

**Project :**

**Configuration of Point to site VPN**

**SUBMITTED BY :**

**1.Vinayak Sain 2.Ankit Lalawat**

B. Tech (CS with Cloud tech and info security) BCA (CT & ITIMS)

4th Yr(7th SEM) 3rd Yr(5th SEM)

2018BCCX1073 2019BCTX1001

**3.Tasneem Fatima 4.Yogesh Mandora**

MCA MCA

2nd Yr(3rd SEM) 2nd Yr(3rd SEM)

1MCA/20/007 1MCA/20/011

**Under the Guidance of**

Miss Reema Rani

POORNIMA UNIVERSITY

**SCHOOL OF COMPUTER SCIENCE & ENGINEERING**

[2020-2021]

**ACKNOWLEDGEMENT**

I would like to express my deep sense of respect and gratitude towards my advisor and guide Ma’amReema Rani who has been the guiding force behind the work.

I am greatly indebted to her for constant encouragement and invaluable advice in every aspect of my academic life. Her presence and optimism have provided an invaluable influence on my career and outlook for the future. I consider it my good fortune to get an opportunity to work with such a wonderful person.

I express my gratitude to Celebal technologies, Jaipur for mentoring me and also helping me learn. He has been a great source of inspiration to me and I thank him from the bottom of my heart.

**(TEAM)**

**TABLE OF CONTENTS**

**Chapter 1**

Objectives

Introduction

**Chapter 2**

Terminologies

**Chapter 3**

Outcome

Conclusion

**Chapter 4**

References

**Chapter 1**

**OBJECTIVE**

It helps you securely connect individual clients running Windows, Linux, or macOS to an **Azure** VNet. **Point-to-Site VPN** connections are useful when you want to connect to your VNet from a remote location, such when you are telecommuting from home or a conference.

**INTRODUCTION**

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet

Basically, a machine on-premises is connected to a virtual network using point-to-site connectivity. However, we can connect up to 128 on-premise machines to a virtual network in Azure. The access to the virtual network in the cloud is granted through a certificate. The certificate has to be installed on each local machine that needs to be connected to the virtual network.

**Chapter 2**

**TERMINOLOGIES USED**

▪ VNet

▪ VPN GATEWAY

▪ MICROSOFT CERTIFICATES

▪ VPN CLIENT

▪ GENERATE ROOT CERTIFICATE

▪ GENERATE CLIENT CERTIFICATE

**VNet :-** When using a virtual network as part of a cross-premises architecture, be sure to coordinate with your on-premises network administrator to carve out an IP address range that you can use specifically for this virtual network. If a duplicate address range exists on both sides of the VPN connection, traffic will route in an unexpected way. Additionally, if you want to connect this virtual network to another virtual network, the address space cannot overlap with the other virtual network. Plan your network configuration accordingly.

**VPN GATEWAY :-** The virtual network gateway uses a specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We recommend that you create a gateway subnet that uses a /27 or /28.

**MICROSOFT CERTIFICATE :-** Certificates are used by Azure to authenticate clients connecting to a VNet over a Point-to-Site VPN connection. Once you obtain a root certificate, you [upload](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal#uploadfile) the public key information to Azure. The root certificate is then considered 'trusted' by Azure for connection over P2S to the virtual network. You also generate client certificates from the trusted root certificate, and then install them on each client computer. The client certificate is used to authenticate the client when it initiates a connection to the VNet.

**VPN CLIENT:-** To connect to the virtual network gateway using P2S, each computer uses the VPN client that is natively installed as a part of the operating system. For example, when you go to VPN settings on your Windows computer, you can add VPN connections without installing a separate VPN client. You configure each VPN client by using a client configuration package. The client configuration package contains settings that are specific to the VPN gateway that you created.

**GENERATE ROOT CERTIFICATE :-** Obtain the .cer file for the root certificate. You can use either a root certificate that was generated with an enterprise solution (recommended), or generate a self-signed certificate. After you create the root certificate, export the public certificate data (not the private key) as a Base64 encoded X.509 .cer file. You upload this file later to Azure.

**GENERATE CLIENT CERTIFICATE :-** Each client computer that you connect to a VNet with a Point-to-Site connection must have a client certificate installed. You generate it from the root certificate and install it on each client computer. If you don't install a valid client certificate, authentication will fail when the client tries to connect to the VNet.

**Chapter 3**

**OUTCOME**

P2S VPN will create a secure connection to the **Azure** Virtual Network from an individual client computer. The main point is that if we log-off or restart the workstation, it loses connection, and we have to reconnect every time.

**CONCLUSION**

P2S VPN lets us create a secure connection to the virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.

**Chapter 4**

**REFERENCES**

<https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-creating-an-azure-point-to-site-vpn/ba-p/326264>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>

[www.youtube.com](http://www.youtube.com)