Actividad 2.1.3
Creación y configuración del grupo de seguridad de red

CONTENIDO

1.- Objetivos

- Conocer el servicio de grupo de seguridad de Azure
- Crear un grupo de seguridad de red para proteger recursos en red
- Configurar en el grupo de seguridad reglas de entrada para permitir el acceso a cualquier máquina de las redes por SSH (puerto 22) y RDP (puerto 3389)
- Asociar el grupo de seguridad creado a las dos redes creadas previamente
- Entender cómo varios grupos de seguridad pueden actuar en conjunto

2.- Requisitos previos

Que el centro haya proporcionado una cuenta del tipo @iesclaradelrey.es, válida para iniciar sesión en los distintos servicios de Microsoft.

Que se hayan realizado las actividades previas en las que:

- Se activaba la cuenta y la suscripción de Azure for Students.
- Se creaban redes virtuales.

3.- Calificación

Para superar la actividad bastará con entregar una captura de pantalla en la que se vea el listado de reglas en el grupo de seguridad. Algo similar a esto:

Prioridad	Nombre	Puerto	Protocolo	Origen	Destino	Acc
Reglas de seguridad de entrada						
100	AllowAnySSHInbo...	22	TCP	Cualquiera	Cualquiera	✓
110	AllowAnyRDPInbo...	3389	TCP	Cualquiera	Cualquiera	✓
65000	AllowVnetInBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	✓
65001	AllowAzureLoadBalan...	Cualquiera	Cualquiera	AzureLoadBalancer	Cualquiera	✓
65500	DenyAllInBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	✗
Reglas de seguridad de salida						
65000	AllowVnetOutBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	✓
65001	AllowInternetOutBound	Cualquiera	Cualquiera	Cualquiera	Internet	✓
65500	DenyAllOutBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	✗

La plataforma Azure es un sistema en constante cambio y evolución, por lo que cualquier captura de pantalla de esta actividad puede ser diferente a la pantalla real actual.

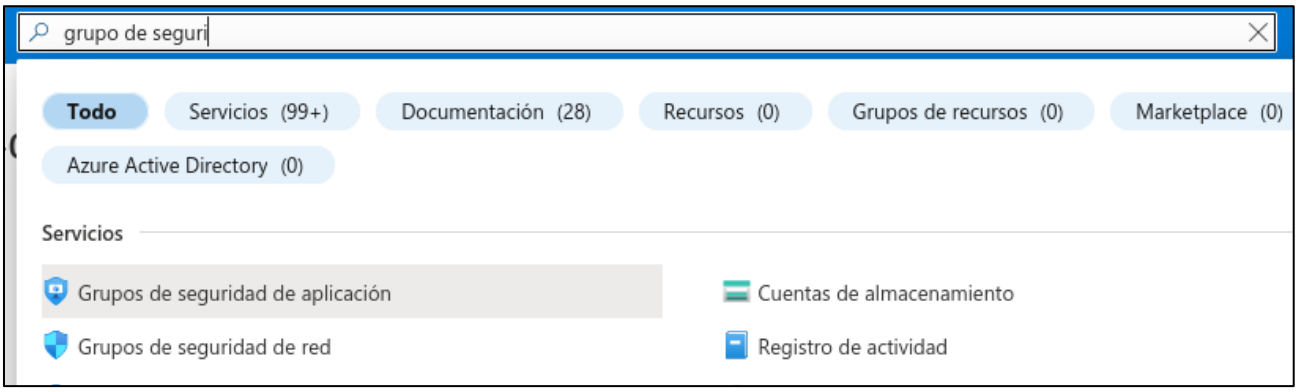
4.- Actividades a realizar

Un grupo de seguridad de red en Azure es un recurso que permite limitar el tráfico desde y/o hacia otros recursos de Azure. Podría ser algo muy similar a un firewall, pero muy específico de la infraestructura en Azure. Para más información se recomienda la lectura del siguiente artículo de Microsoft Ignite:

https://learn.microsoft.com/es-es/azure/virtual-network/network-security-groups-overview

4.1.- Creación del grupo de seguridad

Usando el buscador general del portal de Azure, acceder a la página "Grupos de seguridad de red"



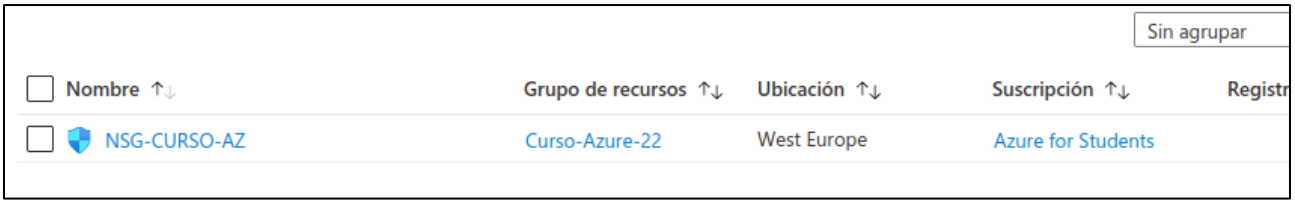
El listado de grupos de seguridad aparece vacío si no se ha creado ningún grupo previamente.

