

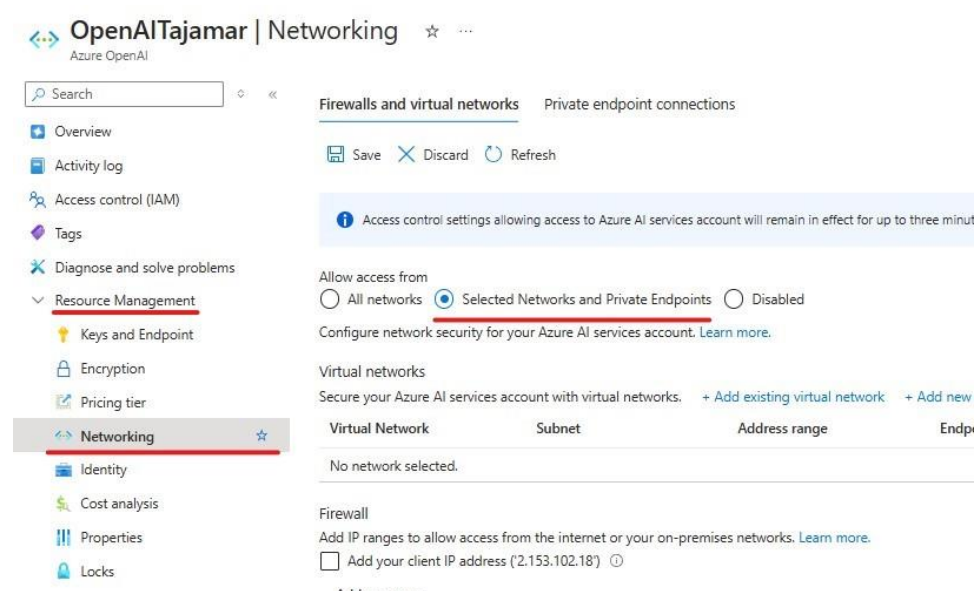
Restringir acceso a OpenAI a una subred

Se deben crear los siguientes servicios:

- Virtual Network
- Subnet
- Network Security group
- Application Security group
- Private Endpoint

Vamos a nuestro recurso **OpenAI**

Clicleamos en **Networking** en la parte izquierda -> **Selected Networks and Private Endpoints**



Deberíamos seleccionar una **Virtual network**, pero no tenemos ninguna creada. Crearemos una.

Crear **virtual network**, seleccionar **resource group**, seleccionar nombre y región.

Project details

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

Subscription *

Resource group *

[Create new](#)

Instance details

Virtual network name *

Region *

[Deploy to an Azure Extended Zone](#)

En la seccion **IP addresses** , seleccionar **Add a subnet**

Seleccionamos **Next y Crear**.

Una vez creada la **virtual network**, seleccionamos la **subnet** (subred1)

Si no está creada, vamos a **Settings** -> **subnets** -> pinchar en **+Subnet**

Cambiar nombre (ej: subred1)

arch resources, services, and docs (G+)

Home > openai

openai | Virtual network

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender Cloud

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose

Name *

IPv4

Include an IPv4 address space ☒

IPv4 address range *

10.0.0.0 - 10.0.255.255

Starting address *

Size

Subnet address range

IPv6

[Add](#) [Cancel](#) [Give feedback](#)

IPv4 address range: +65.000 IP desde 10.0.0.0 hasta 10.0.255.255

Starting address: 10.0.1.0

Size: /24 (256 addresses)

A continuación, crearemos un recurso **Network security group**

Create network security group ...

Basics Tags Review + create

Project details

Subscription *	Azure for Students
Resource group *	openai

[Create new](#)

Instance details

Name *	openai-NSG
Region *	East US

Se puede poner reglas de entrada, que rangos de IP y en qué puertos, quién puede acceder

Necesitaremos crear un Grupo de Seguridad de Aplicación.

Vamos a create **Application Security Group**

Lo siguiente será ir a nuestro recurso de OpenAI y crear un endpoint privado.

Vamos a **Resource groups** -> **OpenAI** -> **Networking** -> **Private Endpoints connections** -> **+Private Endpoint**

Create a private endpoint ...

⚠ Changes you make on this tab may affect any configuration you've done on other tabs. Review all options prior to creating the private endpoint.

✓ Basics ② Resource ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * ⓘ	Azure for Students
Resource group * ⓘ	openai

[Create new](#)

Instance details

Name *	openai-private-endpoint
Network Interface Name *	openai-private-endpoint-nic
Region *	East US

En la sección **Virtual network**:

Seleccionamos la Virtual network creada y la subnet.

Private IP configuration: **Dynamically allocate IP address**

Seleccionamos el **Application security group** creado anteriormente.

Create a private endpoint ...

