Міністерство освіти і науки України

Національний лісотехнічний університет України

Кафедра інформаційних технологій

**ЗВІТ ДО ЛАБОРАТОРНОЇ РОБОТИ № 5**

з навчальної дисципліни

**«Хмарні технології»**

на тему:

**«Налаштування Virtual Network»**

**Виконав:**

студент групи КН-32/1

Стасів В. Я.

**Перевірив:**

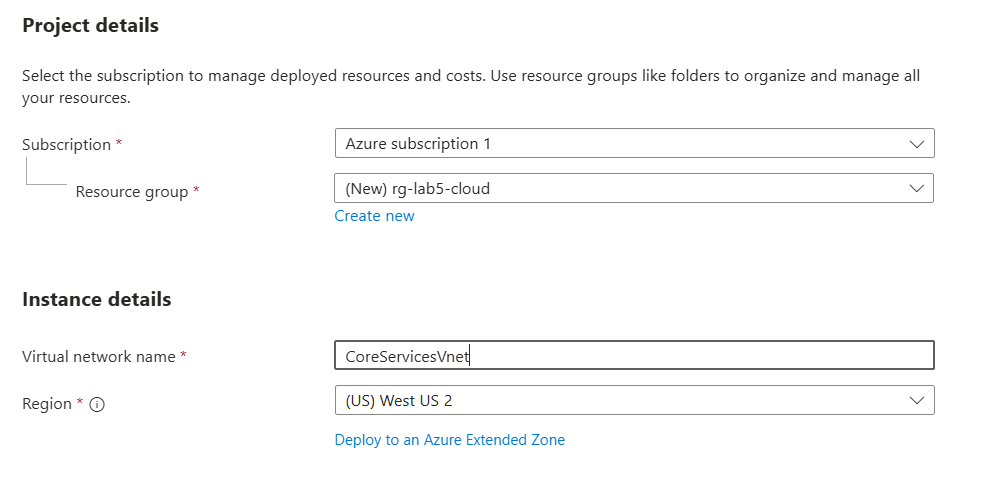
Антоник А. В.

Львів – 2025

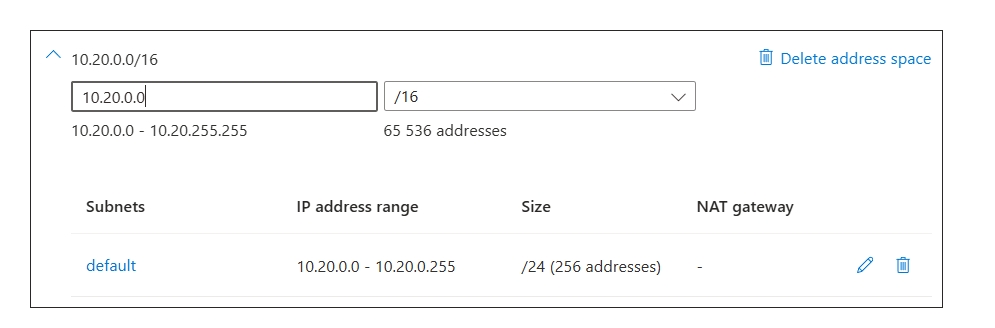
Мета: Ця лабораторна робота присвячена віртуальним мережам. У цій лабораторній роботі ви вивчите основи віртуальної мережі та створення підмереж, дізнаєтеся як захистити свою мережу за допомогою груп мережевої безпеки і груп безпеки додатків.

