**Cross Premises Connectivity using Site to Site VPN**

*Aproject report submitted in partial fulfillment of the Academic requirements*

*for the award of the Degree of*

**BACHELOR OF ENGINEERING**

**IN**

**INFORMATION TECHNOLOGY**

**By**

**K Harshitha (2451-19-737-105)**

**M Srinidhi (2451-19-737-112)**

**S Revanth Aryan (2451-19-737-118)**

***Under the guidance of***

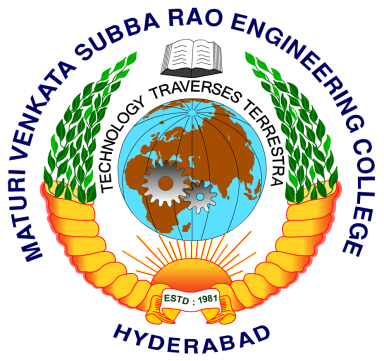
**Guide Name (Mr. D Muninder)**

**Designation (Assistant Professor), Dept. of I.T**

**Maturi Venkata Subba Rao (MVSR) Engineering College**

**Nadergul, Hyderabad.**

**(July, 2022)**

****

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**MATURI VENKATA SUBBA RAO (MVSR) ENGINEERING COLLEGE**

**(Affiliated to Osmania University, Hyderabad. Recognized by AICTE)**

**Nadergul, Saroornagar Mandal, Hyderabad-501510**

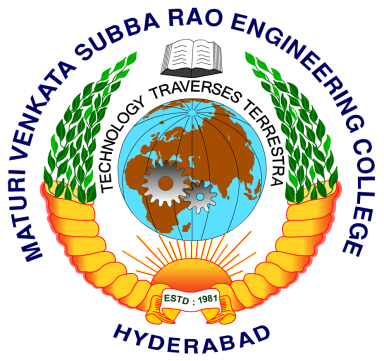
**2021-2022**

**MATURI VENKATA SUBBA RAO (MVSR)**

**ENGINEERING COLLEGE**

**(Affiliated to Osmania University, Hyderabad. Recognized by AICTE)**

**Nadergul, Saroornagar Mandal, Hyderabad-501510**

****

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**CERTIFICATE**

Certified that this a Bonafide Major Project work carried out by

Ms.  **K Harshitha** Bearing H.T. No.  **2451-19-737-105** in the course Mini Project – I (PW653IT) prescribed for B.E(3/4) Sem: **VI** by **Osmania University**, in the Department during the academic year 2021 - 2022.

Faculty in-Charge Guide Signature

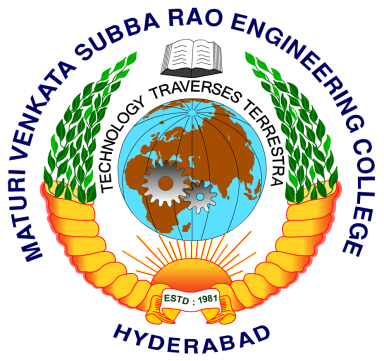
Head of the Department

**MATURI VENKATA SUBBA RAO (MVSR)**

**ENGINEERING COLLEGE**

**(Affiliated to Osmania University, Hyderabad. Recognized by AICTE)**

**Nadergul, Saroornagar Mandal, Hyderabad-501510**

****

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**CERTIFICATE**

Certified that this a Bonafide Major Project work carried out by

Ms.**M Srinidhi\_** Bearing H.T. No. **2451-19-737-112** in the course Mini

Project – I (PW653IT) prescribed for B.E (3/4) Sem: **VI** by **Osmania University**, in the Department during the academic year 2021 - 2022.

Faculty in-Charge Guide Signature

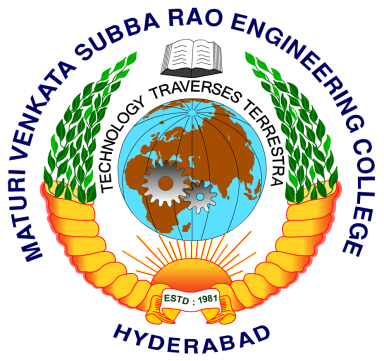
Head of the Department

**MATURI VENKATA SUBBA RAO (MVSR)**

**ENGINEERING COLLEGE**

**(Affiliated to Osmania University, Hyderabad. Recognized by AICTE)**

**Nadergul, Saroornagar Mandal, Hyderabad-501510**

****

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**CERTIFICATE**

Certified that this a Bonafide Major Project work carried out by

Mr. **\_S Revanth Aryan\_** Bearing H.T. No. **2451-19-737-118** in the course Mini Project - I(PW653IT) prescribed for B.E(3/4) Sem: **VI** by **Osmania University**, in the Department during the academic year 2022 - 2022.

Faculty in-Charge Guide Signature

Head of the Department

**ACKNOWLEDGEMENT**

We with extreme jubilance and deepest gratitude, would like to thank Mr. D Muninder, Assistant Professor, Department of Information Technology, Maturi Venkata Subba Rao (MVSR) Engineering College, for her constant encouragement and facilities provided to us to complete our project in time.

With immense pleasure, we record our deep sense of gratitude to our beloved Head of the department **Dr. K. Venu Gopal Rao** Department of Information Technology, MVSR Engineering College, for permitting us to carry out this project.

We would like toextend our gratitude to**Mr. D. Muninder, Assistant Professor**,**Mrs. K. Ramya Madhavi, Assistant Professor, Mrs. J. Sowjanya, Assistant Professor,** and **S. Kalyana Chakravarthy, Lab Assistant**, Department of Information Technology, Maturi Venkata Subba Rao Engineering College, for his valuable suggestions and timely help during the course of the project.

We express, from the bottom of my heart, my deepest gratitude to my parents and family for the support, dedication, comprehension, and love.

Finally, we express our heartfelt thanks to each one who directly and indirectly helped us in successful completion of this project work.

**K Harshitha (2451-19-737-105)**

**M Srinidhi (2451-19-737-112)**

**S Revanth Aryan (2451-19-737-118)**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| **1** | **ABSTRACT** | 7 |
| **2.** | **INTRODUCTION** | 8-11 |
| **3.** | **LITERATURE REVIEW** | 12 |
| **4.** | **SYSTEM ANALYSIS** | 13-14 |
|  | 4.1 Objectives | 13 |
|  | 4.2 Problem Specification | 13 |
|  | 4.3 Proposed System | 13 |
|  | 4.4 Applications | 14 |
|  | 4.5 Modules and their functionalities | 14 |
| **5.** | **REQUIRMENTS SPECIFICATION** | 15-24 |
|  | 5.1 Software Requirements | 24 |
|  | 5.2 Hardware Requirements | 24 |
| **6.** | **DESIGN** | 25-30 |
|  | 6.1 System Architecture | 26 |
|  | 6.2 Flowchart | 27 |
|  | 6.3 Algorithm | 28 |
|  | 6.4 UML Diagrams | 26 |
|  | 6.5 DFD | 26-27 |
| **7.** | **TESTING** | 31-32 |
| **8.** | **IMPLEMENTATION** | 33 |
| **9.** | **SCREENSHOTS** | 33-45 |
| **10.** | **CONCLUSIONS AND FUTURE ENHANCEMENTS** | 46-47 |
| **11.** | **REFERENCES** | 48 |
| **APPENDICES:** | A. List of abbreviations |  |
|  | B. List of Figures |  |
|  | C. List of Tables |  |

**ABSTRACT**

This project demonstrates us to use VNets (Virtual Network Gateway) to provision and manage virtual private networks (VPNs) in Azure and, optionally, link the VNets with other VNets in Azure, or with your on-premises IT CIDR block, and can be linked to other VNets and on-premises networks as long as the CIDR blocks do not overlap.There is an increasing demand nowadays to connect to internal networks from distant locations. Employees often need to connect to internal private networks over the Internet (which is by nature insecure) from home, hotels, airports or from other external networks. Security becomes a major consideration when staff or business partners have constant access to internal networks from insecure external locations. VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private “tunnel” to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet

**CHAPTER 1**

**INTRODUCTION**

* 1. **INTRODUCTION TO CLOUD COMPUTING:**

Cloud computing is the use of various services, such as software development platforms, servers, storage, and software, over the internet, often referred to as the "cloud."