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network ① openai-vn (openai)

Subnet * ① subred1

Network policy for private endpoints Disabled (edit)

Private IP configuration

☒ Dynamically allocate IP address

☐ Statically allocate IP address

Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)

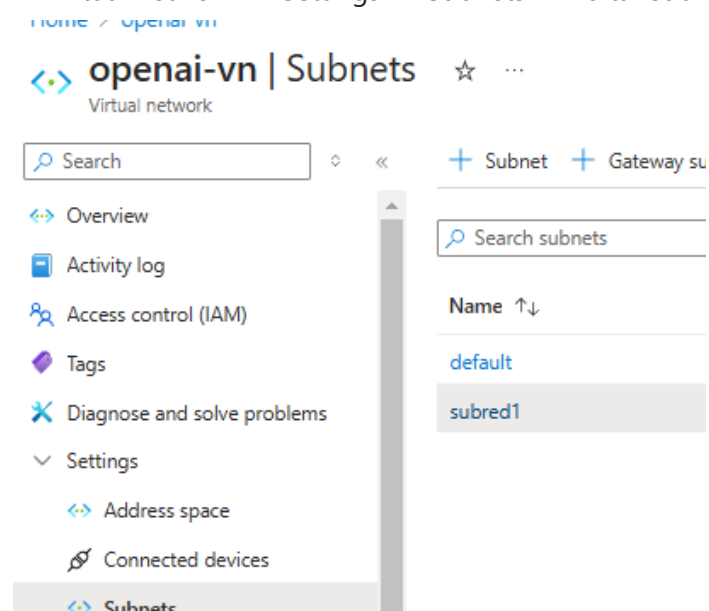
[+ Create](#)

Application security group

openai-ASG

Clickeamos en **Next** y **Crear** para crear el **private endpoint**

En virtual network -> Settings -> Subnets -> Editar subnet (subred1)



En la sección **Security**:

Network security group: seleccionar que recién creado

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#)

NAT gateway [ⓘ]

i A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Network security group [ⓘ]

Route table


Ahora iremos a nuestro servicio **Network Security Group** , en **Settings** en la parte izquierda, vamos a **Inbound security rules** -> **+Add** con esto añadiremos reglas de acceso.

[Home](#) > [openai-NSG](#)


openai-NSG | Inbound security rules ☆ ⋮

Network security group


[+ Add](#) [Hide default rules](#) [Refresh](#)


 Overview


 Activity log


 Access control (IAM)

 Tags

 Diagnose and solve problems

 Settings

 **Inbound security rules**

 Outbound security rules

Network security group security rules are evaluate same priority and direction as an existing rule. You

	Priority ^{↑↓}	Name ^{↑↓}
<input type="checkbox"/>	65000	AllowVnetInBou
<input type="checkbox"/>	65001	AllowAzureLoa
<input type="checkbox"/>	65500	DenyAllInBoun

Source: Application security group

Seleccionamos nuestro **application security group creado**

Ranges -> *

Destination -> Any

Destination port ranges -> 443

Action -> Allow

Priority -> 100



Add inbound security rule

openai-NSG

Source ⓘ

Application security group

Source application security groups

openai-ASG

No application security groups found

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges * ⓘ

443

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMPv4

Click en Add

Crear otra pero cambiando configuración:

Source -> Any

Destination -> Application security group

Service -> Custom

Destination port ranges -> 443

Action -> Deny

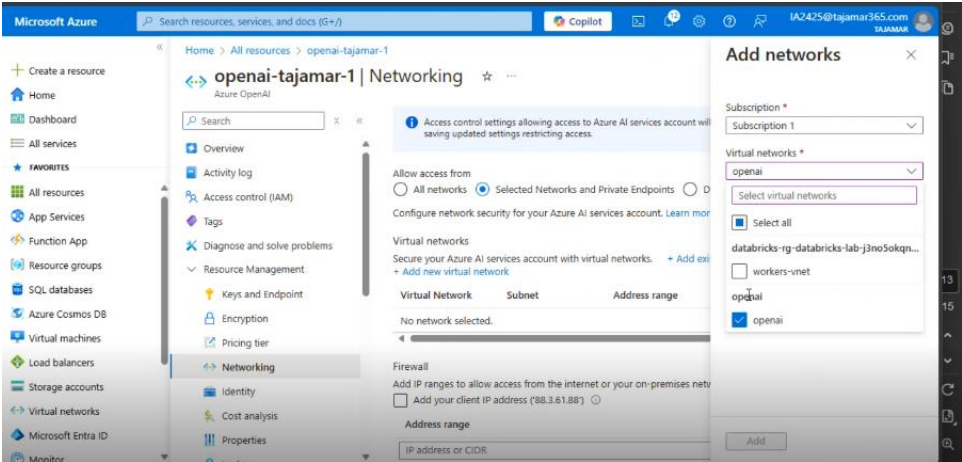
Priority -> 110

Ranges -> *

Si la otra falla, si no se permite el acceso por la de priority 100, la siguiente a evaluar será la de 110.

Denegará el acceso a cualquiera que no esté permitido en esta regla 100.

Por último, vamos a nuestro recurso de Azure OpenAI,
Azure OpenAI -> Resource Management -> Networking -> Selected Networks and Private Endpoints -> **+Add existing network**



Elegir virtual network

Elegir subred

Clickear en Enable

Add n

... Enabling service endpoints

Enabling service endpoints for 1 virtual network(s).

Subscription

Azure for Students

Virtual networks

openai-vn

Subnets

subred1 (Service endpoint required)

Waiting for the networks to finish updating in response to enabling service endpoints for 'Microsoft.CognitiveServices'.

Virtual network	Service endpoint status
openai-vn	...
subred1	Updating

Si se quiere dar acceso a un recurso solamente a una IP -> ponerlo en Adress range la IP que pueda acceder.