Лабораторна робота №5

РОБОТА З МЕРЕЖЕВИМИ СЕРВІСАМИ AZURE: AZURE VIRTUAL NETWORK, NETWORK SECURITY GROUP, AZURE DNS, VIRTUAL NETWORK PEERING, NETWORK VIRTUAL APPLIANCE

Мета: ознайомитися з основними мережевими сервісами платформи Microsoft Azure та навчитися створювати, налаштовувати й аналізувати хмарну мережеву інфраструктуру. Дослідити принципи побудови віртуальних мереж (Virtual Network) і планування їх адресного простору, створення підмереж (Subnets), груп безпеки мережі (Network Security Group) та груп безпеки застосунків (Application Security Group) для контролю трафіку. Навчитися налаштовувати публічні та приватні зони Azure DNS, з'єднувати віртуальні мережі за допомогою Virtual Network Peering, керувати маршрутизацією трафіку за допомогою користувацьких маршрутів (User-defined routes) та спрямовувати трафік через мережевий віртуальний пристрій (Network Virtual Appliance).

Теоретичні відомості

Azure Virtual Network та адресний простір

Azure Virtual Network (VNet) – базовий будівельний блок приватної мережі в Azure, що забезпечує взаємодію ресурсів Azure (віртуальних машин, кластерів Kubernetes, приватних кінцевих точок тощо) між собою, з Інтернетом та з локальними мережами. Віртуальна мережа створюється в межах одного регіону та однієї Subscription, а її обов'язковими параметрами є ім'я, Resource group, регіон та адресний простір (address space).

Адресний простір задається одним або кількома префіксами в нотації CIDR (Classless Inter-Domain Routing). Як правило, використовуються приватні діапазони, визначені RFC 1918: `10.0.0.0/8`, `172.16.0.0/12` та `192.168.0.0/16`. Довжина префікса визначає, скільки старших бітів адреси

є незмінними для всієї мережі: для префікса /16 фіксованими є перші два октети, тому мережа 10.5.0.0/16 охоплює адреси від 10.5.0.0 до 10.5.255.255. Отже, записи 10.5.15.0/16 та 10.5.115.0/16 описують одну й ту саму мережу 10.5.0.0/16, а адресний простір має задаватися адресою, вирівняною за довжиною префікса.

Адресний простір віртуальної мережі розподіляється між підмережами (Subnets). Кожна підмережа займає частину адресного простору VNet і не може перетинатися з іншими підмережами. У кожній підмережі Azure резервує п’ять адрес: адресу мережі (x.x.x.0), адресу шлюзу за замовчуванням (x.x.x.1), дві адреси для зіставлення DNS-сервісу Azure (x.x.x.2, x.x.x.3) та широкомовну адресу (x.x.x.255 для підмережі /24). Тому перша адреса, яку отримує ресурс у підмережі, – x.x.x.4.

Планування адресного простору має враховувати майбутні з’єднання: віртуальні мережі, які з’єднуються між собою (за допомогою Virtual Network Peering чи VPN) або з локальною мережею організації, не повинні мати адресних просторів, що перетинаються (overlap). Змінити адресний простір після підключення ресурсів складно, тому діапазони варто розподіляти заздалегідь.

Network Security Group та Application Security Group

Network Security Group (NSG) – набір правил безпеки, що дозволяють або забороняють вхідний (inbound) та вихідний (outbound) мережевий трафік. NSG асоціюється з підмережею або мережевим інтерфейсом (NIC) віртуальної машини. Кожне правило містить такі параметри: ім’я, пріоритет (від 100 до 4096), джерело та призначення (IP-адреса або діапазон, service tag чи Application Security Group), діапазони портів, протокол (TCP, UDP, ICMP або Any) та дію (Allow або Deny). Правила обробляються в порядку зростання пріоритету: щойно трафік відповідає правилу, обробка

припиняється, тому правило з меншим числовим значенням пріоритету має перевагу. NSG працює як stateful-фільтр: для дозволеного з'єднання зворотний трафік дозволяється автоматично.

Кожна NSG містить стандартні правила (табл. 1), які неможливо видалити, проте можна перевизначити власними правилами з меншим значенням пріоритету.

Таблиця 1

Стандартні правила Network Security Group

Напрям	Ім'я правила	Пріоритет	Джерело → призначення	Дія
Inbound	AllowVnetInBound	65000	VirtualNetwork → VirtualNetwork	Allow
Inbound	AllowAzureLoadBalancerInBound	65001	AzureLoadBalancer → Any	Allow
Inbound	DenyAllInBound	65500	Any → Any	Deny
Outbound	AllowVnetOutBound	65000	VirtualNetwork → VirtualNetwork	Allow
Outbound	AllowInternetOutBound	65001	Any → Internet	Allow
Outbound	DenyAllOutBound	65500	Any → Any	Deny

Service tag – іменована група IP-префіксів певної служби, якою керує Microsoft, наприклад, `Internet`, `VirtualNetwork`, `AzureLoadBalancer` чи `Storage`. Service tags дають змогу не вказувати конкретні IP-адреси в правилах.

Application Security Group (ASG) дає змогу групувати мережеві інтерфейси віртуальних машин за їх роллю (наприклад, вебсервери чи сервери баз даних) та використовувати такі групи як джерело або призначення в правилах NSG замість IP-адрес. Під час додавання нової віртуальної машини до ASG на неї автоматично поширюються відповідні правила, тому ASG доцільно використовувати, коли набір віртуальних машин однакової ролі змінюється.

