



AZURE Y VNETS



5 DE DICIEMBRE DE 2025

ALEJANDRO SAINZ SAINZ
CLOUD COMPUTING

1	EXPLICACIÓN DE LA PRÁCTICA.....	4
2	COMENZANDO	4
3	PREGUNTAS ADICIONALES.....	13

Captura 1 1- Creación de la Red Virtual	4
Captura 1 2 Al final fue Suiza.....	5
Captura 1 3 La creación de las Subredes.....	5
Captura 1 4 Creando máquina Virtual de Front.....	6
Captura 1 5 Creación de la MV Back	6
Captura 1 6 Asignación de Subredes	7
Captura 1 7 Creando reglas de E/S.....	7
Captura 1 8 Archivo RDP.....	8
Captura 1 9 Escritorio de front	8
Captura 1 10 Las dos MV	8
Captura 1 11 De esto me entero lo justo.....	9
Captura 1 12 Progresando.....	10
Captura 1 13 Al fin resultados.....	10
Captura 1 14 La inversa también	11
Captura 1 15 IIS.....	11
Captura 1 16 Primero Front	12
Captura 1 17 Repetimos	12
Captura 1 18 Parece que bien	13

1 EXPLICACIÓN DE LA PRÁCTICA

En esta práctica tenemos que crear una red virtual en Azure con dos subredes. Se crearán dos MV después y se asignará cada una a una de las subredes. Después tenemos que conseguir que se vean la una a la otra. Para finalizar, debemos desplegar un servidor web en una MV y acceder a él desde la otra MV.

En esta práctica he tenido una serie de problemas. Puede ser que me haya saltado algún paso en la configuración de la red virtual, o algún paso en la configuración de red de las MV. Al final, no voy a esconderlo, tuve que tirar de IA y buscar ayuda para resolverlo, ya que hubo una serie de formas de localizar el problema que yo no conocía ni por asomo.

Sin más, vamos al lío.

2 COMENZANDO

Lo primero que tenemos que hacer es acceder a la plataforma de Azure y crear una red virtual.

Crear red virtual

Datos básicos Seguridad Direcciones IP Etiquetas Revisar y crear

Detalles del proyecto

Seleccione la suscripción para administrar recursos implementados y los costes. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.

Suscripción *	Azure for Students
Grupo de recursos *	ExamenDecroly
	Crear nuevo

Detalles de instancia

Nombre de red virtual *	red_virtual_prueba
Región *	(Europe) West Europe
Implementación en una zona extendida de Azure	

Anterior

Siguiente

Revisar y crear

Captura 1 1- Creación de la Red Virtual

Como vemos en la captura superior, debemos indicar la suscripción, el grupo de recursos, nombre y región. Ahora, no sé por qué, no me vale cualquier región. Así que, a probar varias, hasta dar con la que vale.

Cree subredes para segmentar el espacio de direcciones de la red virtual en intervalos más pequeños para que lo usen las aplicaciones. Al implementar recursos en una subred, Azure asigna al recurso una dirección IP de la subred.

Nombre	IPv4	IPv6	Direcciones IP ...	Delegado a	Grupo de segu...	Tabla de rutas
default	10.0.0.0/24	-	251	-	-	
front	10.0.1.0/24	-	251	-	-	
back	10.0.2.0/24	-	251	-	-	

Captura 1 2 Al final fue Suiza

Tras probar varias veces, con Suiza del norte, pude crear la red virtual. Además, en la configuración de esta red, creé las dos subredes que se ven en la imagen. Aquella con el nombre default, es una subred que viene por defecto. Luego más adelante se borra para que no coincida con la dirección de red de nuestra red principal.

Agregar una subred

10.0.0.0/16 Eliminar espacio de direcciones

10.0.0.0 /16 10.0.0.0 - 10.0.255.255 65.536 direcciones

Subredes	Intervalo de direcciones IP	Tamaño	NAT Gateway
frontend	10.0.1.0 - 10.0.1.255	/24 (256 direcciones)	-
backend	10.0.2.0 - 10.0.2.255	/24 (256 direcciones)	-

Anterior Siguiente

Captura 1 3 La creación de las Subredes

Para que se vea lo explicado en el punto anterior, aquí podemos ver la captura de la pantalla en la que se crean las dos subredes de las que hemos hablado.