Clic en "Crear", y aparecerá el formulario para crear el grupo. En este formulario hay que completar:

- Suscripción y grupo de recursos. Usaremos el grupo de recursos creado en anteriores actividades.
- Nombre del grupo de seguridad.
- Región. Por defecto usará la misma que el grupo de recursos que hayamos elegido.

Se pulsa "Revisar y crear" y luego "Crear".

Una vez completada la creación del grupo, lo tendremos disponible en el listado de grupos de seguridad.



Y haciendo clic en el nombre del grupo accederemos a su configuración.

4.2.- Añadir reglas para permitir conexiones entrantes SSH y RDP

La página de configuración del grupo de seguridad muestra las reglas predefinidas por defecto, y que no se pueden eliminar ni modificar:

Prioridad	Nombre	Puerto	Protocolo	Origen	Destino	Acción
Reglas de seguridad de entrada						
65000	AllowVnetInBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Cualquiera	Cualquiera	AzureLoadBalancer	Cualquiera	Allow
65500	DenyAllInBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Deny
Reglas de seguridad de salida						
65000	AllowVnetOutBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Cualquiera	Cualquiera	Cualquiera	Internet	Allow
65500	DenyAllOutBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Deny

Vamos a añadir la regla para permitir SSH entrante. Para ver las reglas de seguridad de entrada, hacemos clic, en el menú del recurso, en la opción “Reglas de seguridad de entrada”. Aparecerán sólo las reglas de entrada. Hacemos clic en “Agregar” y aparecerá un formulario en el que tenemos que completar los siguientes campos:

- Origen. Desde donde se reciben las conexiones. Elegimos “Any”, pero puede ser:
  - Any: cualquier origen
  - IP Addresses: un rango de direcciones IP
  - My IP address: calcula la IP desde la que estamos conectando al portal de Azure
  - Service Tag: Un sistema para englobar en etiquetas distintos orígenes de conexión.
  - Application Security Group. Otro tipo de grupo de seguridad que hay que definir previamente.
- Intervalos de puertos de origen. Elegimos * (todos los puertos)
- Destino. Hacia donde se dirigen las conexiones. Elegimos “Any”, pero pueden ser los mismos que los usados en “Origen”, excepto que no hay la opción “My IP Address”, porque se trata de direcciones internas de la red.
- Servicio. Esto nos facilita la rápida configuración de reglas de servicios habitualmente utilizados. Si elegimos SSH automáticamente se completan los campos de Intervalos de puerto de destino y protocolo. Si se elige “Custom” hay que especificar puertos y protocolo destino.
- Acción. Permitir o denegar. En nuestro caso usamos permitir.
- Prioridad. Un número del 0 en adelante. Hay que tener en cuenta que:
  - Las reglas se evalúan según su orden de prioridad de menor a mayor (la de prioridad 5 va antes que la de prioridad 100).
  - Cuando se cumple una regla, se dejan de evaluar las de mayor orden de prioridad (mayor valor para prioridad)
  - Se recomienda dejar espacios entre las prioridades de reglas para poder ordenarlas fácilmente sin tener que andar modificando la prioridad de demasiadas reglas. Usar el 100, el 200, el 300, etc. de forma que podamos insertar la 150 si lo necesitamos, por ejemplo.
- Nombre. Nombre que damos a la regla para identificarla. Azure nos sugiere un nombre para la regla en función de los valores seleccionados.
- Descripción.

Pulsamos en agregar.

Repetir los pasos para agregar una regla para conexiones por RDP (Remote Desktop Protocol).

Una vez añadidas las dos reglas, quedará algo así:

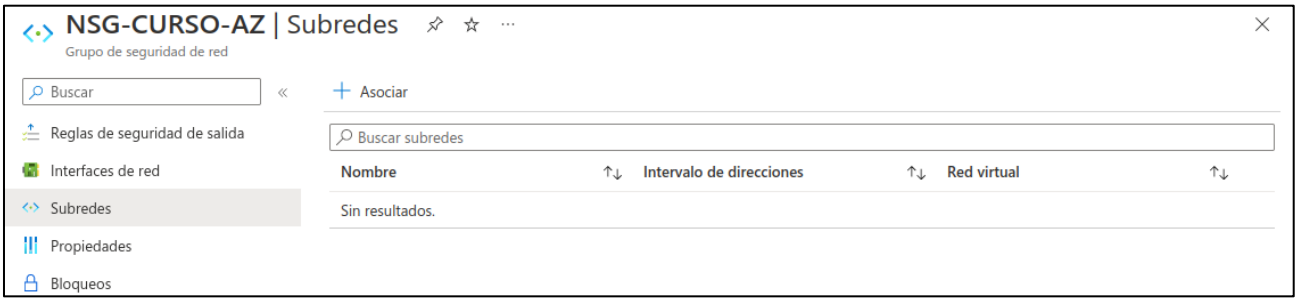
Prioridad	Nombre	Puerto	Protocolo	Origen
100	⚠ AllowAnySSHInbound	22	TCP	Cualquiera
110	⚠ AllowAnyRDPInbound	3389	TCP	Cualquiera
65000	AllowVnetInBound	Cualquiera	Cualquiera	VirtualNetwork
65001	AllowAzureLoadBalancerInBo...	Cualquiera	Cualquiera	AzureLoadBalancer
65500	DenyAllInBound	Cualquiera	Cualquiera	Cualquiera