Завдання 1

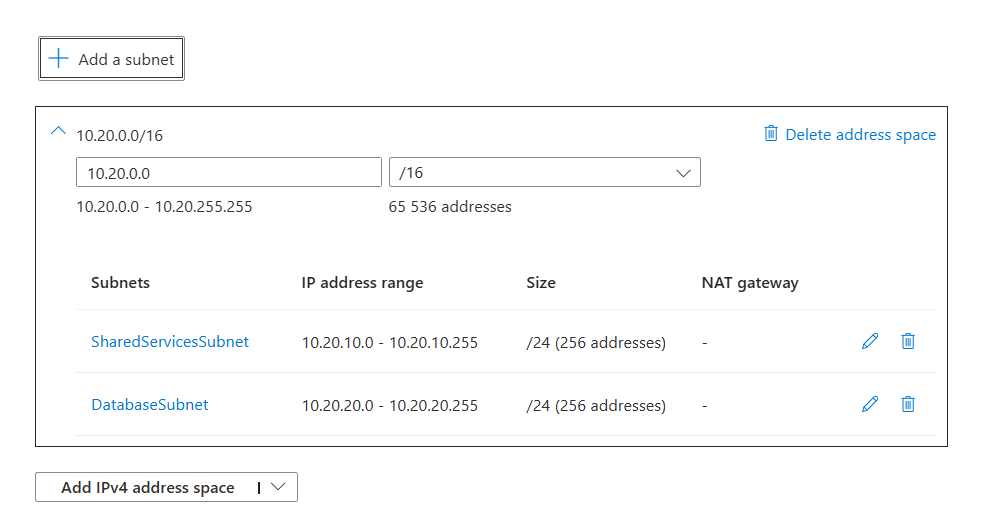
Створіть ресурсну групу rg-lab5-cloud, після цього створіть віртуальну мережу з підмережами, увійдіть на портал Azure, знайдіть і виберіть Virtual Networks, натисніть кнопку Create на сторінці Virtual networks.



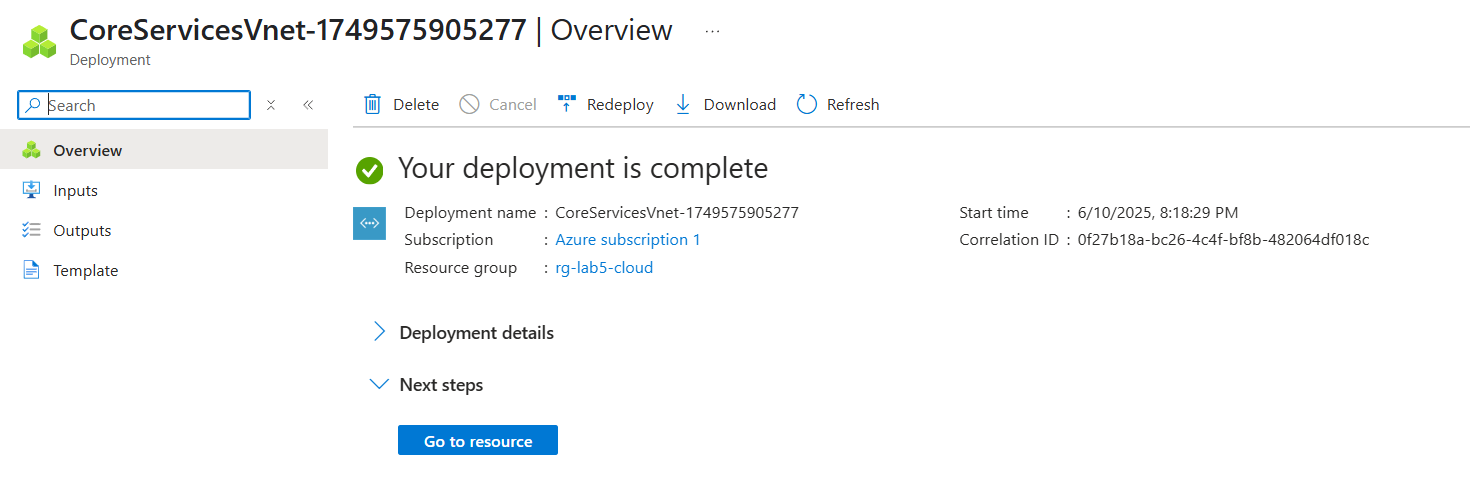
Перехожу на вкладку IP-adresses:



