Create NSG and Rules

Objective

- Criar NSG, Rules para SSH (porta 22), e SSH para IP restrito.

Comments

Today I practiced NSG (Network Security Groups), an important topic for the AZ-104 exam, which I'm currently studying for. I used Azure CLI to create a Resource Group, VM, VNet, Subnet, NSG, and an Inbound Rule.
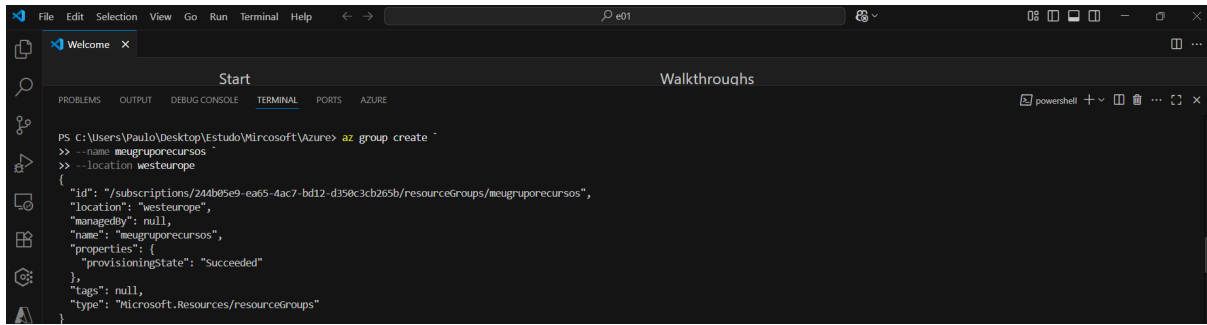
At first, I created an SSH rule that allowed inbound traffic to my subnet.

Then, I deleted that rule and created a new SSH rule restricted to my laptop's public IP — and everything worked as expected.
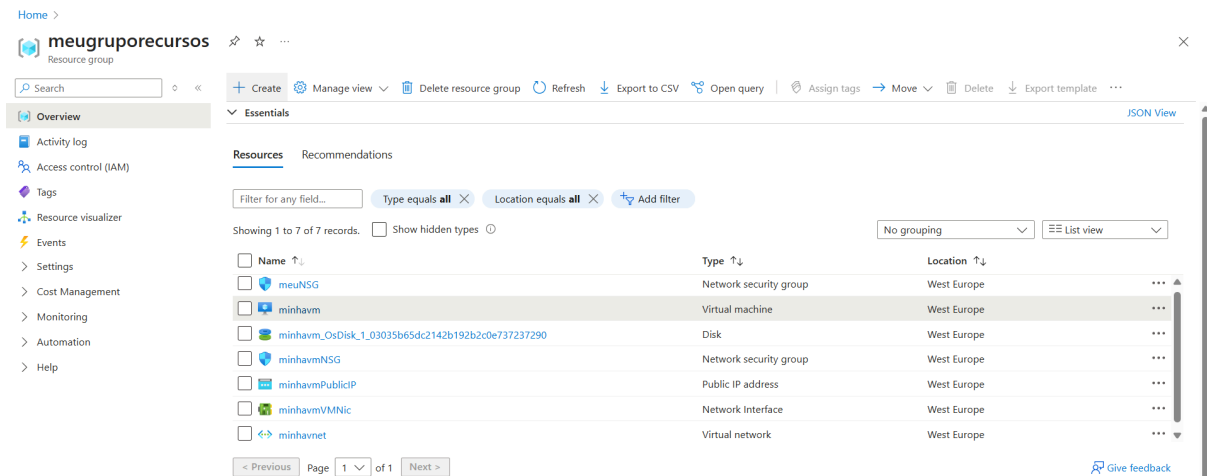
It was a smooth process, and I'm getting more and more comfortable with Azure cloud concepts.

The CLI commands are becoming more intuitive as I keep practicing — and I'm focusing a lot on mastering the CLI, as it will be a solid foundation for my future career as a Cloud Engineer.