Los iconos de advertencia informan de algún potencial problema. En este caso es que estas reglas dan acceso indiscriminado por SSH y RDP a cualquier máquina que esté conectada a una red protegida con este grupo de seguridad.

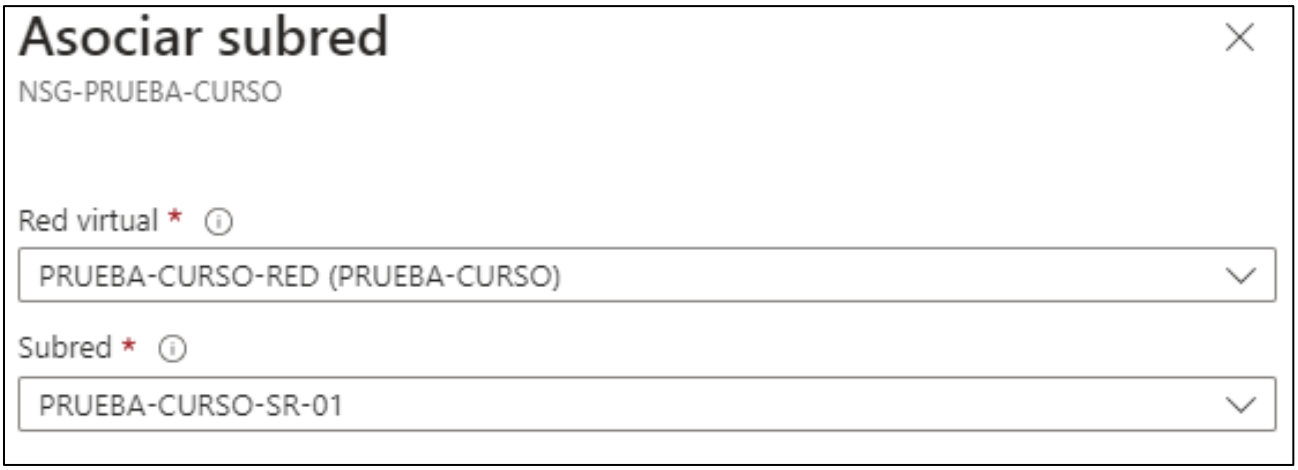
4.3.- Configurar las redes previamente creadas para que usen este grupo de seguridad de red

La configuración del grupo de seguridad se hace a nivel de subred, así que en nuestro caso tendremos que asociar el grupo de seguridad a las cuatro subredes.

Para asociar subredes al grupo de seguridad, en la página del grupo de seguridad hacemos clic en la opción de menú “Subredes”. Aparecerá el listado de subredes asociadas vacío.



Hacemos clic en “Asociar” y completamos el formulario. Sólo hay que seleccionar la red y luego la subred y hacer clic en “Aceptar”.



Repetimos el proceso para las demás subredes y ya tendremos todas protegidas bajo el mismo conjunto de reglas.

5.- Actuación conjunta de grupos de seguridad de red, y solución de problemas asociados a reglas en un grupo de seguridad

Los grupos de seguridad pueden asociarse a subredes, como hemos hecho en este caso, pero también a otros recursos.

Un uso habitual es asociarlos a las interfaces de red de una máquina virtual.

Puede darse el caso de que una conexión entrante tenga que pasar por más de un grupo de seguridad para alcanzar su destino. En estos casos:

- Para que una conexión entrante alcance su objetivo, tiene que haber alguna regla que le permita el acceso en TODOS los grupos de seguridad por los que la conexión “pase”.
- Para que la conexión se rechace, basta que se rechace en UNO de los grupos de seguridad por los que debe pasar.

Hay más información de cómo funciona y procesa conexiones un grupo de seguridad de red en https://learn.microsoft.com/es-es/azure/virtual-network/network-security-group-how-it-works

Para solventar problemas de conectividad provocados por reglas en los grupos, podemos usar una herramienta que permite analizar qué reglas aplican a cierta interfaz de red de una máquina virtual. Para acceder a esta herramienta, en el menú del grupo de seguridad, tenemos una opción “Reglas de seguridad vigentes”, que permite seleccionar la interfaz de red que queremos analizar, y nos mostrará las reglas que aplican.