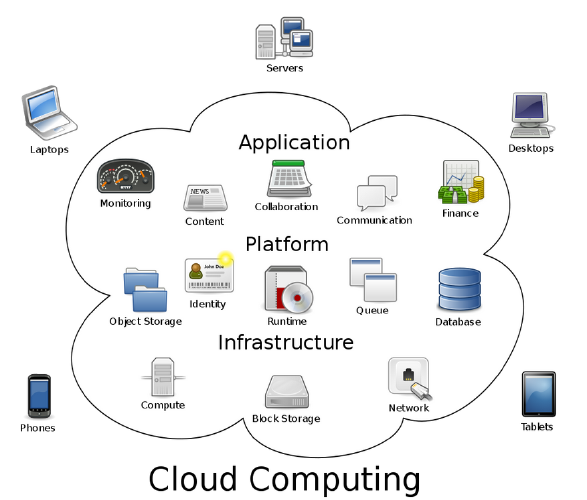


Fig: 1.1 The Architecture of Cloud Computing

**Types of Cloud Computing:**

Based on a service that the cloud is offering, we classify as:

* **Infrastructure as a Service (IaaS)** means you're buying access to raw computing hardware over the Net, such as servers or storage. Since you buy what you need and pay-as-you-go, this is often referred to as utility computing. Ordinary web hosting is a simple example of IaaS: you pay a monthly subscription or a per-megabyte/gigabyte fee to have a hosting company serve up files for your website from their servers.
* **Software as a Service (SaaS)** means you use a complete application running on someone else's system. Web-based email and Google Documents are perhaps the best-known examples. Zoho is another well-known SaaS provider offering a variety of office applications online.
* **Platform as a Service (PaaS)** means you develop applications using Web-based tools so they run on systems software and hardware provided by another company. So, for example, you might develop your own ecommerce website but have the whole thing, including the shopping cart, checkout, and payment mechanism running on a merchant's server. App Cloud (from salesforce.com) and the Google App Engine are examples of PaaS.

**AZURE CLOUD COMPUTING**

Cloud Computing is a kind of outsourcing computer programs. using cloud computing, users ae able to access software applications from wherever they are. Cloud Computing

Is a better way that come with storing your own data, because you’re not managing hardware and software.

Azure Cloud Computing is a Microsoft’s public Cloud Computing platform. Users can pick from these services to develop and scale new applications or run existing applications.Azure enables the rapid development of solutions and provides the resources to accomplish tasks that may not be feasible in an on-premises environment. Azure's compute, storage, network, and application services allow you to focus on building great solutions without the need to worry about how the physical infrastructure is assembled.

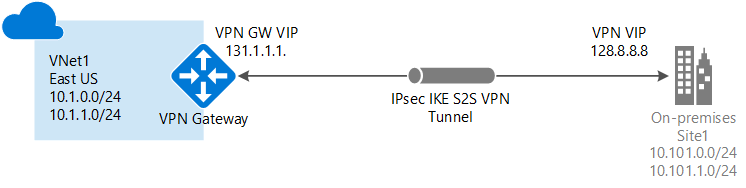
**1.3 INTRODUCTION TO AZURE SITE TO SITE VPN**

Azure Site-to-Site VPN gateway connection is used to connect our on-premises network to an Azure virtual network over an IPsec VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it. A Virtual Private Network (VPN) lets you protect traffic that travels over lines that your organization may not own or control. VPNs can encrypt traffic sent over these lines and authenticate peers before any traffic is sent.most organizations already have a network on their premises and would want to connect it to Windows Azure rather than putting everything on cloud. It is also called hybrid network connectivity. It is connecting virtual net in Azure to on-premises network. Setting up a site-to-site connectivity network is quite easy for someone who knows the basics of networking like IPs, subnetting and default gateways.

The things that are required before configuring the network in this case are −

* A VPN device that can be configured.
* Externally facing IP address for that VPN device.

VPN services helps to improve network flexibility and reduce operating costs, many large enterprises are evaluating the use of VPN devices, as well as the Azure VPN services that have been announced over the past year Even if they have already adopted remote access VPNs, enterprises should come up to speed on the various site-to-site VPN options to determine Which best matches their network requirements.



**Figure 1.2:VIRTUAL GATEWAY CONNECTION TO ON PREMISES**

There are two most common types of VPNs:

1. VPDN (Virtual Private Dial-up Network)

2. Site-to-Site VPN

1**.VPDN (Virtual Private Dial-up Network):**

A **VPDN**is a user-to-LAN connection, where faraway users connect with the enterprise LAN. For this, the employer needs to provide the software to the users so that they can easily reach the **Network Access Server** (a service provider setup) from their desktop, laptop, computers, mobiles, or tablets. This type of secure and encrypted connection between the remote users and company’s network is provided by the third-party service provider.

**2. Site-to-Site VPN:**

Site-to-Site means multiple fixed sites are connected over a public network (like the Internet). A site-to-site VPN requires large-scale encryption and dedicated equipment.Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. A **site-to-site VPN** allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

* 1. **FUNCTIONALITIES**

Azure Site to Site VPNprovidesfollowingfunctionalities:

* Site to Site VPNprovides remote users secure access to their organization’s network so that they can send and receive data securely.
* It provides benefits of security, enhanced functionalities, and management policies of the private network.
* The confidentiality is maintained as the transmitted information cannot be read by anyone else.
* Authentication creates better security and manageability for the VPN
* Site-to-Site VPN Gateways can communicate with each other in a bi-directional relationship. This kind of VPN can be used to mesh the company’s branches into one corporate network.
* The S2S VPN is the fastest way to establish a trusted private connection

**CHAPTER 2**

**2. LITERATURE SURVEY**

**1**.Hybrid cloud environments are a highly scalable and cost-effective option for enterprises that need to expand their on-premises infrastructure. In every hybrid cloud solution, the issue of inter-cloud network connectivity must be overcome to allow communications, possibly secure, between resources scattered over multiple networks. [**Adel Nadjaran Toosi**]

**2.**VNet peering is a newfeature introduced August 2016 within Microsoft Azure that connects two VNets, providing low latency and high-speed connectivity between your Azure virtual networks. A VNet that is using the remote gateway of a peered VNet cannot have a local gateway configured as well [**Rick Donato**]

**3**. Cloud is an abstract, virtual environment where programs and data are stored.Also, in Cloud Computing users do not need to buy software or maintain expensive servers and devices for data storage, this leads to significant reduction of expenses, office space, and internal staff for IT support and increase of data security [1-2]. [**G. CARUTASU1, M. A. BOTEZATU1, C. BOTEZATU1]**

**4**.Virtual Networking is a vital type of service that provides a virtual network inside the cloud infrastructure of any vendor. Offered components include subnets, internet gateway, virtual private gateway, routers, peering connections, customer gateway, and hardware Virtual Private Network (VPN) connections. These services also provide VNet isolation, on-premises connections, and network traffic routing and filtering. [**Ioannis Papapanagiotou**]

**5.** Microsoft Azure concentrates on the features of the Azure platform that you are most likely to need to know rather than on every feature and service available on the platform. This book also provides several walkthroughs you can follow to learn how to create VMs and virtual networks, websites, and storage accounts, and so on. In many cases, real-world tips are included to help you get the most out of your Azure experience.**[Michael Collier Robin Shahan]**

**CHAPTER 3**

**3. SYSTEM ANALYSIS**

**3.1 Existing System:**

Organizations are stretched while managing a greater number of physical units, and when trying to set up and maintain them, the networking devices and applications in distributed sites, support time needed by organizations are coupled and will be increasing their cost gradually.

“Vnet peering is a mechanism that connects two virtual networks (VNets) in the same region through the Azure backbone network’’. When two virtual networks are peered, they appear as one for connectivity purpose. When two vnet’s are peered through remote gateway, we cannot configure local network gateway. Azure’s Virtual Network (VNet) is a logical isolation of Azure which enables you to securely connect Azure resources to each other. VNet lets you create your own private space in Azure

**Drawbacks:**

* Good security is not seen by vnet peering over internet.
* Every Virtual network peer must reside in same region
* Each VNet peer should not have an overlapping IP address space.
* Remote Gateway - A VNet that is using the remote gateway of a peered VNet cannot have a local gateway configured as well. In other words, a single virtual network can have only one gateway. It can either be a local gateway or a remote gateway (in the peered virtual network

**3.2 Proposed System:**

This project (site-to-site VPN) is about creating a secure connection between your on-premises site and our virtual network. This project provides a standard IPsec VPN in Azure.

With the help of this project (Clouding computing) we can ensure resources i.e., security wise as well as cost redundancies also. Usage of too many physical machines can be reduced. Time span delay is reduced regarding maintenance, updating, deploying and hardware related performance can be eliminated.

This project demonstrates about connecting with VPN devices.

Cloud organizations will be able to reduce expenditures and increase productivity. Cloud networking always has a simplified and updated ways to maintain, deploy and process virtual networks. Extra investment for physical and hardware infrastructure can be optimized by using cloud computing.

Once a site-to-site VPN is setup you have IP level connectivity between your premises and virtual networks in Azure. Site to site VPN enables us to build hybrid azure applications.