Azure DNS: публічні та приватні зони

Azure DNS – служба хостингу DNS-зон на інфраструктурі Microsoft. **Публічна DNS-зона** (DNS zone) містить записи (record sets) домену,

доступні з Інтернету. Azure DNS не реєструє домени: домен реєструється в реєстратора, після чого в налаштуваннях домену в реєстратора як NS-сервери вказуються чотири сервери імен Azure DNS (наприклад, `ns1-06.azure-dns.com`, `ns2-06.azure-dns.net`, `ns3-06.azure-dns.org`, `ns4-06.azure-dns.info`). Цей процес називається делегуванням домену. Зміни делегування поширюються протягом часу, що визначається значеннями TTL відповідних записів.

Приватна DNS-зона (Private DNS zone) забезпечує розв'язання імен лише всередині віртуальних мереж, пов'язаних із зоною за допомогою virtual network link. Якщо для зв'язку ввімкнено **auto registration**, мережа стає registration virtual network: для кожної віртуальної машини в ній автоматично створюється A-запис, який видаляється після зупинки чи видалення машини. Без auto registration мережа є resolution virtual network і може лише розв'язувати записи зони. Одна віртуальна мережа може мати лише одну зону з увімкненою auto registration. Запити до приватних зон обробляє DNS-сервіс Azure за адресою `168.63.129.16`, тому з-за меж пов'язаних віртуальних мереж (наприклад, з Azure Cloud Shell чи локального комп'ютера) записи приватної зони не розв'язуються.

Virtual Network Peering

Virtual Network Peering з'єднує дві віртуальні мережі так, що ресурси в них взаємодіють через магістральну мережу Microsoft з низькою затримкою, без шлюзів, публічних IP-адрес та шифрування на рівні VPN. Розрізняють peering у межах одного регіону та global peering між регіонами. Peering створюється в обох напрямках: в Azure Portal обидва зв'язки створюються однією операцією, а в Azure CLI кожен зв'язок створюється окремою командою; з'єднання працює, коли обидва зв'язки мають стан **Connected**. Peering не є транзитивним: якщо мережа A з'єднана з B, а B – з

C, мережі A та C не взаємодіють без окремого peering. Адресні простори з'єднуваних мереж не повинні перетинатися.

Маршрутизація, User-defined routes та Network Virtual Appliance

Azure автоматично створює системні маршрути (system routes) для кожної підмережі: трафік у межах віртуальної мережі та до пов'язаних через peering мереж передається напряму, а трафік до Інтернету – через інфраструктуру Azure. Для зміни стандартної поведінки створюється таблиця маршрутів (route table) з користувацькими маршрутами (User-defined routes, UDR), яка асоціюється з однією або кількома підмережами. Маршрут містить префікс призначення та тип наступного переходу (next hop type): **Virtual network gateway**, **Virtual network**, **Internet**, **Virtual appliance** (з IP-адресою пристрою) або **None** (трафік відкидається). Якщо до адреси призначення підходять кілька маршрутів, обирається маршрут з найдовшим префіксом (longest prefix match), а за однакової довжини користувацькі маршрути мають перевагу над системними.

Network Virtual Appliance (NVA) – віртуальна машина, що виконує мережеві функції: міжмережевий екран, маршрутизатор, систему виявлення вторгнень, WAN-оптимізатор тощо. Щоб NVA могла пересилати пакети, адресовані іншим вузлам, переадресацію IP (IP forwarding) необхідно ввімкнути двічі: на мережевому інтерфейсі в Azure та в операційній системі віртуальної машини. Користувацький маршрут з next hop type Virtual appliance спрямовує трафік підмережі через NVA, наприклад, для інспекції трафіку між публічною та приватною підмережами через периметрову мережу (DMZ).

Azure Load Balancer та Azure Application Gateway

Azure Load Balancer розподіляє вхідний трафік між віртуальними машинами на транспортному рівні (рівень 4 моделі OSI, протоколи TCP та UDP) за правилами балансування та перевірками стану (health probes).

Може бути публічним або внутрішнім; рекомендованим є SKU Standard. Azure Application Gateway – балансувальник навантаження вебтрафіку на прикладному рівні (рівень 7 моделі OSI, протоколи HTTP та HTTPS), який підтримує маршрутизацію за шляхом URL та іменем хоста, завершення TLS (TLS termination), прив'язку сеансів та Web Application Firewall (WAF).

Azure Network Watcher

Azure Network Watcher – набір інструментів для моніторингу та діагностики мережевої інфраструктури Azure. Серед них: **IP flow verify** (перевіряє, чи дозволяють правила NSG пакет між заданими адресою та портом), **Next hop** (визначає наступний перехід маршруту для пакета від віртуальної машини), **Connection troubleshoot** (перевіряє з'єднання між джерелом і призначенням), **Connection monitor** (безперервно відстежує доступність і затримку) та **flow logs** (журналювання IP-трафіку). Network Watcher вмикається автоматично в регіоні під час створення першої віртуальної мережі, а його ресурси розміщуються в Resource group `NetworkWatcherRG`.

Хід роботи

У завданнях використовуються такі позначення: **xxx** – скорочена назва обраного регіону серед доступних у політиці Allowed resource deployment regions відповідно до цього файлу, що містить відповідність між повною та скороченою назвою регіону; **yyy** – ініціали студента латинськими літерами; **zzz** – номер варіанту з трьох цифр (наприклад, для 15 варіанту – 015). Скорочення типів ресурсів в іменах відповідають рекомендаціям Cloud Adoption Framework. Усі ресурси та Resource groups створюються в одному регіоні, обраному в кроці 1.1. Адресні простори віртуальних мереж та підмереж обираються згідно з номером варіанту з табл. 2–4. Звіт має містити скріншоти та виведення команд, що підтверджують виконання кожного кроку.

