Azure Point-to-site VPN Demo Walkthrough

This guide provides a walkthrough for Azure Point-to-site VPN.

Contents

[Pre-Requisites 1](#_Toc432886886)

[Setup 1](#_Toc432886887)

[Demo Steps 8](#_Toc432886888)

[Clean Up 11](#_Toc432886889)

## Pre-Requisites

This section lists the pre-requisites required for this demonstration.

* An Azure subscription
* MakeCert.exe

## Setup

Estimated time: 15 minutes

The following procedure will walk you through the setup steps to create a secure point-to-site connection to a virtual network. The order in which you configure each of these is important, so don't skip steps or jump ahead.

1. Create a virtual network and a VPN gateway
2. Create your certificates

**Create a virtual network and a VPN gateway:**

|  |  |
| --- | --- |
| 1. Log in to the Azure portal |  |
| 1. In the lower left corner of the screen, click New. In the navigation pane, click Network Services, and then click Virtual Network. Click Custom Create to begin the configuration wizard. |  |
| 1. On the Virtual Network Details page, enter the following information, and then click the next arrow on the lower right.    1. Name: Name your virtual network. For example "DemoVNetEast". This will be the name that you'll refer to when you deploy VMs and PaaS instances to this VNet.    2. Location: The location is directly related to the physical location (region) where you want your resources (VMs) to reside. Example “East US” |  |
| 1. On the DNS Servers and VPN Connectivity page, enter the following information, and then click the next arrow on the lower right.    1. **DNS Servers:** Enter the DNS server name and IP address, or select a previously registered DNS server from the shortcut menu. This setting does not create a DNS server, it allows you to specify the DNS servers that you want to use for name resolution for this virtual network. **If you want to use the Azure default name resolution service, leave this section blank**    2. **Configure Point-To-Site VPN:** Select the checkbox. |  |
| 1. On the Point-To-Site Connectivity page, specify the IP address range from which your VPN clients will receive an IP address when connected. There are a few rules regarding the address ranges that you are able to specify. It's very important to verify that the range that you specify doesn't overlap with any of the ranges located on your on-premises network. **Keep the default values.** |  |
| 1. On the Virtual Network Address Spaces page, specify the address range that you want to use for your virtual network. These are the dynamic IP addresses (DIPS) that will be assigned to the VMs and other role instances that you deploy to this virtual network. It's especially important to select a range that does not overlap with any of the ranges that are used for your on-premises network. You'll need to coordinate with your network administrator, who may need to carve out a range of IP addresses from your on-premises network address space for you to use for your virtual network. |  |
| 1. Enter the following information, and then click the checkmark to begin creating your virtual network. |  |
| 1. When your virtual network has been created, you will see Created listed under Status on the networks page in the Azure portal. |  |
| 1. Once your virtual network has been created, you can create your dynamic routing gateway. |  |
| 1. In the Azure portal, on the Networks page, click the virtual network that you just created, and navigate to the Dashboard page. |  |
| 1. Click Create Gateway, located at the bottom of the Dashboard page. A message will appear asking Do you want to create a gateway for virtual network "DemoVNetEast". Click Yes to begin creating the gateway. It can take around 15 minutes for the gateway to create. |  |
|  |  |

**Create your certificates:** Certificates are used to authenticate VPN clients for point-to-site VPNs. This procedure has multiple steps. Complete each step, in order as mentioned below.

