Experiment - Configuring a firewall for an Azure storage account using PowerShell

In this experiment, we'll enable firewall rules for an Azure storage account using PowerShell.

Getting ready

Before you start, perform the following steps:

1. Make sure you have an existing Azure storage account. If not, create one by following the *Provisioning an Azure storage account using PowerShell* experiment.
2. Log in to your Azure subscription in PowerShell. To log in, run the **`Connect-AzAccount`** command in a new PowerShell window and follow the instructions.

How to do it...

The steps for this experiment are as follows:

1. Execute the following command to deny access from all networks:

```
Update-AzStorageAccountNetworkRuleSet -ResourceGroupName
AzureDataEngineering -Name adestoragepowershell -DefaultAction Deny
```

You should get a similar output to that shown in the following screenshot:

```
PS C:\windows\temp\Logfiles> Update-AzStorageAccountNetworkRuleSet -ResourceGroupName AzureDataEngine
ering -Name adestoragepowershell -DefaultAction Deny

Bypass              : AzureServices
DefaultAction       : Deny
IpRules             :
VirtualNetworkRules :
ResourceAccessRules :
```

2. reExecute the following commands to add a firewall rule for the client IP address:

```
#get client IP Address
$mypublicIP = (Invoke-WebRequest -uri "http://ifconfig.
me/ip").Content
#Add client IP address firewall rule
Add-AzStorageAccountNetworkRule -ResourceGroupName
AzureDataEngineering -AccountName adestoragepowershell -
IPAddressOrRange
$mypublicIP
```

You should get a similar output to that shown in the following screenshot:

```
PS C:\windows\temp\Logfiles>
PS C:\windows\temp\Logfiles> #get client IP Address
PS C:\windows\temp\Logfiles> $mypublicIP = (Invoke-WebRequest -uri "http://ifconfig.me/ip").Content
PS C:\windows\temp\Logfiles>
PS C:\windows\temp\Logfiles> #Add my client IP address firewall rule
PS C:\windows\temp\Logfiles> Add-AzStorageAccountNetworkRule -ResourceGroupName AzureDataEngineering
-AccountName adestoragepowershell -IPAddressOrRange $mypublicIP
```

3. Execute the following command to whitelist a custom IP to access the storage account:

```
#whitelist a single IP
Add-AzStorageAccountNetworkRule -ResourceGroupName
AzureDataEngineering -AccountName adestoragepowershell -
IPAddressOrRange
"20.24.29.30"
```

You should get a similar output to that shown in the following screenshot:

```
PS C:\windows\temp\Logfiles> #whitelist a single custom IP
PS C:\windows\temp\Logfiles> Add-AzStorageAccountNetworkRule -ResourceGroupName AzureDataEngineering
-AccountName adestoragepowershell -IPAddressOrRange "20.24.29.30"

Action IPAddressOrRange
------ ---------------
 Allow 69.180.128.204
 Allow 20.24.29.30
```

4. Execute the following command to whitelist a custom IP range to access the storage account:

```
#whitelist range of IPs
Add-AzStorageAccountNetworkRule -ResourceGroupName
AzureDataEngineering -AccountName adestoragepowershell -
IPAddressOrRange
"20.24.0.0/24"
```

You should get a similar output to that shown in the following screenshot:

```
PS C:\windows\temp\Logfiles> #whitelist range of custom IPs
PS C:\windows\temp\Logfiles> Add-AzStorageAccountNetworkRule -ResourceGroupName AzureDataEngineering
-AccountName adestoragepowershell -IPAddressOrRange "20.24.0.0/24"

Action IPAddressOrRange
------ ----------------
 Allow 69.180.128.204
 Allow 20.24.29.30
 Allow 20.24.0.0/24
```

5. Execute the following command to get all the existing firewall rules:

```
(Get-AzStorageAccountNetworkRuleSet -ResourceGroupName
AzureDataEngineering -Name adestoragepowershell).IpRules
```

You should get a similar output to that shown in the following screenshot:

```
PS C:\windows\temp\Logfiles> (Get-AzStorageAccountNetworkRuleSet -ResourceGroupName AzureDataEngineer
ing -Name adestoragepowershell).IpRules

Action IPAddressOrRange
------ ----------------
 Allow 69.180.128.204
 Allow 20.24.29.30
 Allow 20.24.0.0/24
```

6. Execute the following commands to remove the firewall rules:

```
#Remove the client IP from the firewall rule
Remove-AzStorageAccountNetworkRule -ResourceGroupName
AzureDataEngineering -Name adestoragepowershell -
IPAddressOrRange
$mypublicIP
```

```
#Remove the single IP from the firewall rule
Remove-AzStorageAccountNetworkRule -ResourceGroupName
AzureDataEngineering -Name adestoragepowershell -
IPAddressOrRange
"20.24.29.30"
#Remove the IP range from the firewall rule
Remove-AzStorageAccountNetworkRule -ResourceGroupName
AzureDataEngineering -Name adestoragepowershell -
IPAddressOrRange
"20.24.0.0/24"
```

You should get the following output:

```
PS C:\windows\temp\Logfiles> #Remove my public IP
PS C:\windows\temp\Logfiles> Remove-AzStorageAccountNetworkRule -ResourceGroupName AzureDataEngineeri
ng -Name adestoragepowershell -IPAddressOrRange $mypublicIP

Action IPAddressOrRange
------ ---------------
 Allow 20.24.29.30
 Allow 20.24.0.0/24

PS C:\windows\temp\Logfiles> #Remove the single IP from the firewall rule
PS C:\windows\temp\Logfiles> Remove-AzStorageAccountNetworkRule -ResourceGroupName AzureDataEngineeri
ng -Name adestoragepowershell -IPAddressOrRange "20.24.29.30"

Action IPAddressOrRange
------ ---------------
 Allow 20.24.0.0/24

PS C:\windows\temp\Logfiles> #Remove the IP range from the firewall rule
PS C:\windows\temp\Logfiles> Remove-AzStorageAccountNetworkRule -ResourceGroupName AzureDataEngineeri
ng -Name adestoragepowershell -IPAddressOrRange "20.24.0.0/24"
PS C:\windows\temp\Logfiles>
```

7. Execute the following command to allow access to all networks:

```
Update-AzStorageAccountNetworkRuleSet -ResourceGroupName
AzureDataEngineering -Name adestoragepowershell -DefaultAction Allow
```

You should get the following output:

```
PS C:\windows\temp\Logfiles> Update-AzStorageAccountNetworkRuleSet -ResourceGroupName AzureDataEngine
ering -Name adestoragepowershell -DefaultAction Allow

Bypass              : AzureServices
DefaultAction       : Allow
IpRules             :
VirtualNetworkRules :
ResourceAccessRules :
```

How it works...

To whitelist an IP or range of IPs, we first need to modify the storage account to use selected networks instead of all networks. This is done by means of the **`Update-AzStorageAccountNetworkRuleSet`** command.

We can then whitelist an IP or range of IPs using the **`Add-AzStorageAccountNetworkRule`** command. We provide the resource group name, storage account name, and the IP or range of IPs to whitelist.

We can get the list of existing rules using the **`Get-AzStorageAccountNet workRuleSet`** command by providing the resource group and the storage account name as the parameter.

We can remove the IPs from the firewall using the **`Remove-AzStorageAccount NetworkRule`** command by providing the resource group name, storage account name, and the IP or the IP range to remove.