1. Створити віртуальну мережу Campus1 з двома підмережами за допомогою Azure Portal.
   1.1. Обрати регіон, у якому для Subscription Azure for Students дозволено розгортання ресурсів і можна створити віртуальні машини. Перелік дозволених регіонів задається політикою Allowed resource deployment regions (в Azure Portal: **Policy** > **Authoring** > **Assignments** > **Allowed resource deployment regions** > **Parameters** > **Allowed locations**), проте не в кожному з них підписці доступні розміри віртуальних машин, на які виділено квоту. Тому в Azure Cloud Shell (Bash) необхідно виконати скрипт, який для кожного дозволеного регіону виводить розміри віртуальних машин з не більше ніж 2 vCPU, що доступні для підписки та мають ненульову квоту сімейства (у дужках наведено сімейство, використану кількість vCPU та ліміт):

```
REGIONS=$(az policy assignment show --name sys.regionrestriction \
  --query "parameters.listOfAllowedLocations.value" -o tsv)

for L in $REGIONS; do
  echo "=== $L"
  az vm list-usage --location $L \
    --query "[?to_number(limit)>\`0\`].[name.value, currentValue,
limit]" -o tsv > ~/quota-$L.txt
  az vm list-skus --location $L --resource-type virtualMachines \
    --query "[?length(restrictions[?type=='Location'])==\`0\` &&
capabilities[?name=='vCPUs' && to_number(value)<=\`2\`]].[name,
family]" -o tsv |
  while read SKU FAMILY; do
    Q=$(grep -i "^$FAMILY[[:space:]]" ~/quota-$L.txt) && echo "
$SKU  ($Q)"
  done
done
```

   1.2. Обрати регіон, для якого скрипт вивів хоча б один розмір з лімітом сімейства не менше 6 vCPU (цього достатньо для трьох віртуальних машин у завданнях 11–12). Перевагу слід надавати розмірам серії B v2 (наприклад, `Standard_B2ats_v2` або `Standard_B2als_v2`); розміри DC*, EC* (confidential

computing) та L* (оптимізовані для сховища) не використовувати. Якщо для регіону виведено лише рядок `=== <регіон>`, створити віртуальні машини в ньому неможливо. Зафіксувати у звіті обраний регіон, його скорочену назву **xxx** та обраний розмір віртуальної машини – вони використовуватимуться в усіх наступних завданнях. Регіон необхідно обрати до створення віртуальних мереж, оскільки віртуальна машина може бути створена лише в регіоні своєї віртуальної мережі.

1.3. У головному пошуку знайти **Virtual networks** та натиснути **Create**.

1.4. На вкладці **Basics** вказати:

- **Subscription** – Azure for Students;
- **Resource group** – натиснути **Create new** та ввести `rg-vnet-xxx-yyy-zzz`;
- **Virtual network name** – `vnet-campus1-xxx-yyy-zzz`;
- **Region** – регіон, обраний у кроці 1.2.

1.5. Перейти на вкладку **Address space**. У блоці запропонованого адресного простору вказати **Starting address** та **Size** – `/16` згідно з адресним простором Campus1 у табл. 2, а запропоновану підмережу `default` видалити (піктограма кошика в рядку підмережі).

1.6. Натиснути **Add a subnet** та на панелі **Add a subnet** вказати:

- **Subnet purpose** – Default;
- **Name** – `snet-campus1-floor1`;
- у розділі **IPv4**: **Include an IPv4 address space** – позначено, **IPv4 address range** – адресний простір Campus1, **Starting address** – початкова адреса Floor1 згідно з табл. 2 (наприклад, `10.15.10.0`), **Size** – `/24 (256 addresses)`;

– **Enable private subnet (no default outbound access)**, **NAT gateway**, **Network security group**, **Route table** та решту параметрів залишити зі значеннями за замовчуванням.

1.7. Натиснути **Add**. Аналогічно створити підмережу `snet-campus1-floor2` з початковою адресою Floor2 згідно з табл. 2.

1.8. Натиснути **Review + create** та **Create**. Після створення додати до звіту скріншот розділу **Settings** > **Subnets** віртуальної мережі.

2. Створити віртуальну мережу Campus2 шляхом експорту та зміни ARM template мережі Campus1.

2.1. Відкрити віртуальну мережу `vnet-campus1-xxx-yyy-zzz`, у розділі **Automation** обрати **Export template** та дочекатися генерації шаблону. Переконатися, що позначено **Include parameters**, та натиснути **Download** – буде завантажено файл `template.json`. Параметри (зокрема ім'я віртуальної мережі) містяться в самому шаблоні в розділі `parameters` як значення `defaultValue`, тому окремий файл параметрів не потрібен.

2.2. Відкрити файл `template.json` у текстовому редакторі (наприклад, Visual Studio Code) та виконати заміну:

– усі входження `campus1` замінити на `campus2` – в імені параметра (наприклад, `virtualNetworks_vnet_campus1_xxx_yyy_zzz_name`), значенні `defaultValue` (`vnet-campus1-xxx-yyy-zzz`) та іменах підмереж;

– адресний простір Campus1 замінити на адресний простір Campus2 згідно з табл. 3;

– діапазони Floor1 та Floor2 мережі Campus1 замінити на діапазони Floor1 та Floor2 мережі Campus2 згідно з табл. 3. Підмережі описуються в експортованому шаблоні двічі (у властивості `subnets` віртуальної мережі та як окремі

ресурси `Microsoft.Network/virtualNetworks/subnets`), тому необхідно замінити всі входження.

2.3. Зберегти зміни у файлі `template.json`.

2.4. У головному пошуку Azure Portal знайти **Deploy a custom template** та обрати **Build your own template in the editor**. Натиснути **Load file**, обрати змінений файл `template.json` та натиснути **Save**.

2.5. На вкладці **Basics** обрати Subscription Azure for Students, Resource group `rg-vnet-xxx-yyy-zzz` та регіон, обраний у кроці 1.2. Переконатися, що в розділі **Instance details** параметр з іменем віртуальної мережі має значення `vnet-campus2-xxx-yyy-zzz` (воно підставляється з `defaultValue`). Натиснути **Review + create** та **Create**.