Виберіть - Add a subnet. Заповніть інформацію про назву та адресу для кожної підмережі. Не забудьте вибрати Додати для кожної нової підмережі. Не забудьте видалити підмережу за замовчуванням - до або після створення іншої підмережі



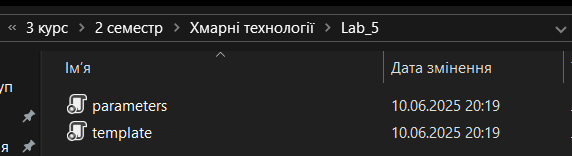
Мережа створена:



У розділі Automation виберіть Export template, а потім зачекайте, поки шаблон буде згенеровано.

Шаблон завантажено та розпаковано:





Завдання 2

Створення віртуальної мережі та підмереж за допомогою шаблону. Відредагуйте файл за допомогою обраного вами редактора. Багато редакторів мають функцію зміни всіх входжень.

Внесіть зміни для віртуальної мережі ManufacturingVnet:

1. Замініть всі входження CoreServicesVnet на ManufacturingVnet.

2. Замініть всі входження 10.20.0.0 на 10.30.0.0

Готово.

Внесіть зміни для підмережі ManufacturingVnet:

1. Змініть усі входження SharedServicesSubnet на SensorSubnet1.

2. Змініть всі входження 10.20.10.0/24 на 10.30.20.0/24.

3. Замініть усі входження DatabaseSubnet на SensorSubnet2.

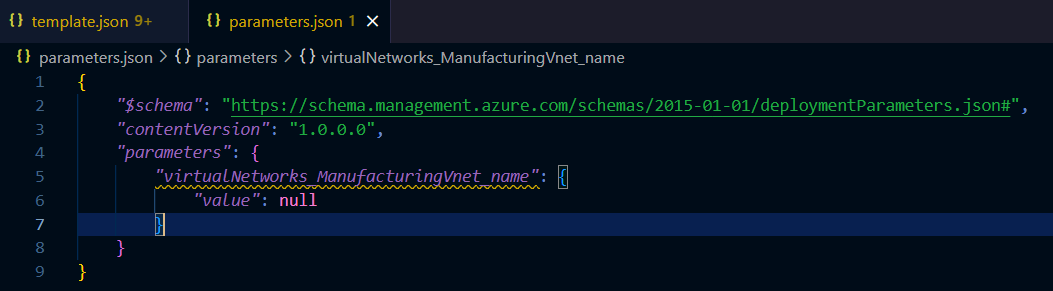
4. Змініть всі входження 10.20.20.0/24 на 10.30.21.0/24

Готово.

Збережіть внесені зміни.

Внесіть зміни до файлу параметрів:

1. Замініть одне входження CoreServicesVnet на ManufacturingVnet.



