# Налаштування мережевих параметрів ВМ Azure

## вміння

* визначати, коли потрібно використовувати групи безпеки мережі
* реалізовувати правила груп безпеки мережі (відкривати порти ВМ)
* оцінювати діючі правила груп безпеки мережі

## вивчаємо

* IP адресація, публічна та приватна ІР адреси, статична та динамічна адреси
* порти, мережеві служби
* групи безпеки мережі, правила груп безпеки мережі, правила вхідного/вихідного трафіку, правила за замовчуванням
* як Azure використовує правила мережі
* Azure Bastion

## ресурси

<https://docs.microsoft.com/ru-ru/learn/modules/create-windows-virtual-machine-in-azure/6-manage-vm>

<https://docs.microsoft.com/ru-ru/learn/modules/configure-network-security-groups/2-implement-network-security-groups>

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

<https://docs.microsoft.com/en-us/learn/modules/secure-and-isolate-with-nsg-and-service-endpoints/>

[https://azure.microsoft.com/ru-ru/services/azure-bastion/#features](https://azure.microsoft.com/ru-ru/services/azure-bastion/" \l "features)

<https://docs.microsoft.com/ru-ru/azure/bastion/>

<https://docs.microsoft.com/ru-ru/learn/modules/connect-vm-with-azure-bastion/>

## Модель OSI та стек протоколів TCP/IP

Модель OSI (Open System Interconnection) - багаторівнева абстрактна мережева модель для комунікацій і розробки мережевих протоколів.

Мережевий протокол - набір правил та дій, що дозволяє здійснювати з'єднання і обмін даними між двома і більше включеними в мережу пристроями.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Рівень OSI | Призначення | Тип даних | Рівень TCP/IP | Протоколи | Імена |
| прикладний | доступ до мережевих служб | дані | прикладний | DHCP, DNS, FTP, HTTP, SSL, POP3, IMAP, SMTP | hostname (opt) |
| представницький | представлення і кодування даних |
| сеансовий | керування сеансом зв’язку |
| транспортний | прямий зв'язок між кінцевими пунктами і надійність | сегменти | транспортний | TCP, UDP | ports |
| мережевий | визначення маршруту і логічна адресація | пакети | мережевий | IP, ICMP, IGMP | IP |
| канальний | фізична адресація | кадри | канальний | Ethernet, Wi-Fi ARP, RARP | MAC |
| фізичний | передача сигналу | біти |

### Мережевий рівень (Network layer)

**визначення маршруту і логічна адресація**

IP (Internet Protocol, міжмережевий протокол) - протокол маршрутизації мережевого рівня