1. Create RG "meugruporecursos"

2. Create Vnet "minhavnet" and Subnet "minhasubnet"

4.Create NSG "meuNSG"


```
}
PS C:\Users\Paulo\Desktop\Estudo\Mircosoft\Azure> az network nsg create `
>> --resource-group meugruporecursos `
>> --name meuNSG `
{
  "NewNSG": {
    "defaultSecurityRules": [
      {
        "access": "Allow",
        "description": "Allow inbound traffic from all VMs in VNET",
        "destinationAddressPrefix": "VirtualNetwork",
        "destinationAddressPrefixes": [],
        "destinationPortRange": "*",
        "destinationPortRanges": [],
        "direction": "Inbound",
        "etag": "W/\"ec282e1e-8173-457e-8b7e-ea2bb026368d\"",
        "id": "/subscriptions/244b05e9-ea65-4ac7-bd12-d350c3cb265b/resourceGroups/meugruporecursos/providers/Microsoft.Network/networkSecurityGroups/meuNSG/defaultSecurityRules/AllowVnetInBound",
        "name": "AllowVnetInBound",
        "priority": 65000,
        "protocol": "*",
        "provisioningState": "Succeeded",
        "resourceGroup": "meugruporecursos",
        "sourceAddressPrefix": "VirtualNetwork",
        "sourceAddressPrefixes": [],
        "sourcePortRange": "*",
        "sourcePortRanges": [],
        "type": "Microsoft.Network/networkSecurityGroups/defaultSecurityRules"
      },
      {
        "access": "Allow",
        "description": "Allow inbound traffic from azure load balancer",
        "destinationAddressPrefix": "*",
        "destinationAddressPrefixes": [],
        "destinationPortRange": "*",
        "destinationPortRanges": [],
        "direction": "Inbound",
        "etag": "W/\"ec282e1e-8173-457e-8b7e-ea2bb026368d\"",
```

Home > meugruporecursos >

meuNSG
Network security group

→ Move ∨   🗑 Delete   ↻ Refresh   🗐 Give feedback

∧ Essentials   JSON View

Resource group (move)   : meugruporecursos   Custom security rules : 1 inbound, 0 outbound
Location   : West Europe   Associated with   : 0 subnets, 0 network interfaces
Subscription (move)   : Azure subscription 1
Subscription ID   : 244b05e9-ea65-4ac7-bd12-d350c3cb265b
Tags (edit)   : Add tags

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
300	permitirSSHrestrito	Any	Any	62.48.234.226	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerI···	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow

4. Create Rule "permitirSSH"

```
PS C:\Users\Paulo\Desktop\Estudo\Mircosoft\Azure> az network nsg rule create `
>> --resource-group meugruporecursos `
>> --nsg-name meuNSG `
>> --name permitirSSH `
>> --priority 200 `
>> --access Allow `
>> --direction Inbound `
>> --source-address-prefixes "*" `
>> --source-port-ranges "*" `
>> --destination-address-prefixes "*" `
>> --destination-port-ranges "*"
```

5.Create VM "minhavm"

```
PS C:\Users\Paulo\Desktop\Estudo\Mircosoft\Azure> az vm create `
>> --resource-group meugruporecursos `
>> --name minhavm `
>> --vnet-name minhavnet `
>> --subnet minhasubnet `
>> --image Ubuntu2204 `
>> --size Standard_B1s `
>> --admin-username azureuser `
>> --admin-password Nikola99530301 `
>> --public-ip-sku Standard `
>>
The default value of '--size' will be changed to 'Standard_D2s_v5' from 'Standard_DS1_v2' in a future release.
Selecting "uksouth" may reduce your costs. The region you've selected may cost more for the same services. You can disable this message in the future with the command "az config set core.display_region
_identified=false". Learn more at https://go.microsoft.com/fwlink/?linkid=222571
{
    "fqdns": "",
    "id": "/subscriptions/244b05e9-ea65-4ac7-bd12-d350c3cb265b/resourceGroups/meugruporecursos/providers/Microsoft.Compute/virtualMachines/minhavm",
    "location": "westeurope",
    "macAddress": "7C-ED-8D-15-B3-BE",
    "powerState": "VM running",
    "privateIpAddress": "10.0.0.4",
    "publicIpAddress": "4.210.160.83",
    "resourceGroup": "meugruporecursos",
    "zones": ""
}
```

