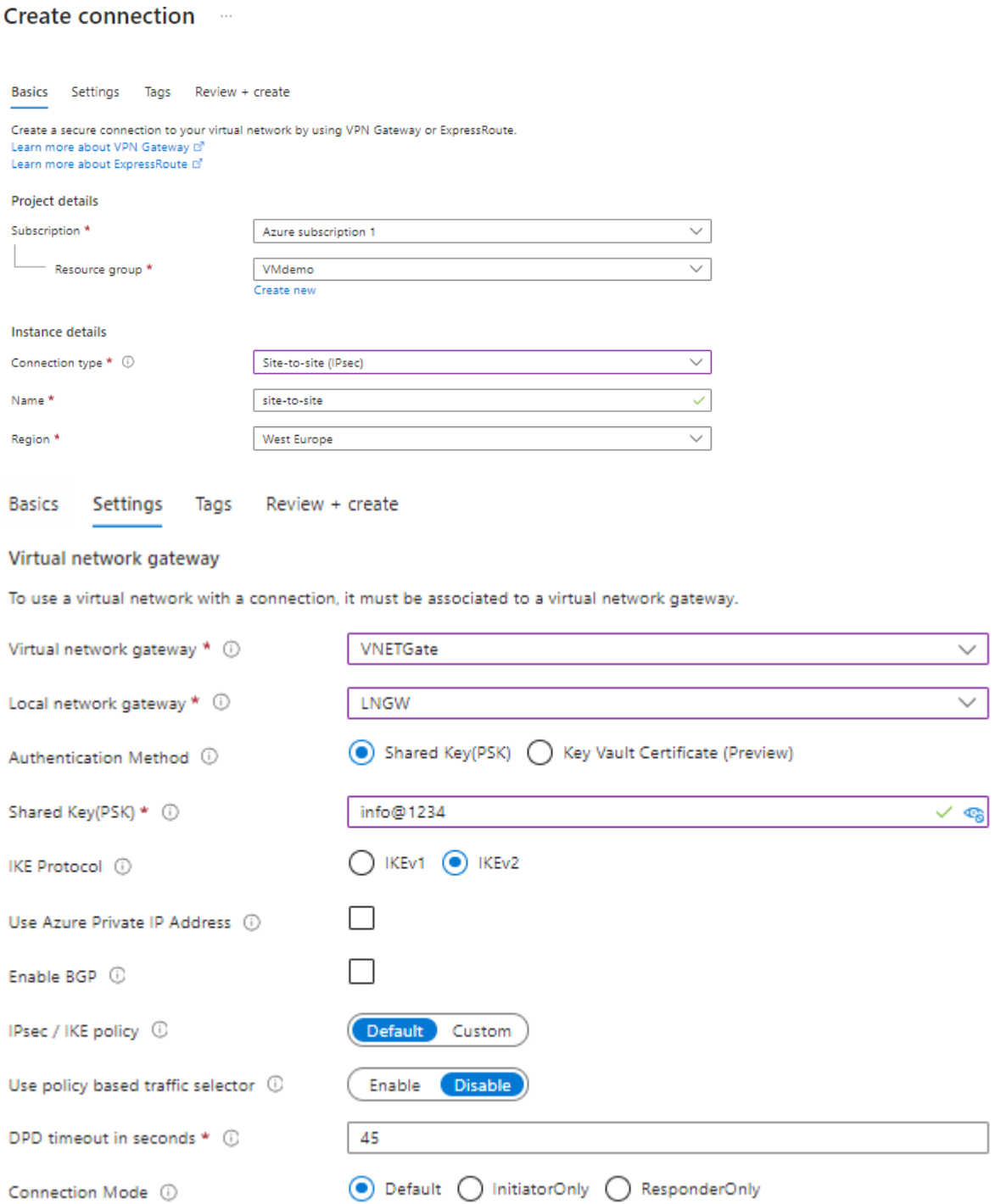
Конфігурація вимає налаштування ресурсів Azure: віртуальну мережу, підмережу (sub-net) з віртуальною машиною; підмережу типу Gate-way, яка включає ресурс Gateway та Local NetworkGateway.
Конфігурація вимає налаштування налаштування локальних пристроїв VPN (VPN Devices) за межами Azure.