2.6. Після завершення розгортання переконатися, що віртуальна мережа `vnet-campus2-xxx-yyy-zzz` містить підмережі `snet-campus2-floor1` та `snet-campus2-floor2` з діапазонами згідно з табл. 3. Додати до звіту змінений `template.json` та скріншот підмереж.

3. Створити Application Security Group.

3.1. У головному пошуку Azure Portal знайти **Application security groups** та натиснути **Create**.

3.2. На вкладці **Basics** вказати **Subscription** – Azure for Students, **Resource group** – `rg-vnet-xxx-yyy-zzz`, **Name** – `asg-campus-web-xxx-yyy-zzz`, **Region** – регіон, обраний у кроці 1.2.

3.3. Натиснути **Review + create** та **Create**.

4. Створити та налаштувати Network Security Group.

4.1. У головному пошуку знайти **Network security groups** та натиснути **Create**. На вкладці **Basics** вказати **Subscription** – Azure for Students, **Resource group** – `rg-vnet-xxx-yyy-zzz`,

Name – `nsg-secure-xxx-yyy-zzz`, **Region** – регіон, обраний у кроці 1.2. Натиснути **Review + create** та **Create**.

4.2. Відкрити створену NSG, у розділі **Settings** обрати **Subnets** та натиснути **Associate**. Обрати **Virtual network** – `vnet-campus1-xxx-yyy-zzz`, **Subnet** – `snet-campus1-floor1` та натиснути **OK**.

4.3. Перейти в **Settings** > **Inbound security rules** та ознайомитися зі стандартними правилами (табл. 1).

4.4. Натиснути **Add** та створити вхідне правило, яке дозволить трафік за портами 80 TCP та 443 TCP для всіх віртуальних машин, що потенційно можуть бути додані до ASG:

- **Source** – Application security group;
- **Source application security groups** – `asg-campus-web-xxx-yyy-zzz`;
- **Source port ranges** – *;
- **Destination** – Any;
- **Service** – Custom;
- **Destination port ranges** – `80,443`;
- **Protocol** – TCP;
- **Action** – Allow;
- **Priority** – `100`;
- **Name** – `AllowCampusASG`.

4.5. Натиснути **Add**. Перейти в **Settings** > **Outbound security rules**, натиснути **Add** та створити вихідне правило, яке заборонить доступ до Інтернету:

- **Source** – Any;
- **Source port ranges** – *;
- **Destination** – Service Tag;
- **Destination service tag** – Internet;

- **Service** – Custom;
- **Destination port ranges** – *;
- **Protocol** – Any;
- **Action** – Deny;
- **Priority** – `4096`;
- **Name** – `DenyFromCampusToInternetOutbound`.

4.6. Натиснути **Add** та додати до звіту скріншоти вхідних і вихідних правил NSG.

5. Зареєструвати безкоштовний домен у доменній зоні `pp.ua` на сайті NIC.UA, використовуючи довільне ім'я домену. Для реєстрації доменів у зоні `pp.ua` необхідно підтвердити номер мобільного телефону.
6. Створити публічну DNS-зону для зареєстрованого домену та делегувати домен в Azure DNS.

6.1. У головному пошуку Azure Portal знайти **DNS zones** та натиснути **Create**.

6.2. На вкладці **Basics** вказати **Subscription** – Azure for Students, **Resource group** – натиснути **Create new** та ввести `rg-dns-xxx-yyy-zzz` (за наявності поля **Resource group location** обрати регіон з кроку 1.2), **Name** – ім'я зареєстрованого домену (наприклад, `example.pp.ua`). Натиснути **Review + create** та **Create**.

6.3. Відкрити створену DNS-зону, перейти в **DNS Management** > **Recordsets** та зафіксувати значення запису `@` типу NS – чотири сервери імен формату `ns1-06.azure-dns.com.`, `ns2-06.azure-dns.net.`, `ns3-06.azure-dns.org.`, `ns4-06.azure-dns.info.`.

6.4. У налаштуваннях домену на сайті NIC.UA вказати ці чотири значення як власні NS-сервери (без крапки в кінці) та зберегти зміни.

6.5. У розділі **Recordsets** натиснути **Add** та створити запис: **Name** – `yyy-zzz`, **Type** – A, **TTL** – залишити запропоноване значення, **IP address** – `127.0.0.1`. Натиснути **Add**.

6.6. Через певний час (від кількох хвилин до кількох годин) перевірити делегування та розв'язання запису на локальному комп'ютері командами `nslookup -type=NS <домен>` та `nslookup yyy-zzz.<домен>`. Виконати додаткову перевірку на сайті whatsmydns.net. Додати результати до звіту.

7. Створити приватну DNS-зону та пов'язати її з віртуальною мережею Campus2.

7.1. У головному пошуку Azure Portal знайти **Private DNS zones** та натиснути **Create**.

7.2. На вкладці **Basics** вказати **Subscription** – Azure for Students, **Resource group** – `rg-dns-xxx-yyy-zzz`, **Name** – `pvt.` + ім'я домену із завдання 5 (наприклад, `pvt.example.pp.ua`). Натиснути **Review + create** та **Create**.

7.3. Відкрити створену приватну зону, у розділі **DNS Management** обрати **Virtual Network Links** та натиснути **Add**. Вказати **Link name** – `link-campus2`, **Subscription** – Azure for Students, **Virtual Network** – `vnet-campus2-xxx-yyy-zzz`, у розділі **Configuration** позначити **Enable auto registration** та натиснути **Create**.

7.4. Дочекатися створення зв'язку та переконатися, що він відображається на сторінці **Virtual Network Links** зі статусом **Completed**.

8. Створити Virtual Network Peering між мережами Campus1 та Campus2 і перевірити зв’язність між віртуальними машинами за допомогою Azure CLI.