Розгортання власного шаблону

1. На порталі Azure знайдіть і виберіть - Deploy a custom template

2. Виберіть Build your own template in the editor, потім Load file

3. Виберіть файл templates.json зі змінами, потім натисніть Save

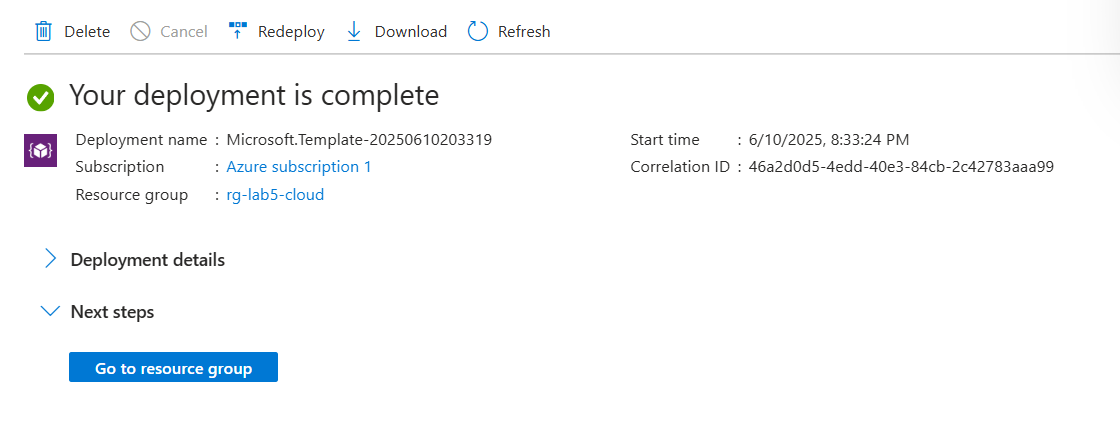
4. Виберіт Edit parameter, потім Load file.

5. Виберіть файл parameters.json з вашими змінами, а потім натисніть кнопку Save.

6. Виберіть Review + create, потім Create.

7. Зачекайте, поки шаблон розгорнеться, а потім переконайтесь, що віртуальну

мережу та підмережі Manufacturing створено.



Завдання 3

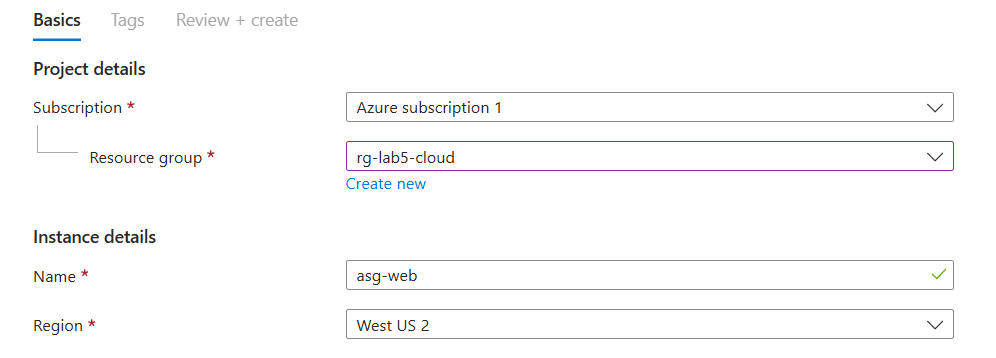
Створення та налаштування зв'язку між Application Security Group і Network Security Group.

У цьому завданні ми створимо Application Security Group і Network Security Group. NSG матиме правило безпеки для вхідного трафіку, яке дозволяє трафік з ASG. Група NSG також матиме правило для вихідного трафіку, яке забороняє доступ до інтернету.

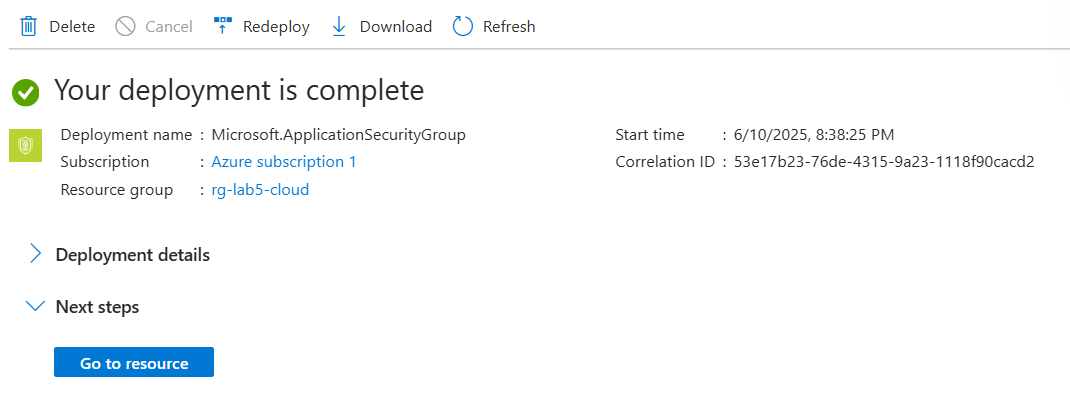
Створення Application Security Group (ASG):

1. На порталі Azure знайдіть і виберіть Application security groups

2. Натисніть Create та введіть основну інформацію.