Створіть ресурс Local network gateway



IP address – ваша загальна доступна IP адреса
https://whatismyipaddress.com/
213.110.141.109
Address Space (s) - IP адреси в мережі організації

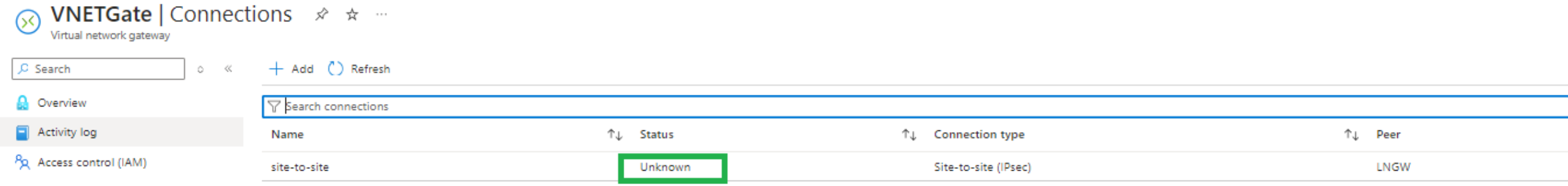


Створіть з'єднання Site-to-Site (iPsec)

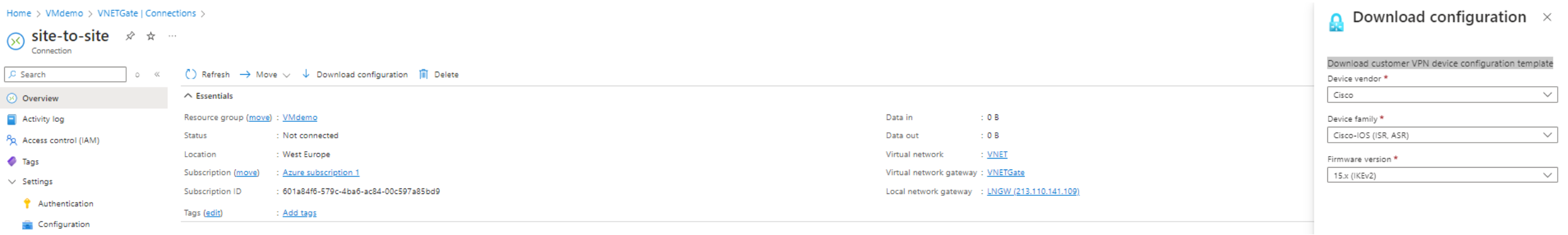
Authentication Method – shared Key (PSK) – спільний ключ з'єднання, для Azure мережі та мережі Організації
IKE Protocol – IKEv2
IKEv1:менш безпечний через обмеження у деяких реалізаціях і складніший процес налаштування. Для встановлення з'єднання використовується два етапи (фази). Спочатку проводиться аутентифікація, а потім створюються захищені сеанси передачі даних.
IKEv2: Більш безпечний, оскільки використовує вдосконалені механізми захисту, меншу кількість повідомлень для встановлення з'єднання та кращі алгоритми шифрування. Процес обміну ключами уніфікований і здійснюється в одній фазі.

Отримайте сценарій конфігурації створеного зв'язку типу "site-to-site"

Статус з'єднання не визначений через відсутність конфігурації з'єднання за межами Azure.



Синтаксис для кожного сценарію конфігурації VPN-пристроїв відрізняється і сильно залежить від моделей і версій мікропрограми.



Визначте, як треба до визначити сценарій конфігурації створеного зв'язку типу "site-to-site"