#### IP-адреса

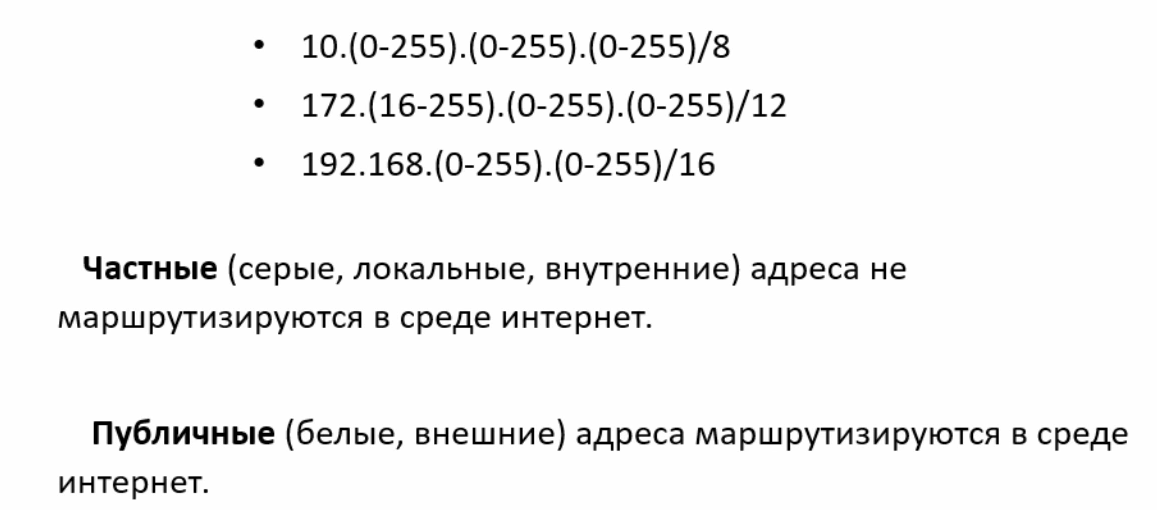
* використовується для однозначної ідентифікації хоста (host) на мережевому рівні
* Ipv4/Ipv6 протоколи
* Ipv4 адресація:
  + 32 біти - 4 десяткові октети, розділені крапками (dotted quad)
  + CIDR:
    - 192.168.0.1/24
    - частина мережі (network), визначається маскою (netmask) підмережі
    - частина хосту (host), визначається маскою підмережі
  + адреси спеціального призначення:
    - адреса мережі: 192.168.0.0/24
    - адреса широкомовної трансляції (broadcast): 192.168.0.255
  + програмно прив'язана до інтерфейсу
  + не може співіснувати в 2-х мережах, розділених маршрутизатором
* Azure:
  + 10.0.0.0/16 (2^16 вузлів)
  + 10.0.0.0-10.0.0.3 та 10.0.255.255 - зарезервовано

#### Динамічна та статична ІР адреси

**DHCP** ([*Dynamic Host Configuration Protocol)*](https://uk.wikipedia.org/wiki/Англійська_мова) - протокол динамічної конфігурації вузла, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі (IP address, netmask address, default gateway, DNS server)

* Azure:
  + динамічна - безкоштовна
  + статична – платна
  + <https://azure.microsoft.com/ru-ru/pricing/details/ip-addresses/>

#### Публічні та приватні адреси

* Публічні (білі, зовнішні)
  + доступні з Інтернету
  + видаються IANA (Internet Assigned Numbers Authority)
* Приватні (сірі, локальні, внутрішні)
  + не доступні з Інтернету
  + локальні мережі
    - 10.0.0.0- 10.255.255.255, 1 мережа
    - 172.16.0.0-172.31.255.255, 16 мереж
    - 192.168.0.0-192.168.255.255, 256 мереж
  + Петлевий інтерфейс
    - 127.0.0.0/8 - 256\*256\*256 вузлів
* Azure:
  + 10.0.0.0/16 – приватні
  + публічні

### Транспортний рівень

**прямий зв'язок між кінцевими пунктами і надійність**

TCP (*Transmission Control Protocol*, протокол управління з'єднанням)

* найпоширеніший протокол транспортного рівня в стеці TCP / IP
* створює повне з'єднання для перевірки помилок, підтверджень тощо.
* використовується для забезпечення надійної передачі даних

**UDP** (*User Datagram Protocol,* ):

* не створює з'єднання між мережевими хостами

#### Порти та сокети

Порт (port)— це ідентифікований номером системний ресурс, що виділяється **додаткам**, що виконується на деякому мережевому хості, для зв'язку з додатками, що виконуються на інших мережевих хостах (в тому числі з іншими додатками на цьому ж хості).

Сокет (socket)- програмний інтерфейс для забезпечення інформаційного обміну між процесами:

**IPv4**:port

#### Мережеві служби (Network services)

* номери портів призначаються організацією IANA (Internet Assigned Numbers Authority)
* для ідентифікації служб використовуються номери портів [0-65535] (Linux)
  + N <1024 - привілейовані порти (служби запускаються тільки суперкористувачем)
  + 1024 <= N <65 535 ефемерні порти, можуть бути не пов'язані зі службою

/etc/services - повний список мережевих служб

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Port** | **Protocol** | | **Service** | **Example Linux Implementation** |  |
| 22 | TCP | | SSH | OpenSSH |  |
| 53 | TCP / UDP | | DNS | BIND |  |
| 80 | TCP | | HTTP | Apache |  |
| 110 | TCP | | POP3 | Dovecot |  |
| 139 | TCP | Windows file sharing | | Samba | |
| 443 | TCP | HTTPS | | Apache | |

netstat

## Відкриття портів у ВМ Azure

### Використання портів

Для чого?