3. Виберіть Review + create, потім Create.

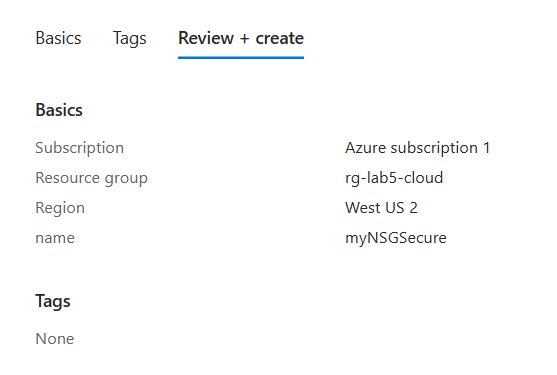


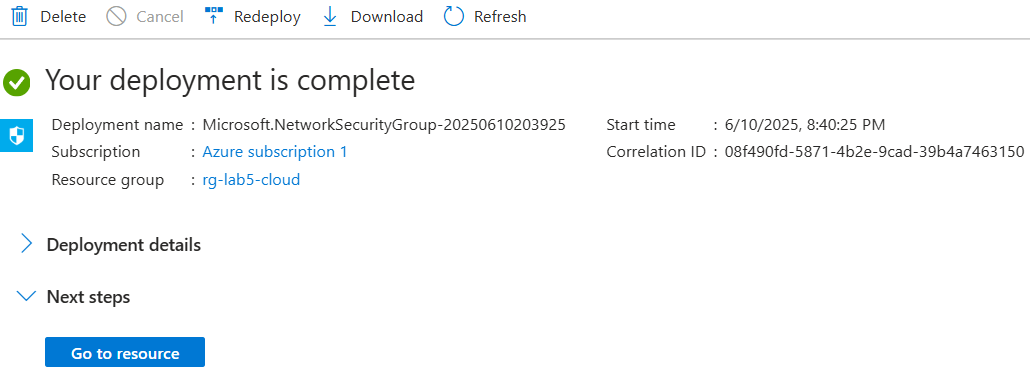
Створення Network Security Group (NSG) і зв’язування CoreServicesVnet:

1. На порталі Azure знайдіть і виберіть Network Security Group

2. Натисніть Create та введіть основну інформацію.

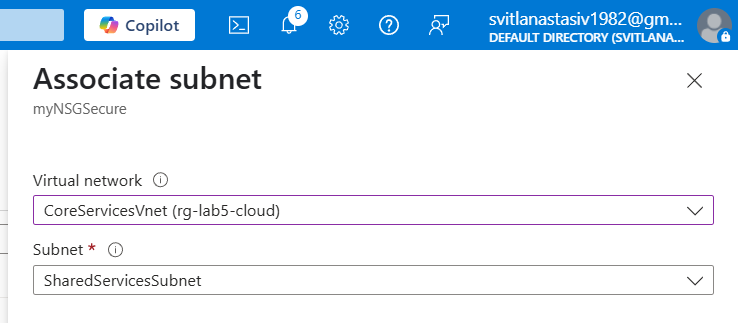
3. Виберіть Review + create, потім Create.