MicrosoftWindowsDesktop.Windows-10-rs5-e-20251202181911 | Información general

Nombre de implementación: CreateVm-MicrosoftWindowsDesktop... Hora de inicio: 2/12/2025, 18:21:13
Suscripción: Azure for Students Id. de correlación: 92117ef8-f1cf-42f7-b220-e29a393ade
Grupo de recursos: Redes

Recurso	Tipo	Estado	Detalles de la operación
front	Microsoft.Compute/virtual...	Created	Detalles de la operación
front151_z1	Microsoft.Network/networkl...	OK	Detalles de la operación
front-ip	Microsoft.Network/publicclp...	OK	Detalles de la operación
frontnsg854	Microsoft.Network/network...	OK	Detalles de la operación

Enviar comentarios
Cuéntenos su experiencia con la implementación

Microsoft Defender for Cloud
Proteja sus aplicaciones e infraestructura.
[Ir a Microsoft Defender for Cloud >](#)

Tutoriales gratuitos de Microsoft
[Comience a aprender hoy >](#)

Trabajar con un experto
Los expertos de Azure son asociados proveedores de servicios que pueden ayudar a administrar sus recursos en Azure y ser la primera línea de soporte técnico.
[Buscar un experto de Azure >](#)

Captura 1 4 Creando máquina Virtual de Front

Como se nos pide en el ejercicio, debíamos crear dos máquinas virtuales. En este caso son dos máquinas idénticas de Windows 10 LTSC. No sé si eso tendrá que ver con algunos de los problemas que vienes más adelante.

Nombre de implementación: CreateVm-MicrosoftWindowsDesktop... Hora de inicio: 2/12/2025, 18:23:56
Suscripción: Azure for Students Id. de correlación: 8df629f8-564a-4d41-957f-3eeb91532
Grupo de recursos: Redes

Recurso	Tipo	Estado	Detalles de la operación
back	Microsoft.Compute/virtual...	Created	Detalles de la operación
back80_z1	Microsoft.Network/networkl...	OK	Detalles de la operación
back-nsq	Microsoft.Network/network...	OK	Detalles de la operación
back-ip	Microsoft.Network/publicclp...	OK	Detalles de la operación

Enviar comentarios
Cuéntenos su experiencia con la implementación

Microsoft Defender for Cloud
Proteja sus aplicaciones e infraestructura.
[Ir a Microsoft Defender for Cloud >](#)

Tutoriales gratuitos de Microsoft
[Comience a aprender hoy >](#)

Trabajar con un experto
Los expertos de Azure son asociados proveedores de servicios que pueden ayudar a administrar sus recursos en Azure y ser la primera línea de soporte técnico.
[Buscar un experto de Azure >](#)

Captura 1 5 Creación de la MV Back

Una vez finaliza la implementación de la primera MV, procedemos a crear la segunda. Idéntica. Nada más que comentar.

Dispositivo ↑	Tipo ↑	Dirección IP ↑	Subred ↑
front151_z1	Interfaz de red	10.0.1.4	front
back80_z1	Interfaz de red	10.0.2.4	back

Captura 1 6 Asignación de Subredes

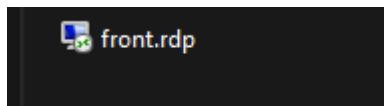
Una vez terminamos con la implementación de las MV, debemos asignarlas a las subredes correspondientes.

Nombre	Puerto	Protocolo	Origen	Destino	Acción
Reglas de puerto de entrada (6)					
300 RDP	3389	TCP	Cualquiera	Cualquiera	Allow
310 TCP	8080	TCP	Cualquiera	Cualquiera	Allow
320 Ping	Cualquiera	ICMP	Cualquiera	Cualquiera	Allow
65000 AllowVnetInBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	Allow
65001 AllowAzureLoadBalancerInBound	Cualquiera	Cualquiera	AzureLoadBalancer	Cualquiera	Allow
65500 DenyAllInBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Deny
Reglas de puerto de salida (5)					
330 PingS	Cualquiera	ICMP	Cualquiera	Cualquiera	Allow
340 TCPS	8080	TCP	Cualquiera	Cualquiera	Allow
65000 AllowVnetOutBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	Allow
65001 AllowInternetOutBound	Cualquiera	Cualquiera	Cualquiera	Internet	Allow
65500 DenyAllOutBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Deny