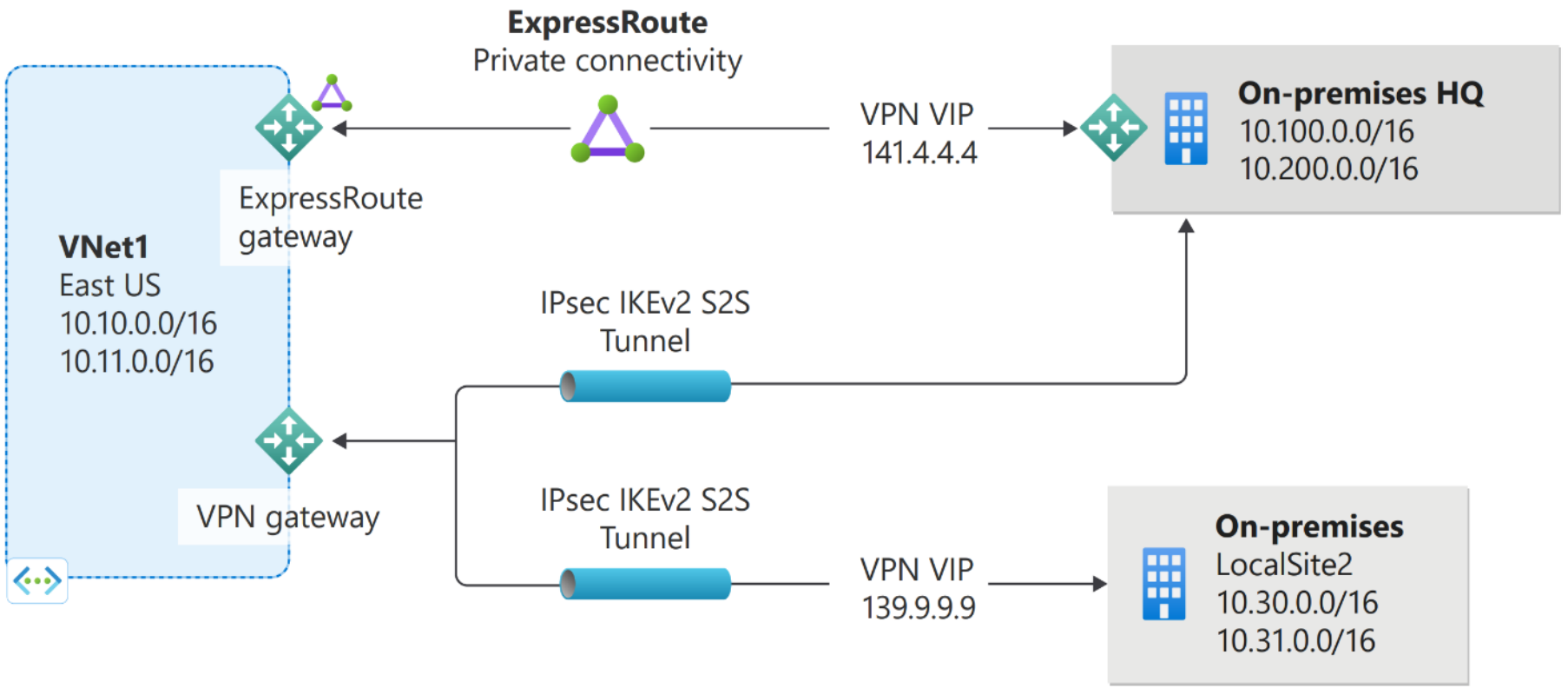
```
120
121  crypto ipsec transform-set site-to-site-TransformSet esp-gcm 256
122    mode tunnel
123    exit
124
125  crypto ipsec profile site-to-site-IPsecProfile
126    set transform-set  site-to-site-TransformSet
127    set ikev2-profile  site-to-site-profile
128    set security-association lifetime seconds 3600
129    exit
130
131  ! ----------------------------------------------------------------------------
132  ! Tunnel interface (VTI) configuration
133  ! - Create/configure a tunnel interface
134  ! - Configure an APIPA (169.254.x.x) address that does NOT overlap with any
135  !   other address on this device. This is not visible from the Azure gateway.
136  ! * REPLACE: Tunnel interface numbers and APIPA IP addresses below
137  ! * Default tunnel interface 11 (169.254.0.1) and 12 (169.254.0.2)
138
139  int tunnel 11
140    ip address 169.254.0.1 255.255.255.255
141    tunnel mode ipsec ipv4
```

```
Search results - (5 hits)
Search "Replace" (5 hits in 1 file of 1 searched) [Normal]
  C:\Users\XIAOMI\Downloads\untitled file.txt (5 hits)
    Line   7: ! !!! Search for "REPLACE" to find the values that require special
    Line  75: ! [REPLACE] access-list number: access-list 101
    Line 136: ! * REPLACE: Tunnel interface numbers and APIPA IP addresses below
    Line 152: ! * REPLACE: Tunnel interface number(s), default tunnel 11 and tunnel 12
    Line 163: ! [REPLACE] Interfaces: Loopback 11, Tunnel 11, Tunnel 12; access-list 101
```

! [REPLACE] access-list number: access-list 101
! * REPLACE: Tunnel interface numbers and APIPA IP addresses below