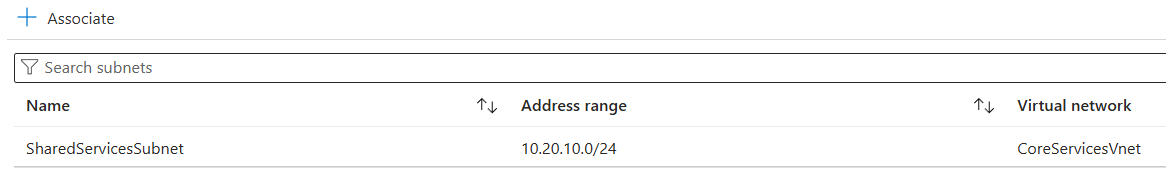


4. Після розгортання NSG натисніть Go to resource.

5. У розділі Settings натисніть Subnets, а потім Associate



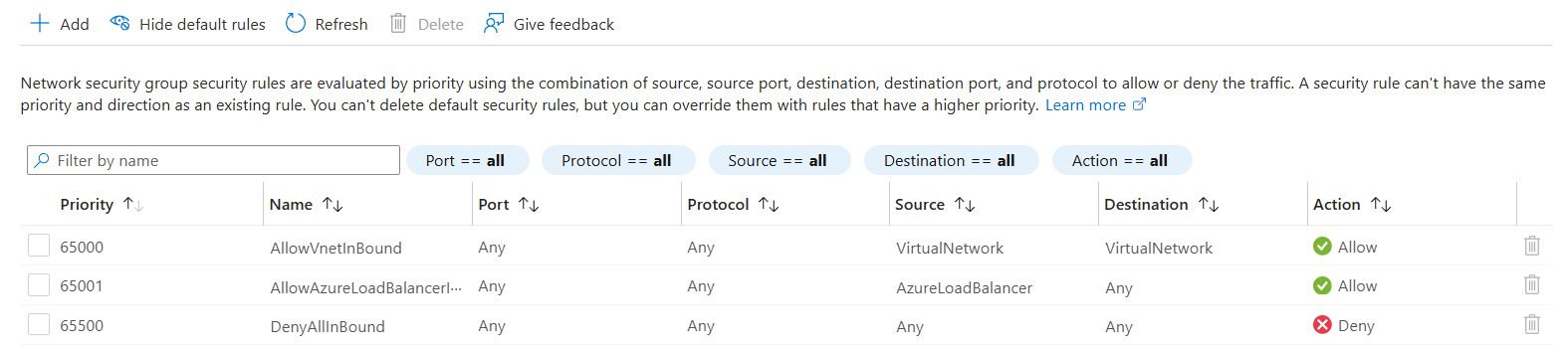
6. Натисніть OK, щоб зберегти асоціацію.



Налаштування правил безпеки для вхідного трафіку, щоб дозволити ASG-трафік:

1. Продовжуйте працювати з NSG. В області Settings виберіть Inbound security

rules.



2. Перегляньте правила вхідного трафіку за замовчуванням. Зверніть увагу, що доступ