8.1. Відкрити Azure Cloud Shell (Bash) та задати змінні, підставивши власні значення:

```
SUFFIX=xxx-yyy-zzz
RG=rg-vnet-$SUFFIX
LOC=<регіон з кроку 1.2, наприклад spaincentral>
SIZE=<розмір віртуальної машини з кроку 1.2, наприклад
Standard_B2ats_v2>
VNET1=vnet-campus1-$SUFFIX
VNET2=vnet-campus2-$SUFFIX
```

8.2. Створити зв’язки peering в обох напрямках:

```
az network vnet peering create --name peer-campus1-to-campus2 \
  --resource-group $RG --vnet-name $VNET1 --remote-vnet $VNET2 --
allow-vnet-access

az network vnet peering create --name peer-campus2-to-campus1 \
  --resource-group $RG --vnet-name $VNET2 --remote-vnet $VNET1 --
allow-vnet-access
```

8.3. Переконатися, що обидва зв’язки мають стан **Connected**:

```
az network vnet peering list --resource-group $RG --vnet-name $VNET1
--output table
az network vnet peering list --resource-group $RG --vnet-name $VNET2
--output table
```

8.4. Перевірити реєстрацію resource provider `Microsoft.Compute` (Azure CLI не реєструє його автоматично) та за потреби зареєструвати його:

```
az provider show --namespace Microsoft.Compute --query
registrationState --output tsv
az provider register --namespace Microsoft.Compute --wait
```

8.5. Створити по одній віртуальній машині в підмережах Floor2 обох мереж (підмережі Floor2 не мають NSG, тому правила із завдання 4 не впливають на перевірку). Віртуальні машини створюються без публічних IP-адрес; диски та мережеві інтерфейси видалятимуться разом із машинами:

```
for N in 1 2; do
  az vm create --resource-group $RG --location $LOC --name vm-
campus$N \
```

```
    --vnet-name vnet-campus$N-$SUFFIX --subnet snet-campus$N-floor2
\
    --image Ubuntu2404 --size $SIZE \
    --admin-username azureuser --generate-ssh-keys \
    --public-ip-address "" --nsg "" \
    --os-disk-delete-option Delete --nic-delete-option Delete
done
```

8.6. Якщо команда повертає помилку `SkuNotAvailable` (тимчасова нестача потужностей у регіоні) або `QuotaExceeded`, обрати інший розмір з результатів скрипта кроку 1.1, змінити значення змінної `SIZE` та повторити команду. Загальна квота vCPU у регіоні для Subscription Azure for Students (`cores`) становить, як правило, 6 vCPU; поточне використання можна переглянути командою `az vm list-usage --location $LOC --query "[?name.value=='cores']" -o table`.

8.7. Отримати приватну IP-адресу віртуальної машини `vm-campus2` та перевірити її доступність з `vm-campus1` за допомогою Run Command (команда виконується всередині віртуальної машини без підключення через SSH):

```
IP2=$(az vm show --show-details --resource-group $RG --name vm-
campus2 --query privateIps --output tsv)
echo $IP2
az vm run-command invoke \
  --resource-group $RG \
  --name vm-campus1 \
  --command-id RunShellScript \
  --scripts "ping -c 4 $IP2" \
  --query "value[0].message" --output tsv
```

8.8. Додати до звіту використані команди та їх виведення.

9. Перевірити роботу приватної DNS-зони.

9.1. Відкрити приватну зону `pvt.<домен>`, перейти в **DNS Management** > **Recordsets** та переконатися, що для віртуальної машини `vm-campus2` автоматично створено A-запис зі значенням **Auto registered** – True.

9.2. Натиснути **Add** та створити запис: **Name** – `app`, **Type** – A, **IP address** – приватна IP-адреса `vm-campus2` (значення змінної `IP2` із кроку 8.7). Натиснути **Add**.

9.3. Перевірити розв'язання записів в Azure Cloud Shell, підставивши ім'я власної приватної зони:

```
ZONE=pvt.<домен>
nslookup app.$ZONE
nslookup vm-campus2.$ZONE
```

9.4. Перевірити розв'язання тих самих записів у віртуальних машинах `vm-campus2` (мережа пов'язана із зоною) та `vm-campus1` (мережа не пов'язана із зоною):

```
for N in 1 2; do
  echo "=== vm-campus$N"
  az vm run-command invoke \
    --resource-group $RG \
    --name vm-campus$N \
    --command-id RunShellScript \
    --scripts "nslookup app.$ZONE; nslookup vm-campus2.$ZONE" \
    --query "value[0].message" --output tsv
done
```

9.5. Зробити висновки щодо результатів розв'язання імен у Cloud Shell, у пов'язаній та непов'язаній віртуальних мережах.

9.6. Видалити віртуальні машини, щоб звільнити квоту vCPU для наступних завдань (без цього кроку створення трьох віртуальних машин у завданнях 11–12 завершиться помилкою `QuotaExceeded`):

```
az vm delete --resource-group $RG --name vm-campus1 --yes
az vm delete --resource-group $RG --name vm-campus2 --yes
```

10. Створити таблицю маршрутів, користувацький маршрут та віртуальну мережу з трьома підмережами, адресні простори обираються згідно з табл. 4.