**ADVANTAGES**

* A Secure connection will be established.
* Usage of too many physical machines can be reduced.
* The S2S VPN is the fastest way to establish a trusted private connection
* Cloud organizations will be able to reduce expenditures and increase productivity.
* Extra investment for physical and hardware infrastructure can be optimized by using Azure cloud computing

**CHAPTER 4**

**4. SYSTEM REQUIREMENTS AND ANALYSIS**

**TECHNOLOGY USED:**

**Microsoft Azure:**

Microsoft Azure is Microsoft's cloud computing platform, providing a wide variety of services you can use without purchasing and provisioning your own hardware. Azure enables the rapid development of solutions and provides the resources to accomplish tasks that may not be feasible in an on-premises environment. Azure's compute, storage, network, and application services allow you to focus on building great solutions without the need to worry about how the physical infrastructure is assembled. Azure also provides several walkthroughs where we can learn how to create VMs and virtual networks, websites and storage accounts, Microsoft provides support for public, private, and hybrid clouds. Microsoft has deployed Azure datacenters in over 22 regions around the globe from Melbourne to Amsterdam and Sao Paulo to Singapore. Additionally, Microsoft has an arrangement with 21Vianet, making Azure available in two regions in China. Microsoft has also announced the deployment of Azure to another eight regions. Only the largest global enterprises are able to deploy datacenters in this manner, so using Azure makes it easy for enterprises of any size to deploy their services close to their customers, wherever they are in the world.

The Windows Azure public cloud platform is one of the three pillars of Microsoft’s Cloud OS vision that will transform the traditional datacenter environment, help businesses unlock insights in data stored anywhere, enable the development of a wide range of modern business applications, and empower IT to support users who work anywhere on any device while being able to manage these devices in a secure and consistent way. The other two pillars of the Cloud OS are, of course, Windows Server 2012 R2 and Microsoft System Center 2012 R2, and Microsoft Press Windows Azure can be anything you want it to be. As a cloud platform from Microsoft that provides a wide range of different services, Windows Azure lets you build, deploy, and manage solutions for almost any purpose you can imagine. In other words, Windows Azure is a world of unlimited possibilities. Whether you’re a large enterprise spanning several continents that needs to run server workloads, or a small business that wants a website that has a global presence, Windows Azure can provide a platform for building applications that can leverage the cloud to meet the needs of your business.

**Why use the cloud?**

Businesses generally consider moving their applications to the cloud for one of three reasons: speed, scale, and economics. Let’s briefly examine each of these advantages that cloud computing can provide.

**Speed:**

Developing applications that run in the cloud can be significantly faster than traditional application development for two reasons. First, you don’t have to deploy, configure, and maintain the underlying computing, storage, and networking infrastructures on which your applications will run. Instead, you can utilize infrastructure resources provided to you by your cloud hosting provider. A good analogy is lighting up your house. If you need to not only purchase and install light bulbs but also pull wires, install switches, buy and set up a generator, and purchase gasoline for your generator, it’s going to take a while until you get your house lit up. But if your light bulbs can leverage the wiring installed by the contractor who built your house and electricity provided by your city’s power station, you’ll be able to get your house lit up in next to no time. A second reason why cloud-based applications can be faster to deploy has to do with how applications are developed. In a typical enterprise environment, developers create and test their applications in a test environment that only partially simulates the final production environment. For example, an application might be developed and tested on a non-clustered host for eventual deployment onto clustered hosts. Mismatches like this between your development and production environments can slow the development process for business applications because certain problems might be missed in testing and only become apparent when the applications are deployed to production, which might necessitate further testing and development until the applications are behaving as intended. With the cloud, however, you can perform your development and testing in the same kind of environment that your applications will be deployed upon—the computing, storage, and networking resources provided to you by your hoster. This can make testing applications simpler and more reliable, thereby reducing the time to deployment.

**Scale:**

Cloud applications can also scale out quickly because commodity compute, storage, and networking resources are pooled by the hoster and can be provisioned to the tenant (your business) as the need arises. Does your application need more compute resources to meet increasing demand from customers? Running it in the cloud can help keep your customers happy. Does a downturn in the market mean that you don’t need all that compute capacity your hoster is providing for your applications? Just scale down how much of your hoster’s compute capacity you are using. In addition to scaling capacity up or down quickly, cloud computing can also provide your applications with global scale and reach for extending your business presence around the world. Such scalability can be essential for businesses to remain competitive in today’s global economy.

**Economics:**

Regarding economic efficiencies, many organizations decide to make the move to the cloud because the cost of running their business applications in the cloud can be significantly lower than running them on-premises. By utilizing a pay-for-what-you-use model for cloud computing, your business only pays for the resources it consumes. The ability to rapidly and easily scale capacity up or down that the cloud offers makes this approach possible and can help organizations save money. In fact, some Windows Azure services, such as Windows Azure Virtual Machines, now support per-minute billing to help customers minimize the cost of running their server workloads in Windows Azure. Cloud computing can also make economic sense for businesses when it comes to hardware acquisition costs. Traditionally, large enterprises have often purchased and deployed storage area networks (SANs) from third-party SAN vendors to meet their escalating data storage needs. By provisioning storage resources from a cloud hosting provider instead, these enterprises can often significantly reduce their storage acquisition and maintenance costs.

**Resisting the cloud:**

If running business applications in the cloud has so many advantages, why doesn’t every business do it? There are several possible reasons for this:

■ Companies that have made large investments in traditional IT infrastructure might prefer to have those investments earn out than adopt the cloud computing approach.

■ Enterprises that have a complex, heterogeneous IT landscape might find it challenging to integrate cloud computing into their existing infrastructure.

■ The reliability of the hosting provider is another issue for many companies. Lack of knowledge about the infrastructure used by the hoster for providing cloud services to customers can make some organizations reluctant to risk a move to the cloud.

■Business politics can also cause a company to resist migrating their applications to the cloud. The traditional in-house IT culture of control can make it difficult to embrace the cloud.

■ Organizations that have special requirements in the areas of security and compliance might have legal or regulatory requirements that block them from implementing different forms of cloud computing.

Windows Azure is an open and flexible cloud platform that enables you to quickly build, deploy, and manage applications across a global network of Microsoft-managed datacenters. You can build applications using any language, tool, or framework. And you can integrate your public cloud applications with your existing IT environment. This definition tells us that Windows Azure is a cloud platform, which means you can use it for running your business applications, services, and workloads in the cloud. But it also includes some key words that tell us even more:

■ **Open Windows** Azure provides a set of cloud services that allow you to build and deploy cloud-based applications using almost any programming language, framework, or tool.

■ **Flexible** Windows Azure provides a wide range of cloud services that can let you do everything from hosting your company’s website to running big SQL databases in the cloud. It also includes different features that can help deliver high performance and low latency for cloud-based applications.

■ **Microsoft-managed** Windows Azure services are currently hosted in several datacenters spread across the United States, Europe, and Asia. These datacenters are managed by Microsoft and provide expert global support on a 24x7x365 basis.

■ **Compatible** Cloud applications running on Windows Azure can easily be integrated with on-premises IT environments that utilize the Microsoft Windows Server platform.

**Windows Azure services**

Windows Azure provides businesses with four basic categories of cloud-based services:

■ Compute services

■ Network services

■ Data services

■ App services

**Compute services:**

Windows Azure compute services provide the processing power required for cloud applications to be able to run. Windows Azure currently offers four different compute services:

■ Virtual Machines This service provides you with a general-purpose computing environment that lets you create, deploy, and manage virtual machines running in the Windows Azure

■ Web Sites This service provides you with a managed web environment you can use to create new websites or migrate your existing business website into the cloud.

■ Cloud Services This service allows you to build and deploy highly available and almost infinitely scalable applications with low administration costs using almost any programming language.

■ Mobile Services This service provides a turnkey solution for building and deploying apps and storing data for mobile devices.

**Network services**:

Windows Azure network services provide you with different options for how Windows Azure applications can be delivered to users and datacenters. Windows Azure currently offers two different network services:

■ Virtual Network This service allows you to treat the Windows Azure public cloud as if it is an extension of your on-premises datacenter.

■ Traffic Manager This service allows you to route application traffic for the user who is using the application to Windows Azure datacenters in three ways: for best performance, in round robin fashion, or using an Active/Passive failover configuration.

**Data services**

Windows Azure data services provide you with different ways of storing, managing, safeguarding, analyzing, and reporting business data. Windows Azure currently offers five different data services:

■ Data Management This service lets you store your business data in SQL databases, either with dedicated Microsoft SQL Server virtual machines, using Windows Azure SQL Database, using NoSQL Tables via REST, or using BLOB storage.

■ Business Analytics This service enables ease of discovery and data enrichment using Microsoft SQL Server Reporting and Analysis Services or Microsoft SharePoint Server running in a virtual machine, Windows Azure SQL Reporting, the Windows Azure Marketplace, or HDInsight, a Hadoop implementation for Big Data.

■ HDInsight This is Microsoft’s Hadoop-based service which brings a 100 percent Apache Hadoop solution to the cloud.