Captura 1 7 Creando reglas de E/S

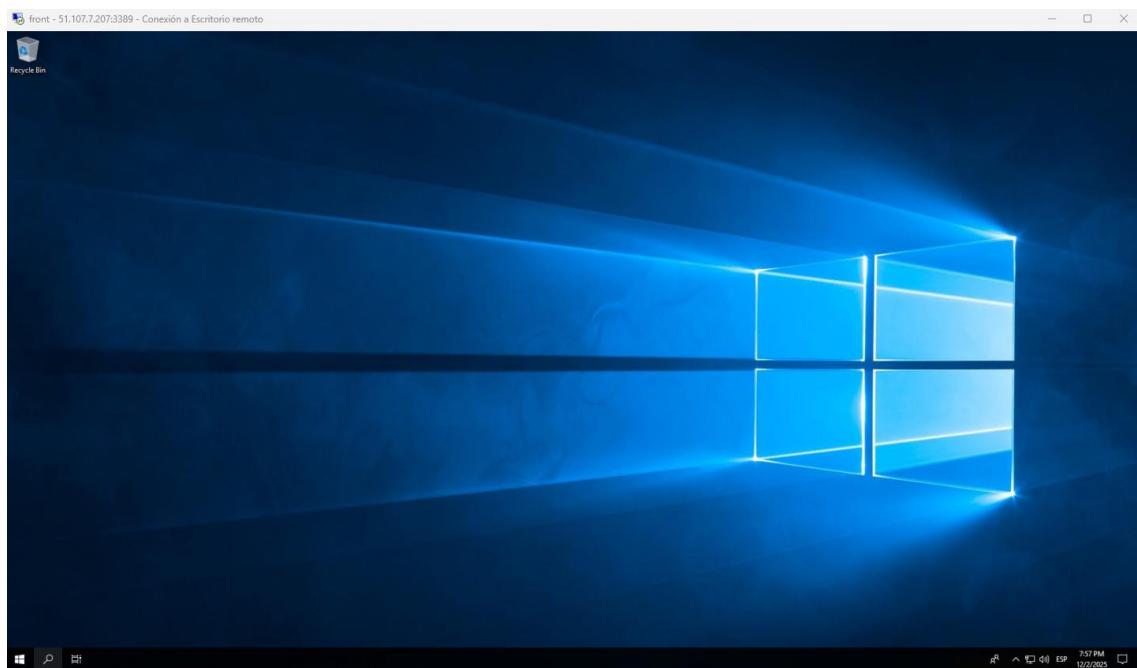
Para asegurarme de la visibilidad y la conectividad de las máquinas, debo repetir este paso en las dos máquinas. Debo crear reglas de E/S para ICMP, el ping, y TCP, la conexión a internet estándar. Además, debo de asegurarme de que hay entradas para RDP, para permitir la entrada por escritorio remoto, y que aparezcan todas las reglas referentes a la red virtual. Esas son el resto que aparecen en la foto en color gris claro.

Ahora lo que debo de hacer es descargar los archivos RDP de cada MV para poder conectarme remotamente a ellas.



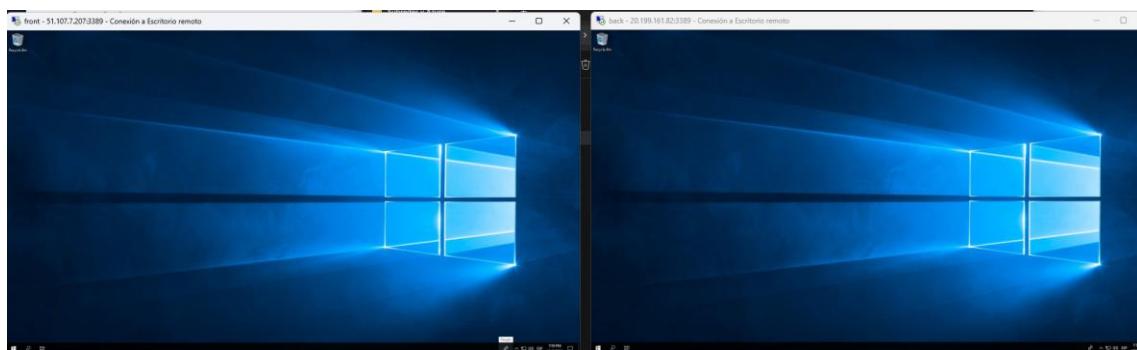
Captura 1 8 Archivo RDP

Usando estos archivos y dirigiéndome a la IP pública de cada una de las MV puedo acceder a sus sistemas.