10.1. В Azure Cloud Shell (Bash) задати змінні та створити окрему Resource group:

```
SUFFIX=xxx-yyy-zzz
RG2=rg-nva-$SUFFIX
LOC=<регіон з кроку 1.2>
SIZE=<розмір віртуальної машини з кроку 1.2>
```

```
VNET=vnet-nva-$SUFFIX
RT=rt-public-$SUFFIX
az group create --name $RG2 --location $LOC
```

10.2. Створити таблицю маршрутів:

```
az network route-table create --name $RT --resource-group $RG2 \
  --location $LOC --disable-bgp-route-propagation false
```

10.3. Створити користувацький маршрут, який спрямовуватиме весь трафік до підмережі `snet-private` через NVA (значення `--address-prefix` – діапазон snet-private, `--next-hop-ip-address` – IP-адреса NVA згідно з табл. 4):

```
az network route-table route create --route-table-name $RT --
resource-group $RG2 \
  --name route-to-private --address-prefix <діапазон snet-private> \
  --next-hop-type VirtualAppliance --next-hop-ip-address <IP-адреса
NVA>
```

10.4. Створити віртуальну мережу з підмережею `snet-public`, а також підмережі `snet-private` та `snet-dmz` (діапазони згідно з табл. 4):

```
az network vnet create --name $VNET --resource-group $RG2 --location
$LOC \
  --address-prefixes <адресний простір VNet> \
  --subnet-name snet-public --subnet-prefixes <діапазон snet-public>

az network vnet subnet create --name snet-private --vnet-name $VNET
\
  --resource-group $RG2 --address-prefixes <діапазон snet-private>

az network vnet subnet create --name snet-dmz --vnet-name $VNET \
  --resource-group $RG2 --address-prefixes <діапазон snet-dmz>

az network vnet subnet list --resource-group $RG2 --vnet-name $VNET
--output table
```

10.5. Асоціювати таблицю маршрутів з підмережею `snet-public`:

```
az network vnet subnet update --name snet-public --vnet-name $VNET \
  --resource-group $RG2 --route-table $RT
```

11. Розгорнути Network Virtual Appliance та ввімкнути переадресацію IP.

11.1. Створити віртуальну машину `vm-nva` у підмережі `snet-dmz`. Ця машина має бути першою в підмережі, щоб отримати IP-адресу NVA згідно з табл. 4:

```
az vm create --resource-group $RG2 --location $LOC --name vm-nva \
  --vnet-name $VNET --subnet snet-dmz \
  --image Ubuntu2404 --size $SIZE \
```

```
  --admin-username azureuser --generate-ssh-keys \
  --os-disk-delete-option Delete --nic-delete-option Delete
```

11.2. Переконатися, що приватна IP-адреса `vm-nva` збігається з IP-адресою NVA в табл. 4:

```
az vm list-ip-addresses --resource-group $RG2 --name vm-nva --output
table
```

11.3. Ввімкнути переадресацію IP на мережевому інтерфейсі `vm-nva`:

```
NICID=$(az vm nic list --resource-group $RG2 --vm-name vm-nva --
query "[].{id:id}" --output tsv)
NICNAME=$(az vm nic show --resource-group $RG2 --vm-name vm-nva --
nic $NICID --query "{name:name}" --output tsv)
echo $NICNAME
az network nic update --name $NICNAME --resource-group $RG2 --ip-
forwarding true
```

11.4. Ввімкнути переадресацію IP в операційній системі `vm-nva`:

```
NVAIP=$(az vm list-ip-addresses --resource-group $RG2 --name vm-nva
\
  --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress"
--output tsv)
echo $NVAIP
ssh -t -o StrictHostKeyChecking=no azureuser@$NVAIP 'sudo sysctl -w
net.ipv4.ip_forward=1; exit;'
```

12. Створити віртуальні машини в публічній та приватній підмережах і перевірити маршрутизацію трафіку через NVA.

12.1. В Azure Cloud Shell створити файл `cloud-init.txt` командою `code cloud-init.txt` та додати до нього конфігурацію, яка встановлює утиліту `traceroute` під час створення віртуальної машини:

```
#cloud-config
package_upgrade: true
packages:
   - inetutils-traceroute
```

12.2. Зберегти файл (Ctrl+S) та закрити редактор (Ctrl+Q).

12.3. Створити віртуальні машини `vm-public` у підмережі `snet-public` та `vm-private` у підмережі `snet-private`:

```
for N in public private; do
  az vm create --resource-group $RG2 --location $LOC --name vm-$N \
    --vnet-name $VNET --subnet snet-$N \
    --image Ubuntu2404 --size $SIZE \
    --admin-username azureuser --generate-ssh-keys \
    --custom-data cloud-init.txt --no-wait \
    --os-disk-delete-option Delete --nic-delete-option Delete
```

```
done
```

12.4. Відстежувати стан віртуальних машин, доки всі три машини не матимуть **ProvisioningState** – Succeeded та **PowerState** – VM running (для виходу натиснути Ctrl+C):

```
watch -d -n 5 "az vm list --resource-group $RG2 --show-details \
  --query '[*].{Name:name, ProvisioningState:provisioningState,
PowerState:powerState}' --output table"
```

12.5. Зберегти публічні IP-адреси віртуальних машин у змінних:

```
PUBLICIP=$(az vm list-ip-addresses --resource-group $RG2 --name vm-
public \
  --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress"
--output tsv)
PRIVATEIP=$(az vm list-ip-addresses --resource-group $RG2 --name vm-
private \
  --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress"
--output tsv)
echo $PUBLICIP $PRIVATEIP
```

12.6. Відстежити маршрут від `vm-public` до `vm-private`. Якщо з'являється помилка `traceroute: command not found`, зачекати 1–2 хвилини, доки cloud-init завершить встановлення пакета, та повторити команду:

```
ssh -t -o StrictHostKeyChecking=no azureuser@$PUBLICIP 'traceroute
vm-private --type=icmp; exit'
```

12.7. Відстежити маршрут у зворотному напрямку – від `vm-private` до `vm-public`:

```
ssh -t -o StrictHostKeyChecking=no azureuser@$PRIVATEIP 'traceroute
vm-public --type=icmp; exit'
```

12.8. Порівняти результати обох перевірок: визначити, через які адреси проходить трафік у кожному напрямку, та пояснити отриманий результат з урахуванням таблиці маршрутів, асоційованої з підмережею `snet-public`. Додати до звіту використані команди та їх виведення.