■ Cache This service provides a distributed caching solution that can help speed up your cloud-based applications and reduce database load.

■ Backup This service helps you protect your server data offsite by using automated and manual backups to Windows Azure.

■ Recovery Manager Windows Azure Hyper-V Recovery Manager helps you protect business critical services by coordinating the replication and recovery of System Center 2012 private clouds at a secondary location.

**App Services:**

Windows Azure currently offers seven different app services:

■ Media Services This service allows you to build workflows for the creation, management, and distribution of media using the Windows Azure public cloud.

■ Messaging This consists of two services (Windows Azure Service Bus and Windows Azure Queue) that allow you to keep your apps connected across your private cloud environment and the Windows Azure public cloud.

■ Notification Hubs This service provides a highly scalable, cross-platform push notification infrastructure for applications running on mobile devices.

■ BizTalk Services This service provides Business-to-Business (B2B) and Enterprise Application Integration (EAI) capabilities for delivering cloud and hybrid integration solutions.

■ Active Directory This service provides you with identity management and access control capabilities for your cloud applications.

■ Multifactor Authentication This service provides an extra layer of authentication, in addition to the user’s account credentials, in order to better secure access for both on-premises and cloud applications.

**Windows Azure solutions**

While in its essence Windows Azure is simply a collection of different kinds of cloud services, it’s what you can do with these services that can make the platform appealing to businesses. In other words, it’s the solutions that matter most for business customers and not the underlying services needed to implement those solutions. With almost two dozen different services currently available with Windows Azure, the number and variety of different kinds of solutions that are possible is almost infinite. And that gets us back to our original answer to the question, “What is Windows Azure?” where we stated that: Windows Azure can be anything you want it to be but while the sky’s the limit as far as what you can do with Windows Azure, Microsoft has identified ten different solution categories where Windows Azure can bring significant benefits to businesses:

■ Infrastructure

■ Mobile

■ Web

■ Media

■ Integration

■ Identity & Access Management

■ Big Data

■ Dev & Test

■ Storage, Backup, & Recovery

■ Data Management

**Infrastructure**:

Windows Azure can provide your business with on-demand infrastructure that can scale and adapt to your changing business needs. You can quickly deploy new virtual machines in minutes, and with pay-as-you-go billing you won’t be penalized when you need to reconfigure your virtual machines. Windows Azure Virtual Machines even offers you a gallery of preconfigured virtual machine images you can choose from so you can get started as quickly as possible. You can also upload or download your virtual disks, load-balance your virtual machines, and integrate your virtual machines into your on-premises environment using virtual networks**.**

**Mobile Windows**:

Azure lets you build and deploy a back-end cloud solution for your mobile device apps. You can use popular development platforms like .NET or NodeJS to create your solution, then deploy it to the cloud using Windows Azure Virtual Machines, Cloud Services, or Mobile Services. Windows Azure Mobile Services, in particular, provides cross-platform support for developing solutions for almost any platform including Windows Phone, Windows Store, Android, Apple iOS, and HTML5. Windows Azure Notification Hubs lets you push out notifications to users to enable real-time interactive applications, and you can use social media platforms from Microsoft, Google, Facebook, or Twitter for user authentication purposes.

**Web:**

With support for both SNI and IP-based SSL certificates, and global datacenters with guaranteed SLA and 24/7 support available, Windows Azure can provide you with a robust and secure platform for giving your business website a global presence. You can use Windows Azure Active Directory for authentication and access control and can securely store your website’s business data in Windows Azure SQL Database, NoSQL Tables, BLOB storage. You can create your website using the language of your choice, such as ASP.NET, PHP, Node.js, Python, or even Classic ASP. And for even faster development, you can quickly build your site using a popular framework or template from the Windows Azure App Gallery, which includes WordPress, Umbraco, DotNetNuke, Drupal, Django, CakePHP, and Express.

**Media**:

Windows Azure Media Services makes it easy to give your business a global media presence. You can quickly build end-to-end media workflows using services from both Microsoft and its partners. Your media can be protected using Digital Rights Management (DRM), and Advanced Encryption Standard (AES) or Playready can be used to protect it during playback.

**Integration:**

Windows Azure provides several different options for integrating your existing on-premises infrastructure with your applications running in the Windows Azure public cloud. Windows Azure Service Bus can be used for communicating between your on-premises and cloud-based applications and services. Windows Azure BizTalk Services provides a robust business-to-business (B2B) and application integration PaaS in the cloud. And you can build your integration solution using the familiar tools of .NET and Visual Studio.

**Identity & access management:**

Windows Azure Active Directory (Windows Azure AD) can provide you with identity services running in the cloud that you can use for managing access by employees, partners, and customers to your corporate assets, including both on-premises and cloud assets. You can even synchronize your on-premises Active Directory infrastructure with Windows Azure AD to provide single sign-on (SSO) for users to access your cloud applications, and Windows Azure Multifactor Authentication can be used to provide an additional layer of authentication to help protect your sensitive business data and applications.

**Big data:**

Windows Azure enables you to quickly build a Hadoop cluster based on 100 percent Apache Hadoop. You can then use Windows Azure PowerShell and the Windows Azure Command-Line Interface to seamlessly integrate HDInsight into your existing analysis workflows and gain actionable insights from HDInsight by mining data with Microsoft Excel.

**Dev &test:**

Windows Azure makes rapid application development and testing easy. Instead of having to go through a traditional procurement process and wait for the new hardware you ordered to arrive, you can simply use Windows Azure Virtual Machines to spin up as many virtual machines as you need and perform your application development and testing in the cloud. Then once your application has been validated, you can deploy it into a production environment that’s identical to your test environment but also provides you with enhanced performance, infinite scalability, and global reach.

**Storage, backup, &recovery:**

Windows Azure Storage can provide you with secure and reliable storage for all your business needs. Geo-replication across different geographical regions ensures redundancy so you can be sure of being able to access your data in the event that a local disaster occurs. Windows Azure Storage can not only scale to meet whatever needs your business might have, it’s also very cost-effective since you only pay for what you use.

**Data management:**

Windows Azure data services can provide you with a consistent experience whether you’re working with relational or nonrelational data and currently supports SQL databases up to 150 GB in size. You can utilize your existing data management skills, such as relational database design and Transact-SQL, and can mix and match data across a variety of different data services to create just the solution your business needs.

**Business Systems Options for Software**

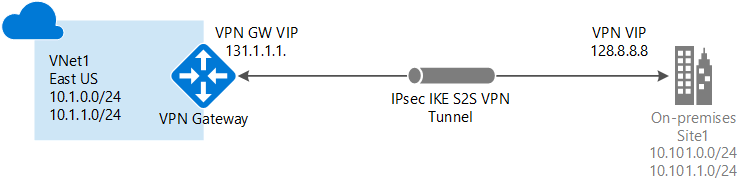
* WINDOWS 7 OS/ WINDOWS XP /WINDOWS VISTA
* Browser: Mozilla Firefox, Chrome
* High Speed Internet
* Microsoft Azure Account

# Business Systems Option for Hardware

* PROCESSOR:2GHz
* RAM : 4GB DD RAM
* HARD DISK: 250GB

**5. SYSTEM DESIGN**

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. A VPN gateway is an azure managed service that is deployed into a vnet and provides the end point for VPN connectivity for site-to-siteVPN. This gateway is a connection point into azure from on premises network (site to site).

****

**Figure 1: VIRTUAL GATEWAY CONNECTION TO ON PREMISES**

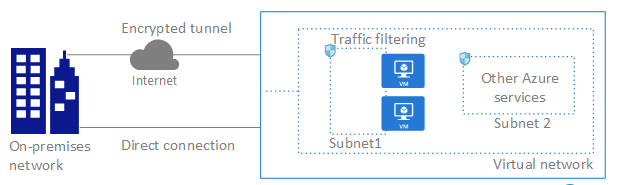


Figure 2: ON **PREMISES TO AZURE CONNECTION**

The Azure Virtual Network service enables to securely connect Azure resources to each other with virtual networks. A virtual network is a representation of own network in the cloud, it the logical isolation of the azure cloud dedicated to subscription.

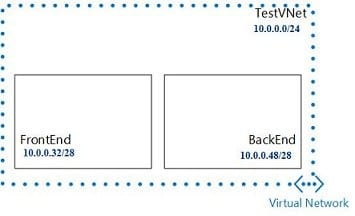


Figure 3: **VIRTUAL NETWORK SUBNET**

Virtual Network can be segmented into multiple subnets. Sub netting allows to create multiple logical networks that exist within a single network, by default there is no security boundary between subnets, so services in each of these subnets can talk to one another.

**5. CODING**

JSON file that defines a simple **Virtual Network with no VPN**.