Captura 1 9 Escritorio de front

Como vemos en la captura anterior, puedo acceder sin problemas a la MV.



Captura 1 10 Las dos MV

En esta otra captura ya tengo acceso a las dos. Eso sí, a una de ellas le tendría que haber cambiado el fondo de escritorio, para diferenciarlas.

Y ahora comenzaron los problemas. Parece ser que Azure, y muy posiblemente, Microsoft en general, deshabilitan la opción de que equipos en diferentes subredes se puedan ver mediante el explorador de red. Así que tenemos que recurrir al fiable ping.

La cosa es que, en mi caso, ni de una a otra, se veían de ninguna forma. Así que toca remar.

Parece ser, que en Azure, para las redes virtuales existen una serie de parámetros, los NSG que gestionan la conectividad de equipos en redes y subredes. Además, si estas máquinas están creadas y conectadas a redes públicas, como si fuese la de casa, no tienen conectividad con otras subredes de la misma red.

Lo segundo algo sabía, lo primero no. Además, por alguna razón, no encontré la manera de cambiarlo de manera gráfica. Y aquí es donde entra nuestro profesor digital, que me pasó una serie de comandos para PowerShell para comprobar ciertas cosas.

```

Core Networking - Time Exceeded (ICMPv6-In) True Inbound Any
Core Networking - Time Exceeded (ICMPv6-Out) True Outbound Any
Core Networking - Parameter Problem (ICMPv6-In) True Inbound Any
Core Networking - Parameter Problem (ICMPv6-Out) True Outbound Any
Core Networking - Neighbor Discovery Solicitation (ICMPv6-In) True Inbound Any
Core Networking - Neighbor Discovery Solicitation (ICMPv6-Out) True Outbound Any
Core Networking - Neighbor Discovery Advertisement (ICMPv6-In) True Inbound Any
Core Networking - Neighbor Discovery Advertisement (ICMPv6-Out) True Outbound Any
Core Networking - Router Advertisement (ICMPv6-In) True Inbound Any
Core Networking - Router Advertisement (ICMPv6-Out) True Outbound Any
Core Networking - Router Solicitation (ICMPv6-In) True Inbound Any
Core Networking - Router Solicitation (ICMPv6-Out) True Outbound Any
Core Networking - Multicast Listener Query (ICMPv6-In) True Inbound Any
Core Networking - Multicast Listener Query (ICMPv6-Out) True Outbound Any
Core Networking - Multicast Listener Report (ICMPv6-In) True Inbound Any
Core Networking - Multicast Listener Report (ICMPv6-Out) True Outbound Any
Core Networking - Multicast Listener Report v2 (ICMPv6-In) True Inbound Any
Core Networking - Multicast Listener Report v2 (ICMPv6-Out) True Outbound Any
Core Networking - Multicast Listener Done (ICMPv6-In) True Inbound Any
Core Networking - Multicast Listener Done (ICMPv6-Out) True Outbound Any
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In) True Inbound Any
File and Printer Sharing (Echo Request - ICMPv4-In) False Inbound Domain
File and Printer Sharing (Echo Request - ICMPv4-Out) False Outbound Domain
File and Printer Sharing (Echo Request - ICMPv6-In) False Inbound Domain
File and Printer Sharing (Echo Request - ICMPv6-Out) False Outbound Domain
File and Printer Sharing (Echo Request - ICMPv4-In) False Inbound Private, Public
File and Printer Sharing (Echo Request - ICMPv4-Out) False Outbound Private, Public
File and Printer Sharing (Echo Request - ICMPv6-In) False Inbound Private, Public
File and Printer Sharing (Echo Request - ICMPv6-Out) False Outbound Private, Public

PS C:\Users\alex> New-NetFirewallRule `>> -Name "Allow-ICMPv4-In" `>> -DisplayName "Allow ICMPv4 In" `>> -Protocol ICMPv4 `>> -IcmpType 8 `>> -Direction Inbound `>> -Action Allow `>> -Profile Any
>>

```

Captura 1 11 De esto me entero lo justo.