|  |  |
| --- | --- |
| 1. To generate a self-signed root certificate, access “makecert.exe” from the command prompt as Administrator. |  |
| 1. Execute the below command   makecert -sky exchange -r -n "CN=RootDemoVNetCertificate" -pe -a sha1 -len 2048 -ss My "RootDemoVNet.cer". |  |
| 1. The command in the following example will create and install a root certificate in the Personal certificate store on your computer and also create a corresponding .cer file that you'll later upload to the Azure portal. |  |
| 1. Once ceritificate created, you can see it in certificate manager🡪 current users🡪perosnal🡪Certificates. Because you have created a root certificate from which client certificates will be generated, you may want to export this certificate along with its private key and save it to a safe location where it may be recovered. |  |
| 1. Upload the root certificate file to the Azure portal. In the Azure portal, on the Certificates page for your virtual network, click Upload a root certificate. On the Upload Certificate page, browse for the .cer root certificate, and then click the checkmark. |  |
| 1. Generate a client certificate. On the same computer that you used to create the self-signed root certificate. To generate a client certificate, access “makecert.exe” from the command prompt as Administrator. |  |
| 1. Change the directory to the location where you want to save the client certificate file. “RootDemoVNetCertificate” refers to the self-signed root certificate that you generated. |  |
| 1. Type the following command:   makecert.exe -n "CN=ClientCertificateName" -pe -sky exchange -m 96 -ss My -in "RootDemoVNetCertificate" -is my -a sha1 |  |
| 1. All certificates are stored in your Personal certificate store on your computer. Check certificate manager to verify. |  |
| 1. Export and install the client certificate. |  |
| 1. A client certificate must be installed on each computer that you want to connect to the virtual network. This means you will probably create multiple client certificates and then need to export them. To export the client certificates, use certmgr.msc. Right-click the client certificate that you want to export, click all tasks, and then click export. |  |
| 1. Export the client certificate with the private key. This will be a .pfx file. Make sure to record or remember the password (key) that you set for this certificate. |  |
| 1. Copy the .pfx file to the client computer. On the client computer, double-click the .pfx file in order to install it. Enter the password when requested. Do not modify the installation location. |  |
|  |  |

## Demo Steps

Estimated time: 10 minutes

The following procedure will walk you through the steps to configure and connect a secure point-to-site connection to a virtual network. The order in which you configure each of these is important, so don't skip steps or jump ahead.

**Note: Make sure step 1 and 2 are successfully completed before continuing with step 3.**

1. Configure your VPN client
2. Connect and Verify the VPN connection

**Configure your VPN client:** To connect to the virtual network, you'll also need to configure your VPN client. The client requires both a client certificate and the proper VPN client configuration in order to connect.

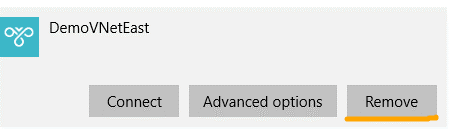
|  |  |
| --- | --- |
| 1. In the Azure portal, on the Dashboard page for your virtual network, navigate to the quick glance menu in the right corner and click the VPN package that pertains to the client that you want to connect to your virtual network. 2. For 32-bit clients, select Download the 32-bit Client VPN Package. 3. For 64-bit clients, select Download the 64-bit Client VPN Package. |  |
| 1. It will take a few minutes to create your client package. Once the package has been completed, you will be able to download the file. The .exe file that you download can be safely stored on your local computer. |  |
| 1. After you generate and download the VPN client package from the Azure portal, you can install the client package on the client computer from which you want to connect to your virtual network. |  |
| 1. Validate client package is installed on your client computer. |  |

**Connect and Verify the VPN connection:**

|  |  |
| --- | --- |
| 1. On the client computer, navigate to VPN connections and locate the VPN connection that you just created. It will be named the same name as your virtual network. Click Connect. |  |
| 1. A pop up message will appear which is used to create a self-signed cert for the Gateway endpoint. Click Continue to use elevated privileges. On the Connection status page, click Connect in order to start the connection. |  |
| 1. If you see a Select Certificate screen, verify that the client certificate showing is the one that you want to use to connect. If it is not, use the drop-down arrow to select the correct certificate, and then click OK. |  |
| 1. You are now connected to your virtual network and have full access to any service and virtual machine hosted in your virtual network. |  |
| 1. To verify that your VPN connection is active, open an elevated command prompt, and run ipconfig/all. |  |
| 1. View the results. Notice that the IP address you received is one of the addresses within the point-to-site connectivity address range that you specified when you created your VNet. |  |

## Clean Up

1. Remove the virtual network client installation from the client machine by clicking on “Remove button” on client machine.



1. Delete the Virtual networks from the azure portal.
2. Remove server and client certificate from the client machine.