На якому рівні протоколу ТСР/ІР?

Які номери портів за замовчуванням?

Окремо відкриваються порти на вхідний і на вихідний трафік

Відкриття портів:

* при створенні нової ВМ можна відкрити поширені порти (RDP, HTTP, HTTPS і SSH)
  + групу безпеки можна не створювати, тоді все дозволено
* якщо вам потрібні інші зміни в брандмауері, необхідно буде внести їх самостійно.

Ця процедура складається з двох етапів:

1. Створіть групу безпеки мережі.

2. Створіть правило вхідного/вихідного трафіку, що дозволяє трафік через відповідний порт.

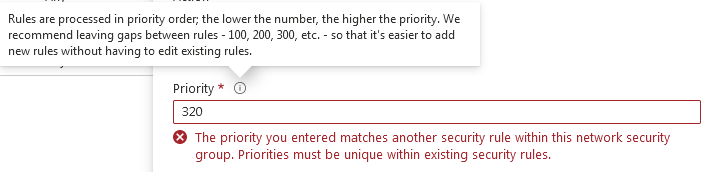
### Правила групи безпеки

#### Правила мережі за замовчуванням

* є у всіх груп безпеки
* стосуються вхідного та вихідного трафіку
  + по 3 правила для забезпечення базового рівня безпеки
* не можна змінити/видалити, але можна перевизначити правилами з вищим пріоритетом
* пріоритет: число від 100 до 4096
  + більше числове значення – менший пріоритет
  + коли трафік відповідає правилу, обробка зупиняється. Це означає, що будь-які інші правила з більш низьким пріоритетом (більше число) не будуть оброблені.

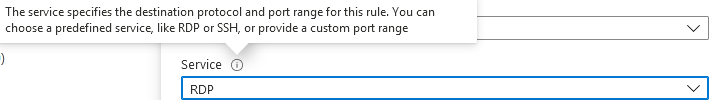
#### Правила безпеки мережі - обмеження

* кількість правил безпеки, які можна створити в NSG, обмежена
* не слід створювати два правила безпеки з однаковим пріоритетом і напрямком
* залишати інтервал між правилами (пріоритетами), щоб легше було вносити зміни.

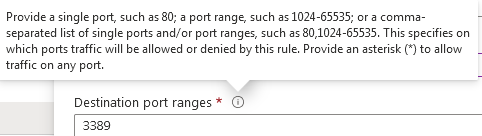


#### Параметри правил

* Ім'я - унікальне ім'я, яке описує його призначення.
* Пріоритет – унікальний, число від 100 до 4096.
* Джерело/призначення (якщо вибрати діапазон, тег служби або групу безпеки додатків, можна створювати менше правил безпеки):
  + всі
  + окрема IP-адреса (список, розділений комами, діапазон IP-адрес, для ВМ - приватна ІР адреса)
  + тег служби (група префіксів IP-адрес з даної служби Azure)
  + група безпеки додатків.
* Протокол: який мережевий протокол перевірятиме правило



* Порти (вказівка діапазону забезпечує більшу ефективність при створенні правил безпеки)
  + можна вказати окремий порт
  + діапазон портів (кома, тире, \*).