En la parte de debajo de la imagen vemos como los protocolos ICMP, tanto entrada como salida, trabajan en los dos ámbitos, público y privado. Y también parece ser, siempre prevalece el más restrictivo dependiendo de que se quiera hacer. Por eso, de serie, la MV opta por la opción pública y no es capaz de encontrar el otro dispositivo situado en otra subred.

Así que, la IA, me da una serie de indicaciones para cambiar ciertas entradas de ICMP. Lo raro, es que esto ya lo había habilitado yo en la plataforma de Azure para cada máquina. Pero bueno, la tecnología es la tecnología.

```
PS C:\Users\alex> New-NetFirewallRule `>> -Name "Allow-ICMPv4-In" `>> -DisplayName "Allow ICMPv4 In" `>> -Protocol ICMPv4 `>> -IcmpType 8 `>> -Direction Inbound `>> -Action Allow `>> -Profile Any `>>

Name          : Allow-ICMPv4-In
DisplayName   : Allow ICMPv4 In
Description   :
DisplayGroup :
Group        :
Enabled       : True
Profile      : Any
Platform     : {}
Direction    : Inbound
Action       : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner         :
PrimaryStatus : OK
Status        : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource  : PersistentStore
PolicyStoreSourceType : Local
```

Captura 12 Progresando

Aquí vemos como agregamos otra nueva regla de entrada y salida. Comentar, que estos comandos hay que hacerlos en cada máquina, pero, indicando que, por alguna razón, la MV de back ya estaba creada con conexión a red privada y no a pública. No sé porque una sí y la otra no, pero así fue.

```
20.199.161.82 - Conexión a Escritorio remoto
Administrator: Windows PowerShell
Recycle Bin

PS C:\Users\alex> Get-NetFirewallRule -Name "Allow-ICMPv4-In" | >> Select DisplayName, Enabled, Direction, Profile | Format-Table -AutoSize
>>
DisplayName      Enabled Direction Profile
-----      -----  -----
Allow ICMPv4 In  True    Inbound   Any

PS C:\Users\alex> ping 10.0.2.4
Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time<1ms TTL=128
Reply from 10.0.2.4: bytes=32 time<1ms TTL=128
Reply from 10.0.2.4: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.2.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\alex> ping 10.0.1.4
Pinging 10.0.1.4 with 32 bytes of data:
Request timed out.

Ping statistics for 10.0.1.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\alex>
```

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.8027]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\alex>ping 10.0.2.4
Pinging 10.0.2.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\alex>ping 10.0.2.4
Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\alex>
```

Captura 13 Al fin resultados

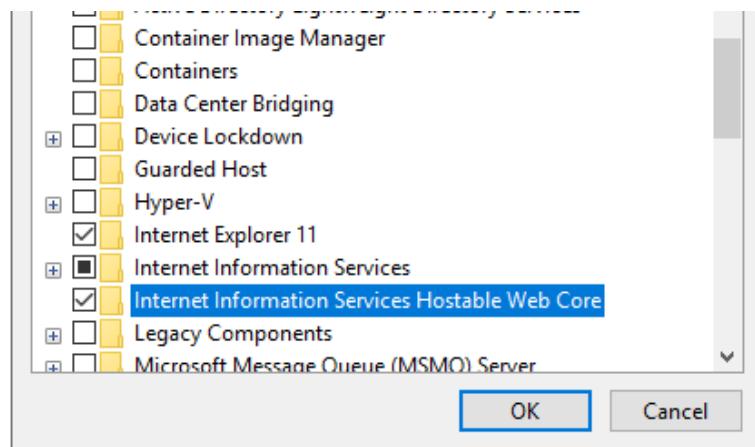
Ya por fin, pude hacer ping de front a back. Ya era una sensación de progreso.