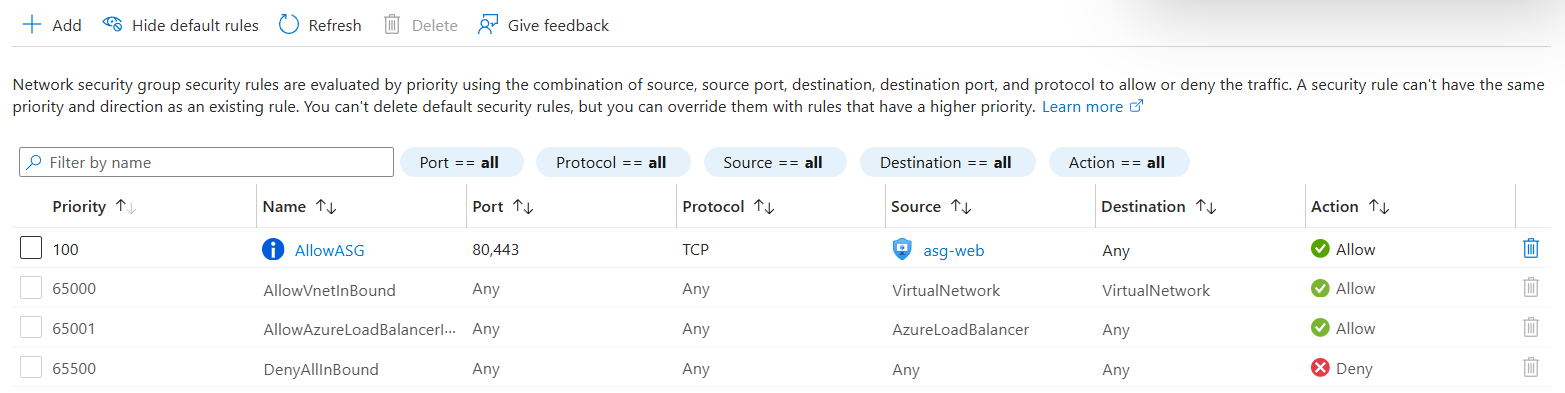
дозволено лише іншим віртуальним мережам і балансувальникам навантаження.

3. Натисніть Add

4. На вкладці Add inbound security rule скористайтеся наведеною нижче

інформацією, щоб додати правило для вхідного порту. Це правило дозволяє трафік

ASG. Після заповнення натисніть Add

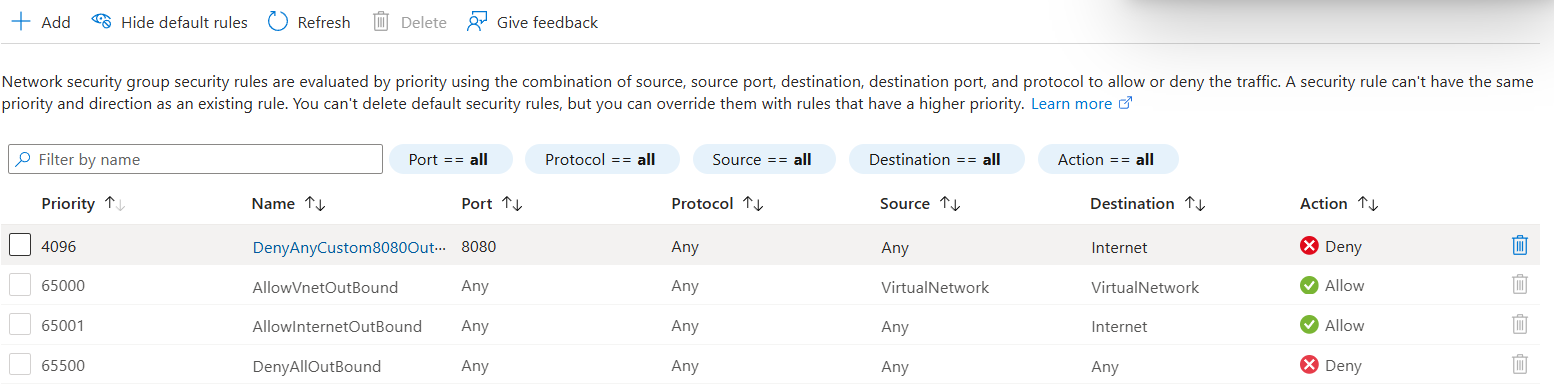


Налаштування вихідного правила NSG, яке забороняє доступ до Інтернету:

1. Після створення вхідного правила NSG виберіть Outbound security rules

2. Натисніть Add, а потім налаштуйте правило для вихідного трафіку, яке забороняє

доступ до інтернету. Завершивши, натисніть Add



Висновок: в ході даної лабораторної роботи я вивчив основи віртуальної мережі та навчився створювати підмережі, дізнався як захистити свою мережу за допомогою груп мережевої безпеки і груп безпеки додатків.