13. Видалити всі ресурси, створені під час виконання лабораторної роботи.

13.1. Видалити Resource groups `rg-nva-xxx-yyy-zzz`, `rg-vnet-xxx-yyy-zzz` та `rg-dns-xxx-yyy-zzz` разом з усіма ресурсами в них

– в Azure Portal (сторінка **Overview** Resource group > **Delete resource group**) або в Azure Cloud Shell:

```
az group delete --name rg-nva-xxx-yyy-zzz --yes --no-wait
az group delete --name rg-vnet-xxx-yyy-zzz --yes --no-wait
az group delete --name rg-dns-xxx-yyy-zzz --yes --no-wait
```

13.2. Видалити Resource group `NetworkWatcherRG`, якщо її було автоматично створено під час виконання лабораторної роботи.

13.3. Перейти в **Resource groups** та **All resources** і переконатися, що ресурсів, створених у лабораторній роботі, не залишилося. Додати до звіту відповідні скріншоти.

Таблиця 2

Адресний простір віртуальної мережі Campus1 згідно з варіантом

№ варіанту	Адресний простір VNet	snet-campus1-floor1	snet-campus1-floor2
1	10.1.0.0/16	10.1.10.0/24	10.1.20.0/24
2	10.2.0.0/16	10.2.10.0/24	10.2.20.0/24
3	10.3.0.0/16	10.3.10.0/24	10.3.20.0/24
4	10.4.0.0/16	10.4.10.0/24	10.4.20.0/24
5	10.5.0.0/16	10.5.10.0/24	10.5.20.0/24
6	10.6.0.0/16	10.6.10.0/24	10.6.20.0/24
7	10.7.0.0/16	10.7.10.0/24	10.7.20.0/24
8	10.8.0.0/16	10.8.10.0/24	10.8.20.0/24
9	10.9.0.0/16	10.9.10.0/24	10.9.20.0/24
10	10.10.0.0/16	10.10.10.0/24	10.10.20.0/24
11	10.11.0.0/16	10.11.10.0/24	10.11.20.0/24
12	10.12.0.0/16	10.12.10.0/24	10.12.20.0/24
13	10.13.0.0/16	10.13.10.0/24	10.13.20.0/24
14	10.14.0.0/16	10.14.10.0/24	10.14.20.0/24
15	10.15.0.0/16	10.15.10.0/24	10.15.20.0/24
16	10.16.0.0/16	10.16.10.0/24	10.16.20.0/24
17	10.17.0.0/16	10.17.10.0/24	10.17.20.0/24
18	10.18.0.0/16	10.18.10.0/24	10.18.20.0/24
19	10.19.0.0/16	10.19.10.0/24	10.19.20.0/24
20	10.20.0.0/16	10.20.10.0/24	10.20.20.0/24
21	10.21.0.0/16	10.21.10.0/24	10.21.20.0/24
22	10.22.0.0/16	10.22.10.0/24	10.22.20.0/24
23	10.23.0.0/16	10.23.10.0/24	10.23.20.0/24
24	10.24.0.0/16	10.24.10.0/24	10.24.20.0/24
25	10.25.0.0/16	10.25.10.0/24	10.25.20.0/24
26	10.26.0.0/16	10.26.10.0/24	10.26.20.0/24
27	10.27.0.0/16	10.27.10.0/24	10.27.20.0/24
28	10.28.0.0/16	10.28.10.0/24	10.28.20.0/24
29	10.29.0.0/16	10.29.10.0/24	10.29.20.0/24

№ варіанту	Адресний простір VNet	snet-campus1-floor1	snet-campus1-floor2
30	10.30.0.0/16	10.30.10.0/24	10.30.20.0/24

Таблиця 3

Адресний простір віртуальної мережі Campus2 згідно з варіантом

№ варіанту	Адресний простір VNet	snet-campus2-floor1	snet-campus2-floor2
1	10.101.0.0/16	10.101.10.0/24	10.101.20.0/24
2	10.102.0.0/16	10.102.10.0/24	10.102.20.0/24
3	10.103.0.0/16	10.103.10.0/24	10.103.20.0/24
4	10.104.0.0/16	10.104.10.0/24	10.104.20.0/24
5	10.105.0.0/16	10.105.10.0/24	10.105.20.0/24
6	10.106.0.0/16	10.106.10.0/24	10.106.20.0/24
7	10.107.0.0/16	10.107.10.0/24	10.107.20.0/24
8	10.108.0.0/16	10.108.10.0/24	10.108.20.0/24
9	10.109.0.0/16	10.109.10.0/24	10.109.20.0/24
10	10.110.0.0/16	10.110.10.0/24	10.110.20.0/24
11	10.111.0.0/16	10.111.10.0/24	10.111.20.0/24
12	10.112.0.0/16	10.112.10.0/24	10.112.20.0/24
13	10.113.0.0/16	10.113.10.0/24	10.113.20.0/24
14	10.114.0.0/16	10.114.10.0/24	10.114.20.0/24
15	10.115.0.0/16	10.115.10.0/24	10.115.20.0/24
16	10.116.0.0/16	10.116.10.0/24	10.116.20.0/24
17	10.117.0.0/16	10.117.10.0/24	10.117.20.0/24
18	10.118.0.0/16	10.118.10.0/24	10.118.20.0/24
19	10.119.0.0/16	10.119.10.0/24	10.119.20.0/24
20	10.120.0.0/16	10.120.10.0/24	10.120.20.0/24
21	10.121.0.0/16	10.121.10.0/24	10.121.20.0/24
22	10.122.0.0/16	10.122.10.0/24	10.122.20.0/24
23	10.123.0.0/16	10.123.10.0/24	10.123.20.0/24
24	10.124.0.0/16	10.124.10.0/24	10.124.20.0/24
25	10.125.0.0/16	10.125.10.0/24	10.125.20.0/24
26	10.126.0.0/16	10.126.10.0/24	10.126.20.0/24
27	10.127.0.0/16	10.127.10.0/24	10.127.20.0/24
28	10.128.0.0/16	10.128.10.0/24	10.128.20.0/24
29	10.129.0.0/16	10.129.10.0/24	10.129.20.0/24
30	10.130.0.0/16	10.130.10.0/24	10.130.20.0/24