```
Request timed out.  
Ping statistics for 10.0.1.4:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
PS C:\Users\alex> ping 10.0.1.4  
  
Pinging 10.0.1.4 with 32 bytes of data:  
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128  
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128  
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128  
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
```

Captura 1 14 La inversa también

Una vez duplicados los pasos, de back a front también pude hacer ping.

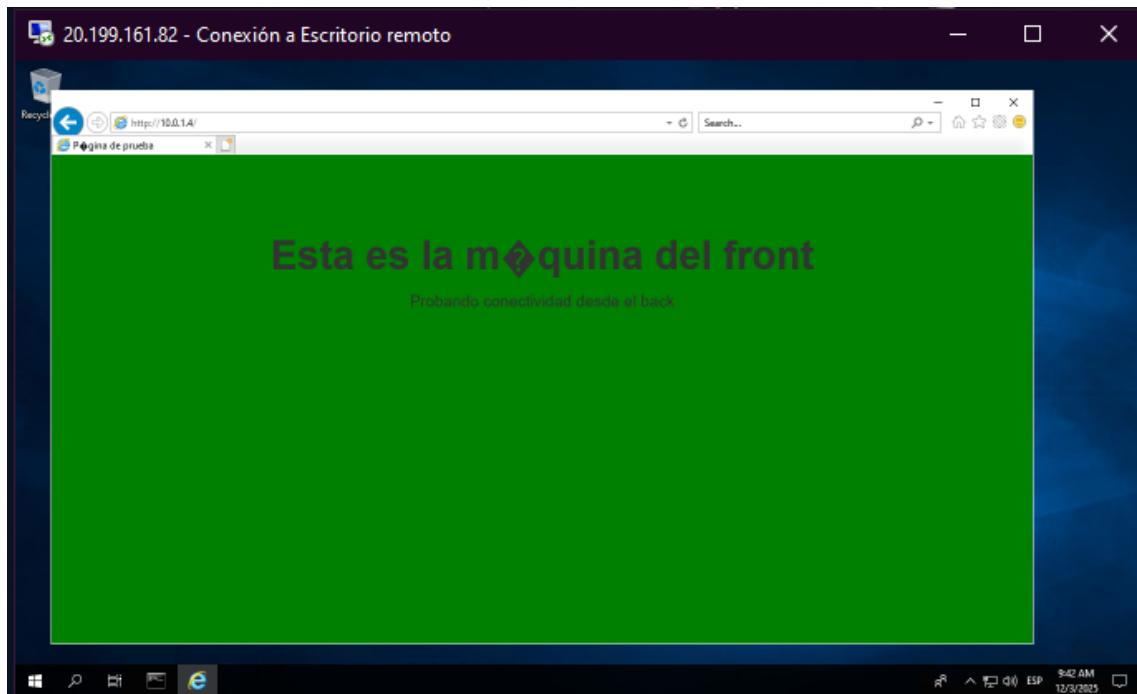
Una vez hecho todo esto, ya solo faltaba habilitar un servidor web, cosa que ya habíamos hecho antes. Y ya que todo lo había tenido que hacer por duplicado, esto también.



Captura 1 15 IIS

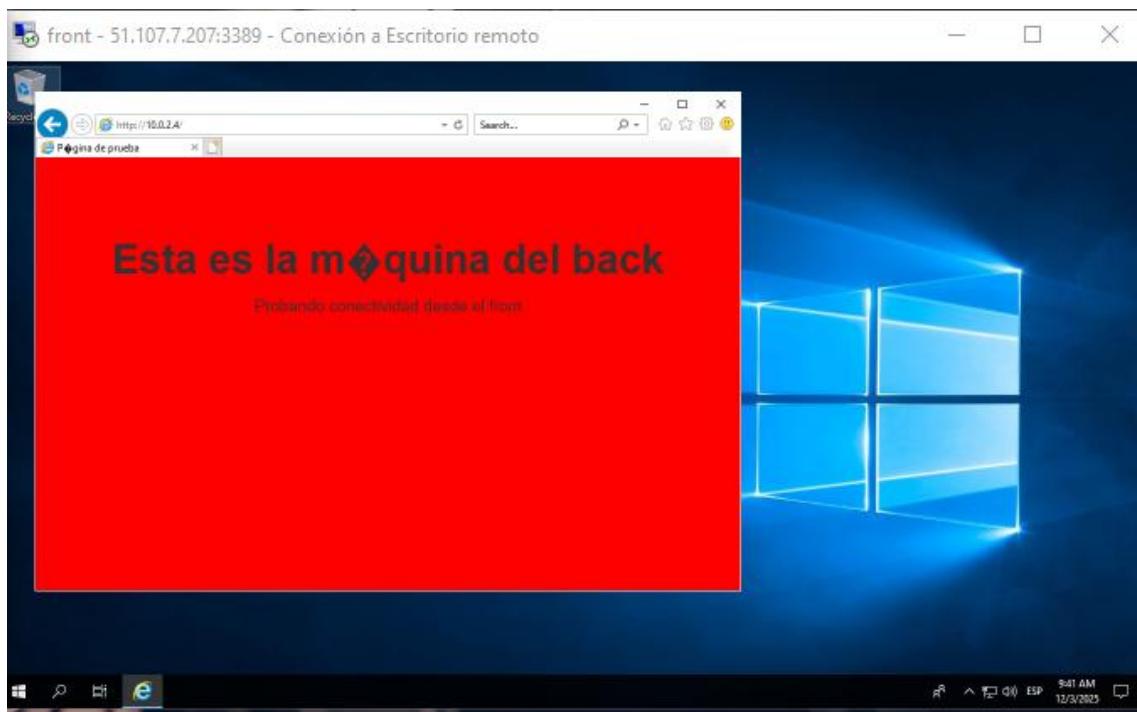
En las dos MV habilitamos y levantamos los servicios IIS, para poder alojar webs.

Genero dos páginas idénticas de las que solo tengo que modificar alguna cosilla, esta vez sí, para que se diferencien una y otra.



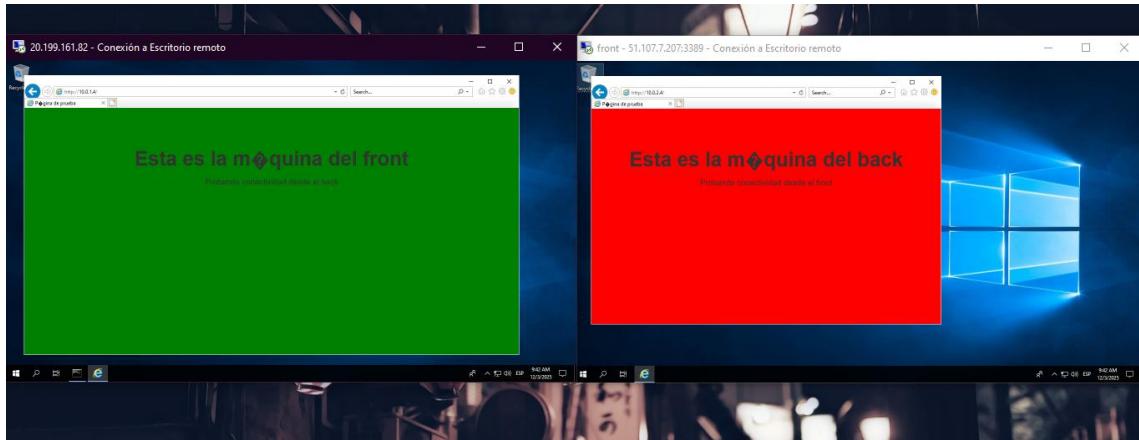
Captura 1 16 Primero Front

Después de preparar IIS en front y alojar una página web, hago una prueba desde back. Se conecta y ve la página.



Captura 1 17 Repetimos

Hago lo mismo en back, y probamos desde front.



Captura 1 18 Parece que bien

Una vez terminadas las pruebas, aquí podemos ver las dos webs. Cada una en su máquina vista desde la otra.

Y con esto damos por terminada esta actividad.

3 PREGUNTAS ADICIONALES

¿Puedo acceder al servicio web desde mi equipo personal?

Basándome en la prueba que he hecho yo, no. Si se me preguntan los motivos, yo me decantaría por pensar que esos equipos tienen salida a internet porque tienen una ip pública, pero esos equipos dan servicio a través de su ip privada, no de la pública. Para eso supongo que tendríamos que establecer una regla para que al acceder por el puerto 80, su Gateway nos diese acceso a lo alojado en el puerto 80 de esa ip privada.

¿Cómo podemos asegurarnos para que un recurso de una subred sea accesible desde otros puntos de la red?

Pues imagino que a través de configuración de reglas de E/S, de tablas de enrutamiento, de plantillas de Grupos de Seguridad (lo que comenté antes de las NSG de Azure) y seguramente de alguna otra cosa que no conozco como opciones de configuración de la Gateway para redirigir el tráfico de red o para exponer un servicio Local a otros fragmentos de la misma red virtual.