6. Access SSH VM

7. Delete Rule "permitirSSH"
I deleted the rule to create another restricted SSH rule.

8. Create Rule "permitirSSHrestrito"


```
Examples from AI knowledge base:
https://aka.ms/cli_ref
Read more about the command in reference docs
PS C:\Users\Paulo\Desktop\Estudo\Mircosoft\Azure> az network nsg rule create `
>> --resource-group meugruporecursos `
>> --nsg-name meuNSG `
>> --name permitirSSHrestrito `
>> --priority 300 `
>> --access Allow `
>> --direction Inbound `
>> --source-address-prefixes 62.48.234.226 `
>> --source-port-ranges "*" `
>> --destination-address-prefixes "*" `
>> --destination-port-ranges "*"
{
    "access": "Allow",
    "destinationAddressPrefix": "*",
    "destinationAddressPrefixes": [],
    "destinationPortRange": "*",
    "destinationPortRanges": [],
    "direction": "Inbound",
    "etag": "W/\"adea2198-6800-4eb3-ab45-1f5620489adf\"",
    "id": "/subscriptions/244b05e9-ea65-4ac7-bd12-d350c3cb265b/resourceGroups/meugruporecursos/providers/Microsoft.Network/networkSecurityGroups/meuNSG/securityRules/permitirSSHrestrito",
    "name": "permitirSSHrestrito",
    "priority": 300,
    "protocol": "*",
    "provisioningState": "Succeeded",
    "resourceGroup": "meugruporecursos",
    "sourceAddressPrefix": "62.48.234.226",
    "sourceAddressPrefixes": [],
    "sourcePortRange": "*",
    "sourcePortRanges": [],
    "type": "Microsoft.Network/networkSecurityGroups/securityRules"
}
```
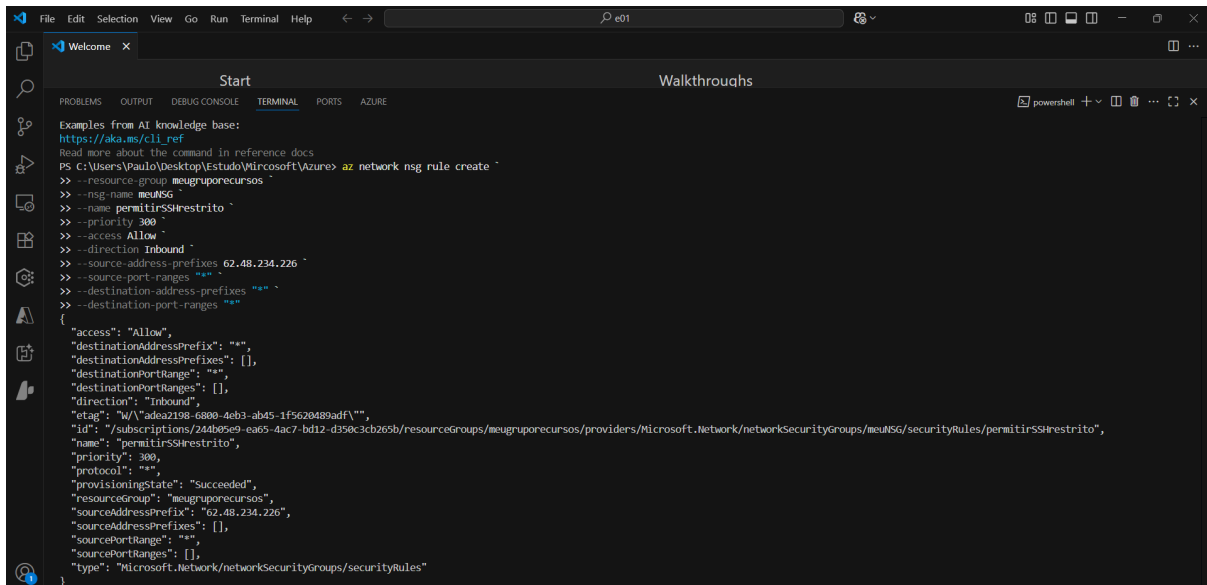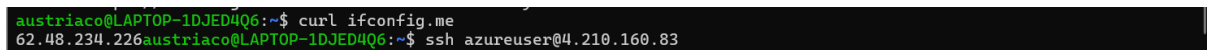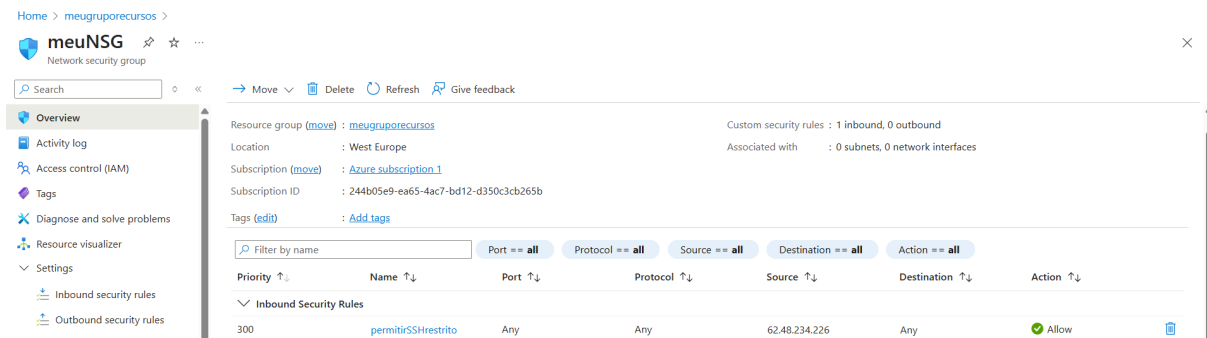
9.Comand Public Ip my Laptop


```
austriaco@LAPTOP-1DJED4Q6:~$ curl ifconfig.me
62.48.234.226austriaco@LAPTOP-1DJED4Q6:~$ ssh azureuser@4.210.160.83
```

10.Connect via SSH my laptop

Thank you if you've seen this far, it may seem a little, but for those who are studying for the AZ-104 exam, this is the way, because practicing every day is what will make me become an excellent Cloud Engineer, thank you all, let's go for more!!!