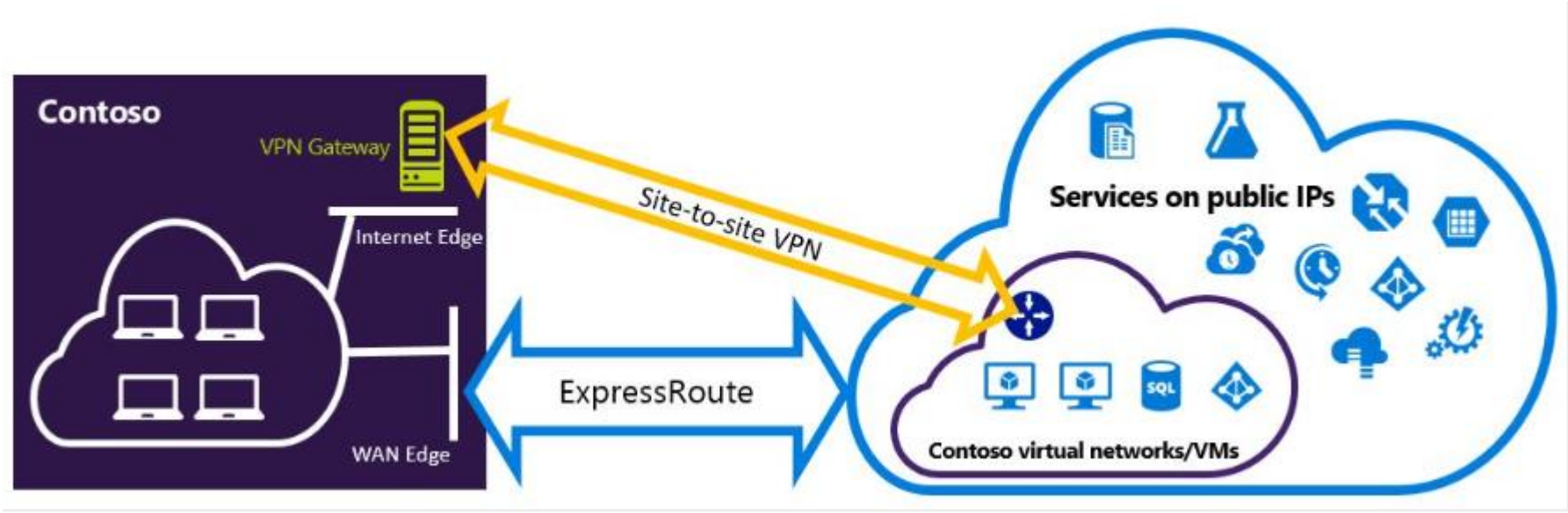
Конфігурація паралельного підключення типу «точка-мережа» і ExpressRout

Налаштування паралельних VPN-підключень типу "мережа-мережа" та ExpressRoute дає ряд переваг.
VPN типу "мережа-мережа" можна налаштувати як безпечний шлях відпрацювання відмови для ExpressRoute.
VPN типу "мережа-мережа" можна використовувати для підключення до сайтів, які не підключені через ExpressRoute.