{

  "$schema": ""<https://mspnp/template-building-blocks/master/schemas/buildingBlocks.json>",

  "contentVersion": "1.0.0.0",

  "parameters": {

    "buildingBlocks": {

      "value": [

        {

          "type": "VirtualNetwork",

          "settings": [

            {

              "name": "Vnet 1",

              "addressPrefixes": [

                "172.16.0.0/16"

              ],

              "subnets": [

                {

                  "name": "GatewaySubnet",

                  "addressPrefix": "172.16.0.0/24"

                },

                {

                  "name": "Subnet-001",

                  "addressPrefix": "172.16.1.0/24"

                }

              ]

            }

          ]

        }

      ]

    }

  }

}

This JSON defines a single Virtual Network, named Vnet1, with an address range and two subnets, named Gateway Subnetand Subnet-1, each with their own address ranges also. Gateway Subnet is going to be used exclusively by our VPN infrastructure later on and Subnet-1 is a normal subnet for any VMs we want to connect to over the VPN.

* **$schema”**: a schema definition for a building blocks parameters file.
* **“value”**: An array containing a series of object definitions representing Azure resources.
* **“type”**: the type of an Azure resource required.
* **“settings”**: type-specific settings for the resource. Can be required or optional.

**Establishing the VPN connection:**

|  |
| --- |
| {    "$schema": "<https://mspnp/template-building-blocks/master/schemas/buildingBlocks.json>",    "contentVersion": "1.0.0.0",    "parameters": {      "buildingBlocks": {        "value": [          {            "type": "VirtualNetwork",            "settings": [              {                "name": "Azure-VNet",                "addressPrefixes": [                  "172.16.0.0/16"                ],                "subnets": [                  {                    "name": "GatewaySubnet",                    "addressPrefix": "172.16.0.0/24"                  },                  {                    "name": "Subnet-001",                    "addressPrefix": "172.16.1.0/24"                  }                ]              }            ]          },          {            "type": "VirtualNetworkGateway",            "settings": [              {                "name": "Azure-VNet-Gateway",                "gatewayType": "VPN",                "VPNType": "RouteBased",                "sku": "Basic",                "isPublic": true,                "virtualNetwork": {                  "name": "Vnet 1"                }              }            ]          },          {            "type": "Connection",            "settings": [              {                "name": "Azure-VPN-Connection",                "connectionType": "IPsec",                "routingWeight": 10,                "VPNType": "RouteBased",                "sharedKey": "Vaishnavi123",                "virtualNetworkGateway": {                  "name": "Azure-VNet-Gateway"                },                "localNetworkGateway": {                  "name": "Azure-Local-Gateway",                  "ipAddress": "2.219.71.91",                  "addressPrefixes": [                    "192.168.0.0/24"                  ]                }              }            ]          }        ]      }    }  } |

The above JSON with type Connection defines the cloud-side of the site-to-site VPN connection, i.e., configures IPsec and the pre-shared authentication key. It specifies the virtual network gateway and local network gateway that will form the connection. Understandably, Azure needs more information about your local Network Gateway than the cloud-side gateway. Its properties are:

* name: specifies a name for your local gateway configuration in Azure.
* Ip Address: the public IP address of your on-premises local gateway.
* address Prefixes specifies the IP ranges whose traffic should be sent over the private connection to your local gateway.

**7. TESTING**

**TESTING METHODOLOGIES USED**

**BLACK BOX TESTING-**

Black Box Testing is a [software testing](https://www.softwaretestingmaterial.com/software-testing/) method in which testers evaluate the functionality of the software under test without looking at the internal code structure. This can be applied to every [level of software testing](https://www.softwaretestingmaterial.com/levels-of-testing/) such as Unit, Integration, System and Acceptance Testing.

**FUNCTIONAL TESTING-**

Validating aSite-to-Site VPNconforms to and correctly performs all its required functions. This entails a series of tests which perform a feature-by-feature validation of behavior, using a wide range of normal and erroneous input data. This can involve testing of the product’s user interface, APIs, database management, security, installation, networking, etc. Functional testing can be performed on an automated or manual basis using black box or white box methodologies

**SYSTEM TESTING-**

Testing conducted on a complete, integrated system to evaluatethe system’s compliance with its specified requirements. System testing falls within thescope of black box testing, and as such, should require no knowledge of the inner designof the code or logic.

**UNIT TESTING-**

Functional and reliability testing in an Engineering environment. Producing tests for the behavior of components of a product to ensure their correct behavior prior to system integration.

**WHITE BOX TESTING-**

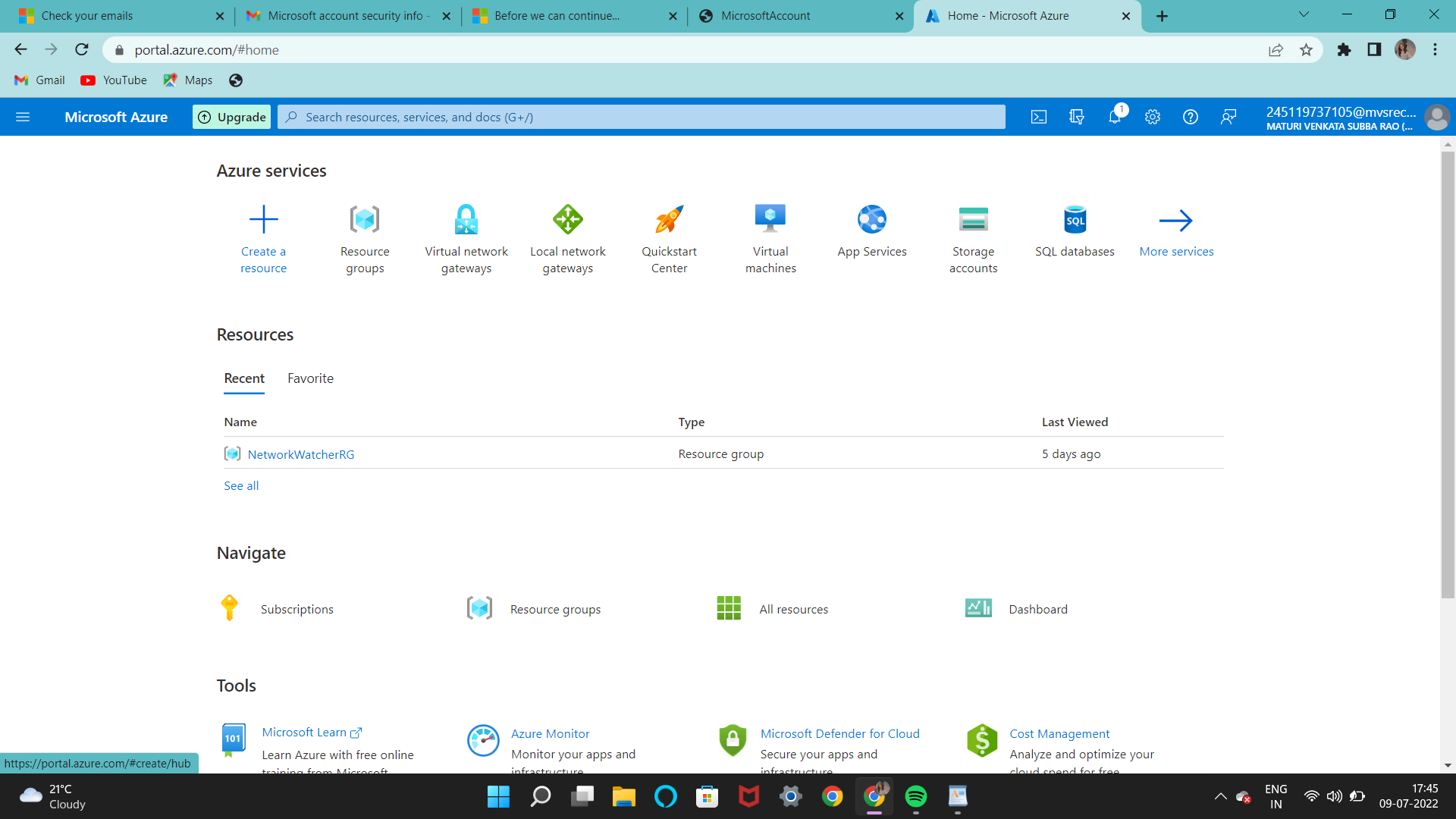
Testing based on an analysis of internal workings andstructure of a piece of software. Includes techniques such as Branch Testing and PathTesting. Also known as Structural Testing and Glass Box Testing