Таблиця 4

Адресний простір віртуальної мережі завдань 10–12 згідно з варіантом

№	Адресний простір VNet	snet-public	snet-private	snet-dmz	IP-адреса NVA
1	10.201.0.0/16	10.201.0.0/24	10.201.1.0/24	10.201.2.0/24	10.201.2.4
2	10.202.0.0/16	10.202.0.0/24	10.202.1.0/24	10.202.2.0/24	10.202.2.4
3	10.203.0.0/16	10.203.0.0/24	10.203.1.0/24	10.203.2.0/24	10.203.2.4
4	10.204.0.0/16	10.204.0.0/24	10.204.1.0/24	10.204.2.0/24	10.204.2.4

№	Адресний простір VNet	snet-public	snet-private	snet-dmz	IP-адреса NVA
5	10.205.0.0/16	10.205.0.0/24	10.205.1.0/24	10.205.2.0/24	10.205.2.4
6	10.206.0.0/16	10.206.0.0/24	10.206.1.0/24	10.206.2.0/24	10.206.2.4
7	10.207.0.0/16	10.207.0.0/24	10.207.1.0/24	10.207.2.0/24	10.207.2.4
8	10.208.0.0/16	10.208.0.0/24	10.208.1.0/24	10.208.2.0/24	10.208.2.4
9	10.209.0.0/16	10.209.0.0/24	10.209.1.0/24	10.209.2.0/24	10.209.2.4
10	10.210.0.0/16	10.210.0.0/24	10.210.1.0/24	10.210.2.0/24	10.210.2.4
11	10.211.0.0/16	10.211.0.0/24	10.211.1.0/24	10.211.2.0/24	10.211.2.4
12	10.212.0.0/16	10.212.0.0/24	10.212.1.0/24	10.212.2.0/24	10.212.2.4
13	10.213.0.0/16	10.213.0.0/24	10.213.1.0/24	10.213.2.0/24	10.213.2.4
14	10.214.0.0/16	10.214.0.0/24	10.214.1.0/24	10.214.2.0/24	10.214.2.4
15	10.215.0.0/16	10.215.0.0/24	10.215.1.0/24	10.215.2.0/24	10.215.2.4
16	10.216.0.0/16	10.216.0.0/24	10.216.1.0/24	10.216.2.0/24	10.216.2.4
17	10.217.0.0/16	10.217.0.0/24	10.217.1.0/24	10.217.2.0/24	10.217.2.4
18	10.218.0.0/16	10.218.0.0/24	10.218.1.0/24	10.218.2.0/24	10.218.2.4
19	10.219.0.0/16	10.219.0.0/24	10.219.1.0/24	10.219.2.0/24	10.219.2.4
20	10.220.0.0/16	10.220.0.0/24	10.220.1.0/24	10.220.2.0/24	10.220.2.4
21	10.221.0.0/16	10.221.0.0/24	10.221.1.0/24	10.221.2.0/24	10.221.2.4
22	10.222.0.0/16	10.222.0.0/24	10.222.1.0/24	10.222.2.0/24	10.222.2.4
23	10.223.0.0/16	10.223.0.0/24	10.223.1.0/24	10.223.2.0/24	10.223.2.4
24	10.224.0.0/16	10.224.0.0/24	10.224.1.0/24	10.224.2.0/24	10.224.2.4
25	10.225.0.0/16	10.225.0.0/24	10.225.1.0/24	10.225.2.0/24	10.225.2.4
26	10.226.0.0/16	10.226.0.0/24	10.226.1.0/24	10.226.2.0/24	10.226.2.4
27	10.227.0.0/16	10.227.0.0/24	10.227.1.0/24	10.227.2.0/24	10.227.2.4
28	10.228.0.0/16	10.228.0.0/24	10.228.1.0/24	10.228.2.0/24	10.228.2.4
29	10.229.0.0/16	10.229.0.0/24	10.229.1.0/24	10.229.2.0/24	10.229.2.4
30	10.230.0.0/16	10.230.0.0/24	10.230.1.0/24	10.230.2.0/24	10.230.2.4

Контрольні запитання

1. Що таке Azure Virtual Network і для чого вона використовується в хмарній інфраструктурі? Які параметри потрібно обов’язково вказати при її створенні?
2. Яка роль Subnet у віртуальній мережі Azure і чому важливо правильно планувати її адресний простір?
3. Поясніть, що таке Network Security Group (NSG). Які параметри визначають правило NSG, та як пріоритет впливає на обробку трафіку?
4. У чому відмінність між Application Security Group (ASG) та Network Security Group (NSG)? Коли доцільно використовувати ASG?
5. Навіщо створюється Azure DNS Zone? Яка різниця між публічною та приватною DNS зоною?
6. Що таке Virtual Network Peering? Які переваги він надає порівняно з традиційним маршрутизуванням?
7. Поясніть відмінність між Azure Load Balancer та Azure Application Gateway. На якому рівні моделі OSI працює кожен з них?
8. Для чого використовується Network Virtual Appliance (NVA)? Наведіть приклади сценаріїв, де її застосування є необхідним.
9. Що таке Azure Private DNS Zone, як вона пов’язана з Virtual Network, та навіщо використовується функція auto-registration?
10. Яким чином Azure Network Watcher допомагає у діагностиці мережевих з’єднань? Наведіть приклад інструмента (Connection Monitor, IP Flow Verify тощо) та його застосування.