How to Configure the Azure Connectivity Agent

https://campus.barracuda.com/doc/41112428/

The Azure Connectivity Agent allows you to use the Barracuda NG Firewall in the Azure Cloud as the default gateway for your Windows Server Azure VMs. The Connectivity Agent must be installed on all VMs in the VNET that initiate outgoing connections.

In this article:

Before you Begin

- Deploy your Barracuda NG Firewall in the Azure Cloud.
- Deploy your Windows Server VMs in the same subnet(s) as the Barracuda NG Firewall.
- Create a PFX client certificate for each Windows Server VM. For more information, see How to Create Certificates with XCA.
- Copy the Azure Connectivity Agent and the client certificates to the Windows Server VM.
- Create a Client-to-Site VPN on the Barracuda NG Firewall. Verify that it can be reached from the subnets where the Windows Server VMs are located. For more information, see Client-to-Site VPN.
- (optional) Lock down the private subnets with Azure Network Security Groups to make sure outgoing traffic is sent through only the Barracuda NG Firewall.

Installing the Azure Connectivity Agent

The PowerShell script provided to configures and silently installs the Azure Connectivity Agent by supplying the PDF container file and the VPN profile parameters.

1. Open a **Windows PowerShell** with Administrator privileges.
2. Change to the directory of the Azure Connectivity Agent.
3. Start the installation of the Azure Connectivity Agent.
   ```
   C:\Azure>.\AzureConnectivityAgent.ps1 johndoe.pfx -PfxFilePassword mysecret -ProfileDescription ConnectivityAgent -ServerAddress vpn.acme.org -TunnelMode TCP -EncryptionAlgorithm AES256 -HashAlgorithm SHA1
   ```
4. The installation of the **Barracuda Network Access Client 3.5 x64** completes without the need for further user interaction.

Display All Azure Connectivity Agent Options

For a list of all available options, enter:

```
C:\Azure>.\Get-Help AzureConnectivityAgent.ps1 -full
```