* Дія: заборонити/дозволити

### Група безпеки мережі

Групи безпеки мережі (NSG)

* є логічним контейнером для правил
* можна пов'язати з мережевим інтерфейсом (для правил окремих вузлів), підмережею у віртуальній мережі (для застосування до кількох ресурсів) або з обома рівнями
* 1 підмережа/мережевий інтерфейс може мати тільки 1 NSG,
* 1 NSG може бути застосовано до кількох під мереж або мережевих інтерфейсів

### Як Azure використовує правила мережі

Для доступу за певним портом потрібно дозвіл (не заборона) на всіх рівнях

Для вхідного трафіку/вихідного послідовність застосування правил різна

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Правила підмережі |  | Правила мережевого інтерфейсу |  | Правила брандмауера |  | **порт**  **порт** |
|  |  | allow |  | allow |  | allow |  |  |
|  |  | do not use |  | do not use |  | do not use |  |  |

Якщо група безпеки не застосовується, Azure дозволяє весь трафік. Це може становити серйозну загрозу, особливо якщо операційна система не надає брандмауер.

### Правила за замовчуванням

#### Правило «Заборонити все»

* за замовчуванням
* додане в кожну групу безпеки
* для вхідного і вихідного трафіку
* з найнижчим пріоритетом 65500 - це означає, що для проходження трафіку через групу безпеки необхідно дозволяюче правило. В іншому випадку трафік буде заблокований останнім правилом за замовчуванням.





#### Правила вихідного трафіку

Додатки можуть виконувати будь-які вихідні запити:

* до Інтернету
* в межах віртуальної мережі



#### Правила вхідного трафіку

* дозволено тільки з віртуальної мережі (наприклад, інші ресурси в тій же локальній мережі)
* з Azure Load Balancer

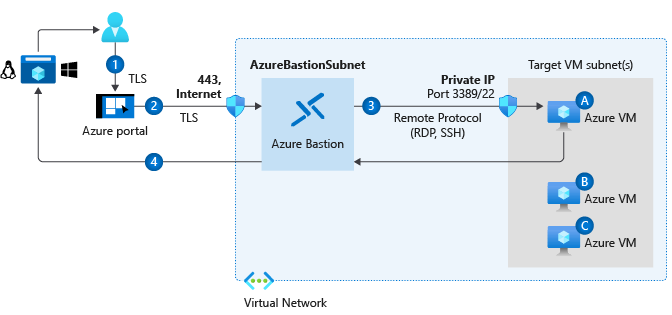


### Effective security rules

* можна перевірити правила безпеки, які застосовуються до мережевого інтерфейсу
* ВМ має бути включена

## Azure Bastion

### Властивості



* розгортається на рівні віртуальної мережі, а не підписки, облікового запису або віртуальної машини
* забезпечує безпечне і просте підключення по протоколу RDP або SSH до віртуальних машин безпосередньо з порталу Azure за допомогою протоколу TLS
* забезпечує підключення до всіх віртуальних машин у віртуальній мережі, в яких він був доданий
* ВМ не потрібні загальнодоступні IP-адреси, агенти або спеціальне клієнтське ПЗ, використовується приватна IP-адреса на віртуальній машині

### Переваги та недоліки

#### Переваги:

* Захист від сканування портів: оскільки вам не потрібно надавати свої віртуальні машини в загальнодоступний Інтернет, ваші віртуальні машини захищені від сканування портів неавторизованих користувачів і користувачами-зловмисниками, розташованими за межами вашої віртуальної мережі.

#### Недоліки:

* дорого коштує

### Правила групи безпеки мережі

Для роботи Бастіону Azure група безпеки мережі повинна дозволити наступний трафік:

|  |  |
| --- | --- |
| Напрямок | Allow/ Not deny |
| Вхідний трафік | Підключення RDP і SSH з діапазону IP-адрес підмережі Бастіону Azure до підмережі віртуальної машини. |
| Вхідний трафік | Доступ TCP з Інтернету через порт 443 до загальнодоступного IP-адресою Бастіону Azure. |
| Вхідний трафік | Доступ TCP з диспетчера шлюзу Azure через порти 443 або 4443. Диспетчер шлюзу Azure управляє з'єднаннями порталу зі службою «Бастіон Azure". |
| Вихідний трафік | Доступ TCP з платформи Azure через порт 443. Цей трафік використовується для журналу ведення діагностики. |