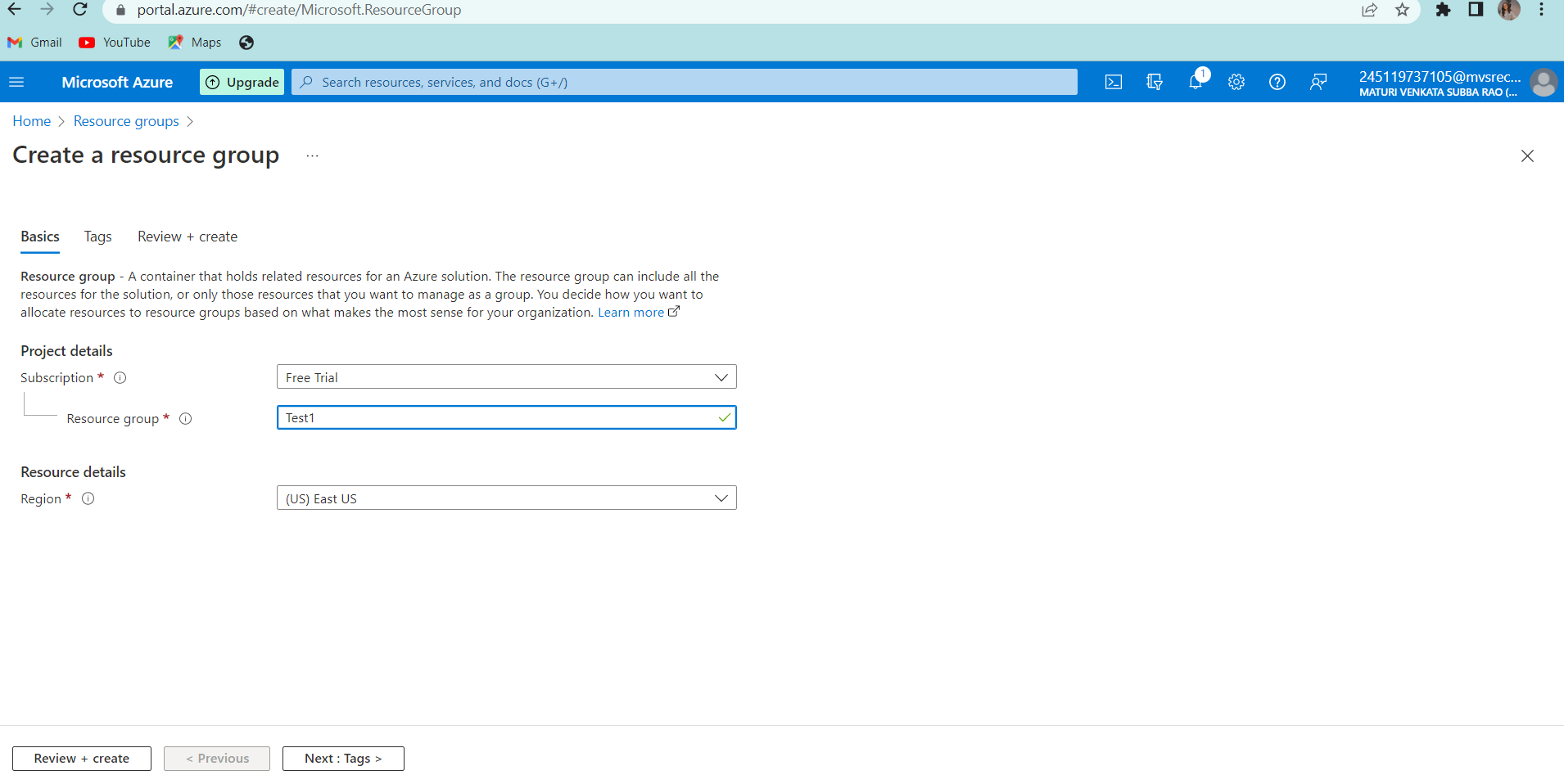
# Test cases and Test Results

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**8. IMPLEMENTATION**

A virtual private network i.e., VPN consists of multiple remote peers transmitting private data security to one another over a secured network, such as internet. Most of the site-to-siteVPNs are implemented based on IPsec policies.



Fig 1: Create a resource

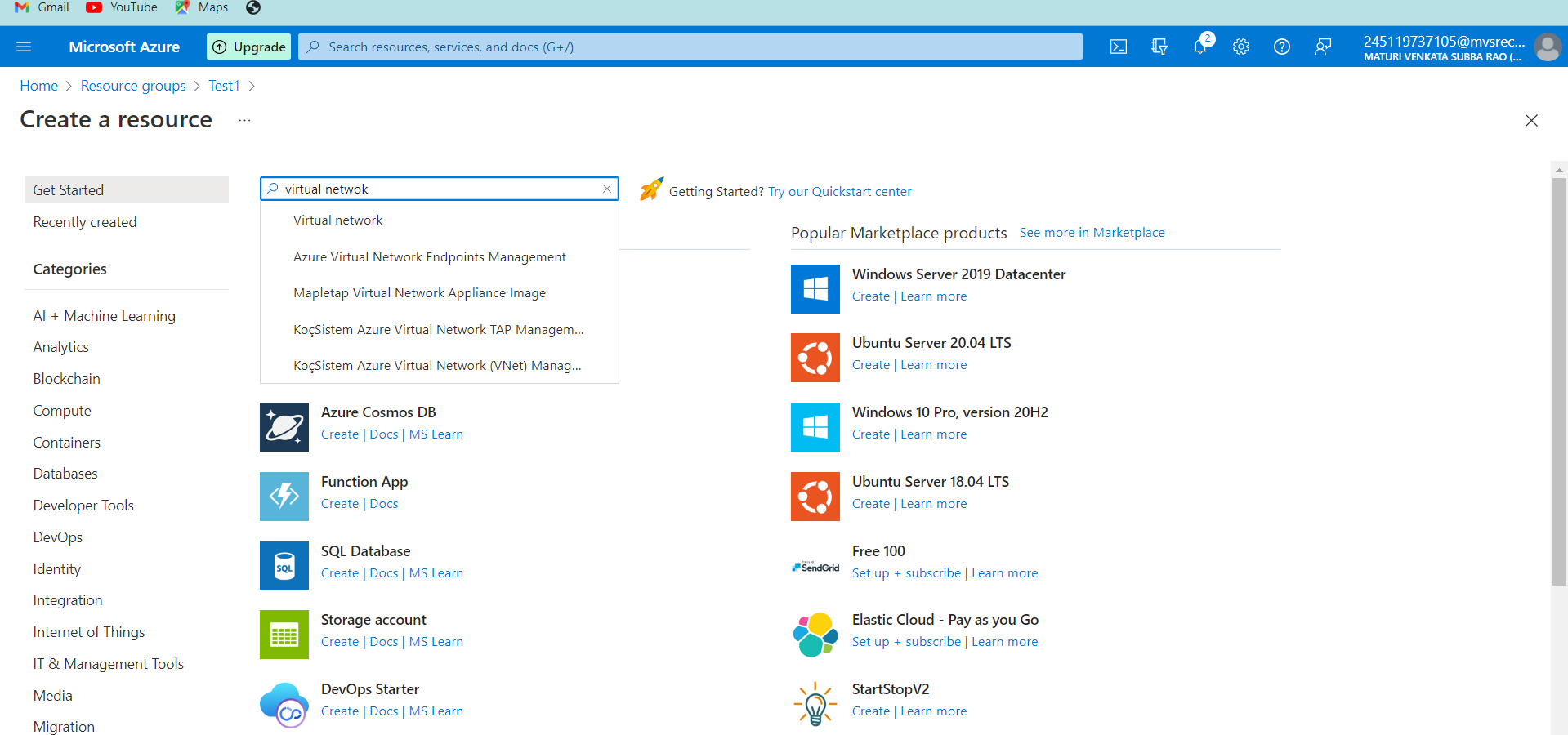
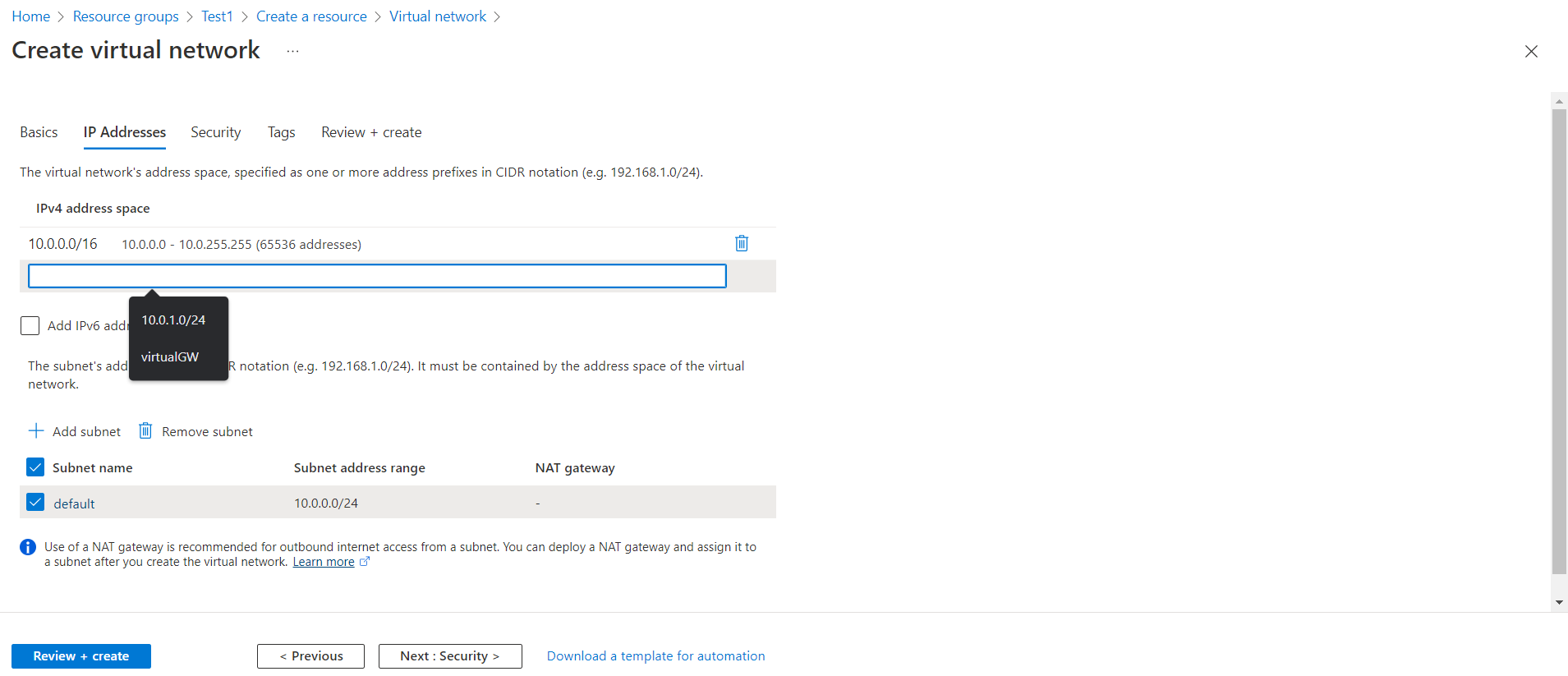