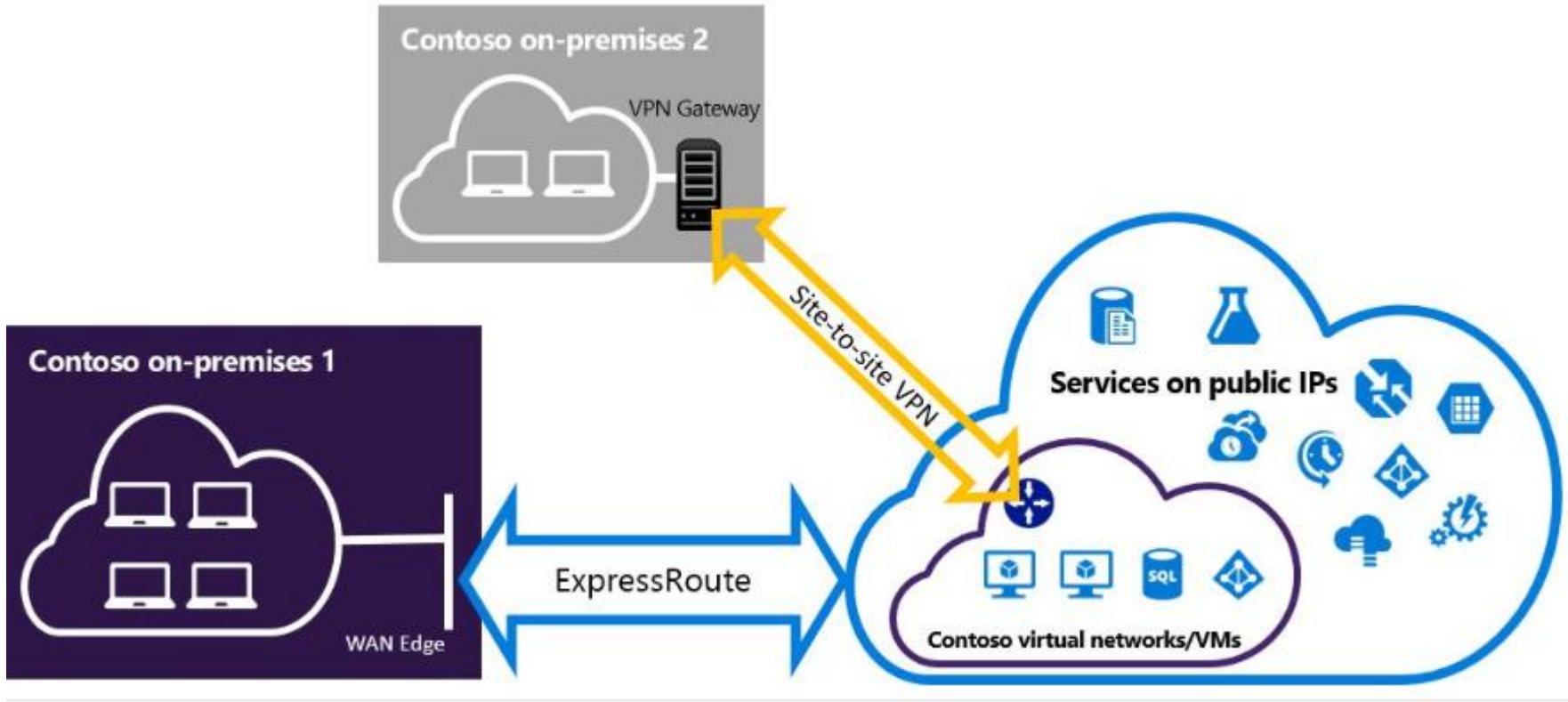
Конфігурація паралельного підключення для відпрацювання безпечного шляху відпрацювання відмови для ExpressRoute

Канал ExpressRoute завжди є основним посиланням.
Дані передаються шляхом VPN "мережа — мережа", тільки якщо канал ExpressRoute не справляється з цим завданням.
Щоб уникнути асиметричної маршрутизації, каналу ExpressRoute – повинен мати перевагу (більший локальний пріоритет) порівняно з шляхом VPN "мережа — мережа.



Конфігурація паралельного підключення для до сайтів, які не підключені через ExpressRoute

Мережі можна налаштувати таким чином, щоб одні з них підключалися безпосередньо до Azure за VPN типу "мережа-мережа", а інші через ExpressRoute.



Групи безпеки для перевірки трафіку

- У групах безпеки мережі використовуються правила, щоб дозволяти чи забороняти трафік по мережі. Кожне правило визначає вихідну та кінцеву адресу (або діапазон), протокол, порт (або діапазон), напрямок (вхідний або вихідний), числовий пріоритет і дозвіл або заборону трафіку, який відповідає правилу. Нижче наведено правила «1» та «2» які застосовуються для груп безпеки підмережі 1 та 2, та правила «A» та «B» що застосовуються на рівнях інтерфейсу мережі.
- Для вхідного трафіку Azure обробляє групу безпеки, пов'язану з підмережею тобто відповідно правил «1» та «2», а потім групу безпеки, що застосовується до мережного інтерфейсу тобто за правилами «A» та «B». Вихідний трафік обробляється у зворотному порядку (спочатку мережний інтерфейс, потім підмережа).
- Групи безпеки є необов'язковими. Якщо група безпеки не застосовується, Azure дозволяє весь трафік. Якщо віртуальна машина має загальнодоступну IP-адресу, це може становити серйозну загрозу, особливо якщо операційна система не надає брандмауера.