Fig 2: Create a virtual network

In the **search market field** field, type 'virtual network'. Locate **Virtual network**from the returned list and click to open the **Virtual Network** page.



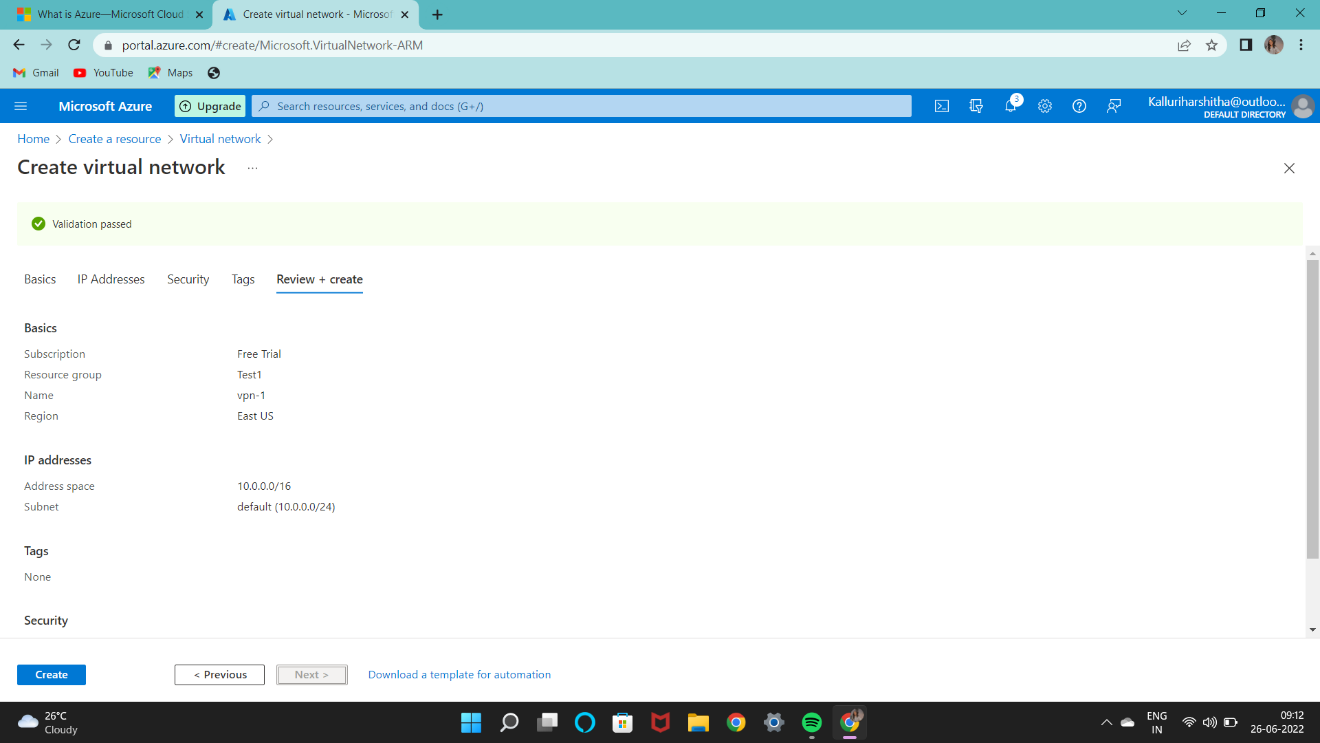


Fig 2.1: creating virtual network

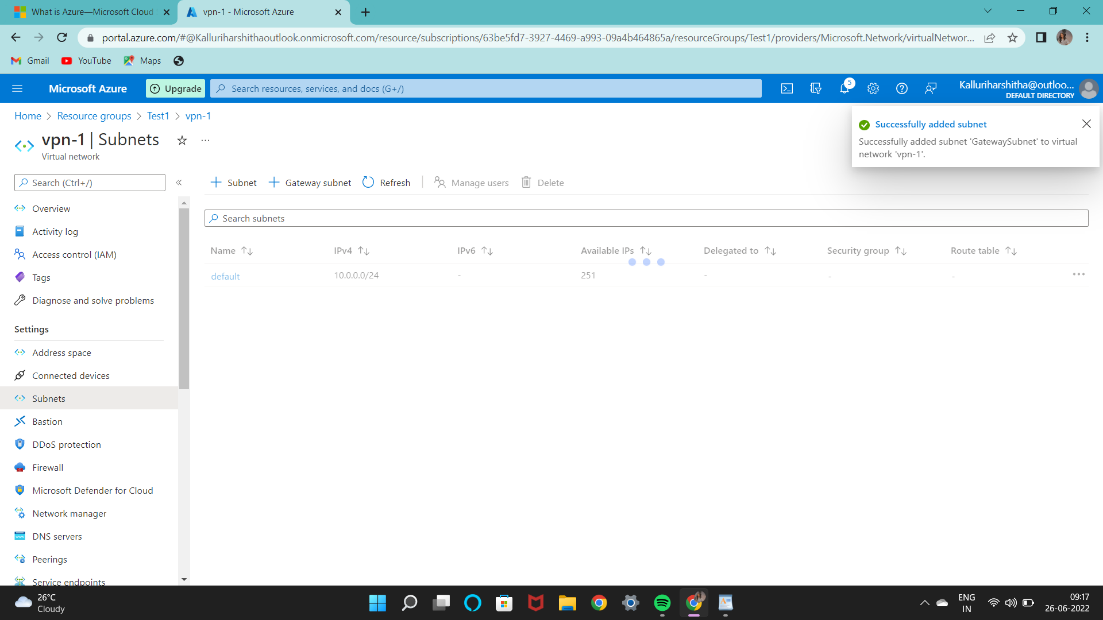
While creating the virtual network, the different fields like:

Name – The name of our virtual machine

Address space – number of address spaces or memory required.

Subnet – subnet with its range is added.

And create button is pressed.



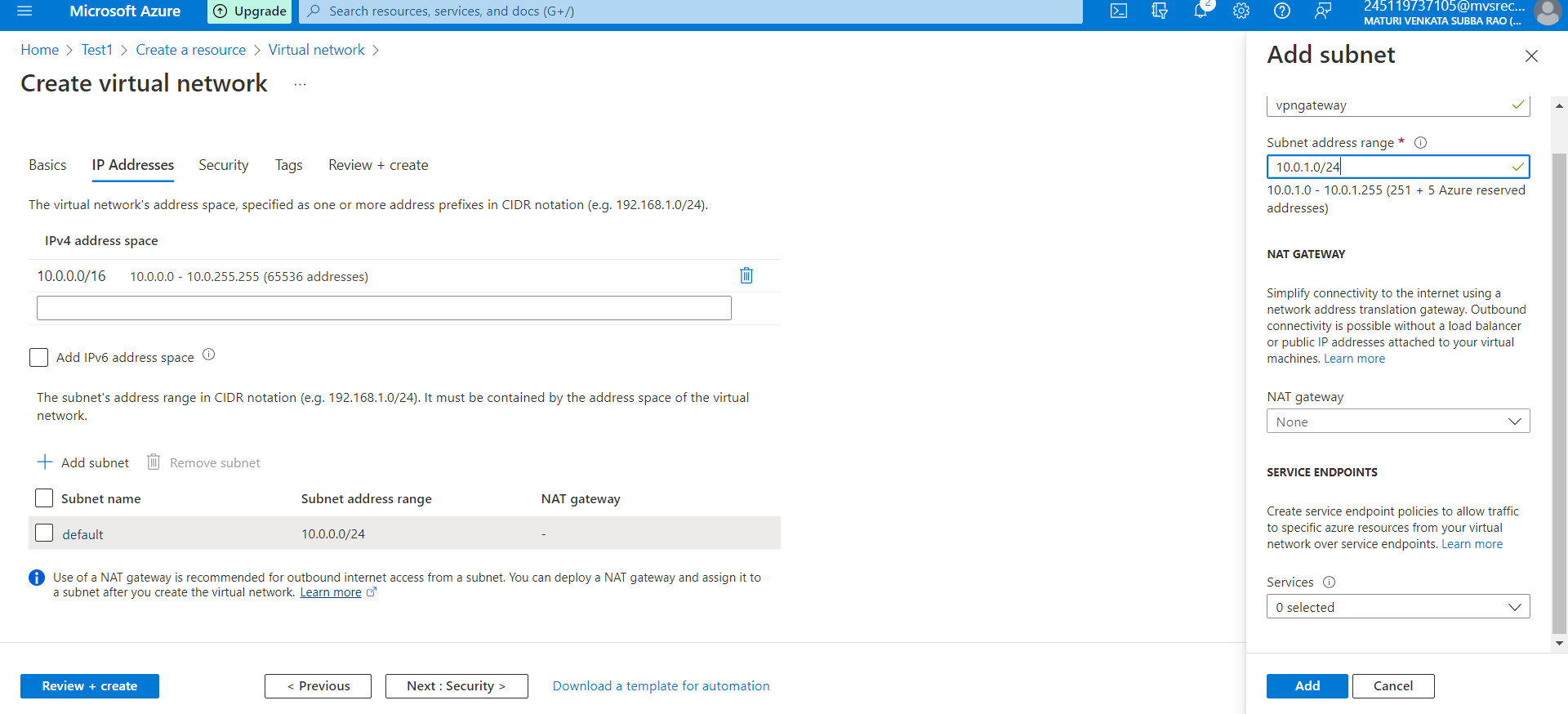
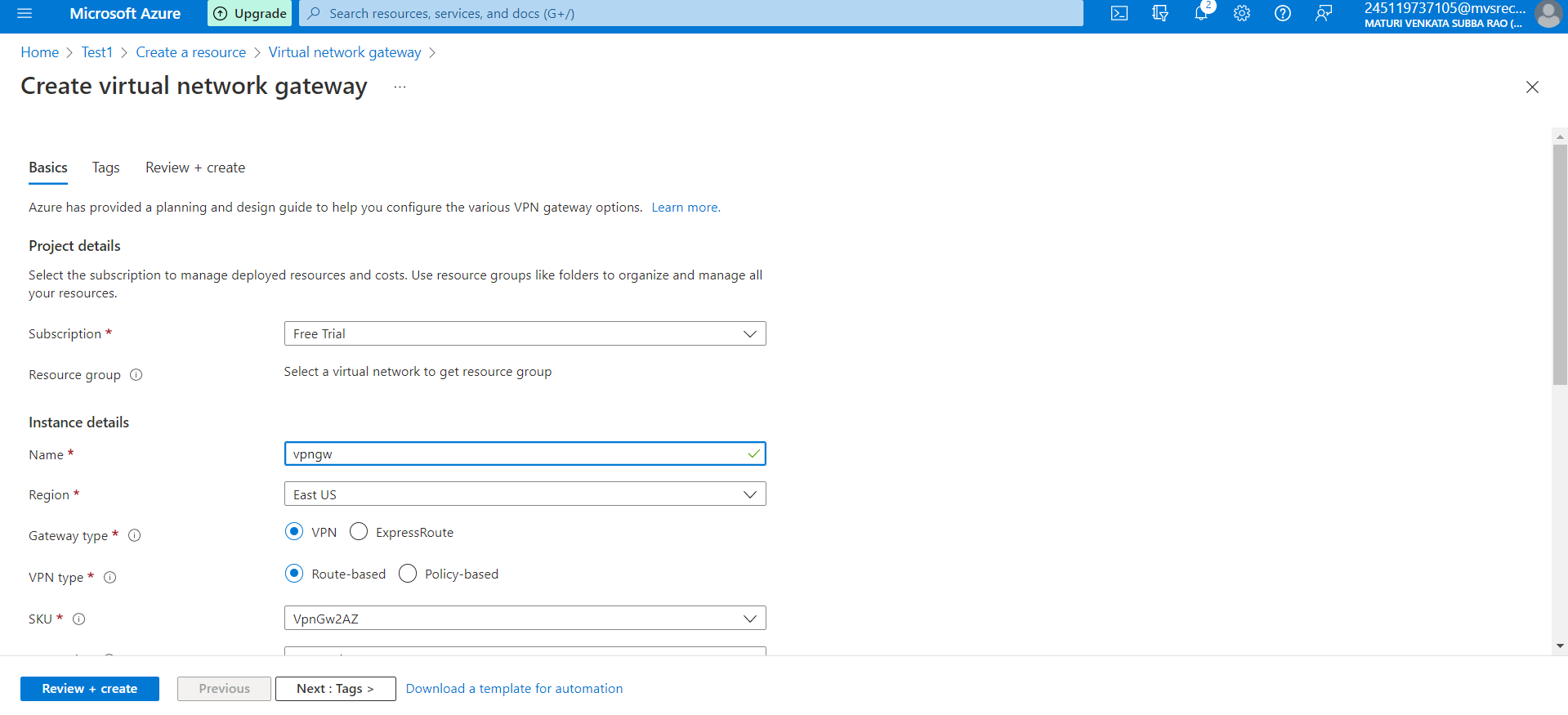


Fig 5: gateway subnet

The virtual network gateway uses 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. The subnet must be named 'Gateway Subnet' for Azure to deploy the gateway resources.



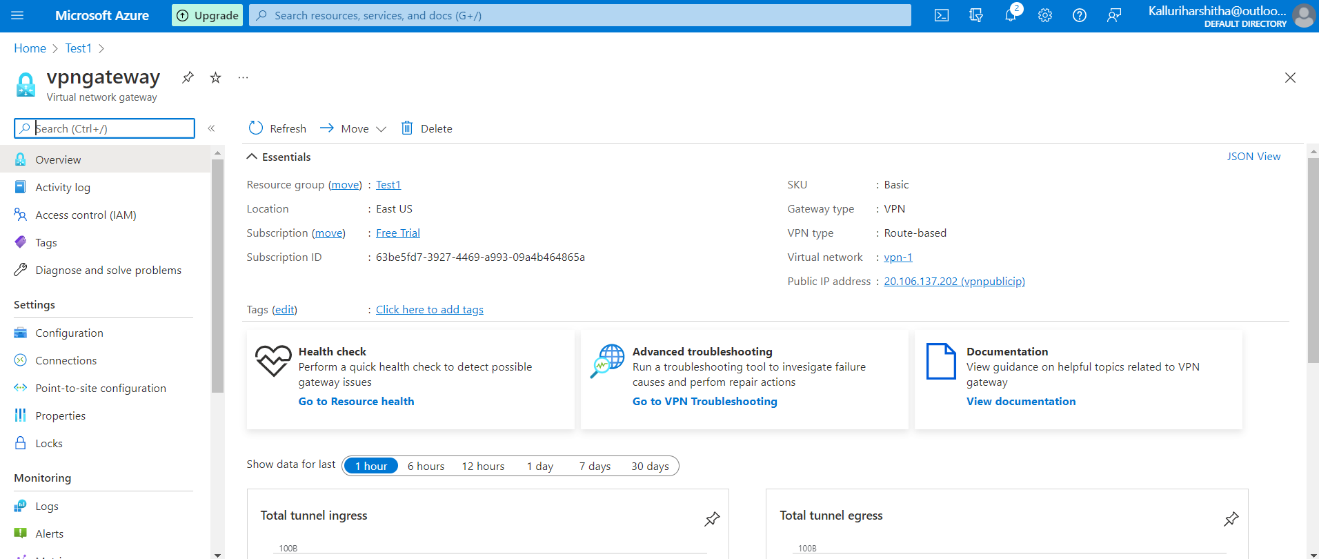
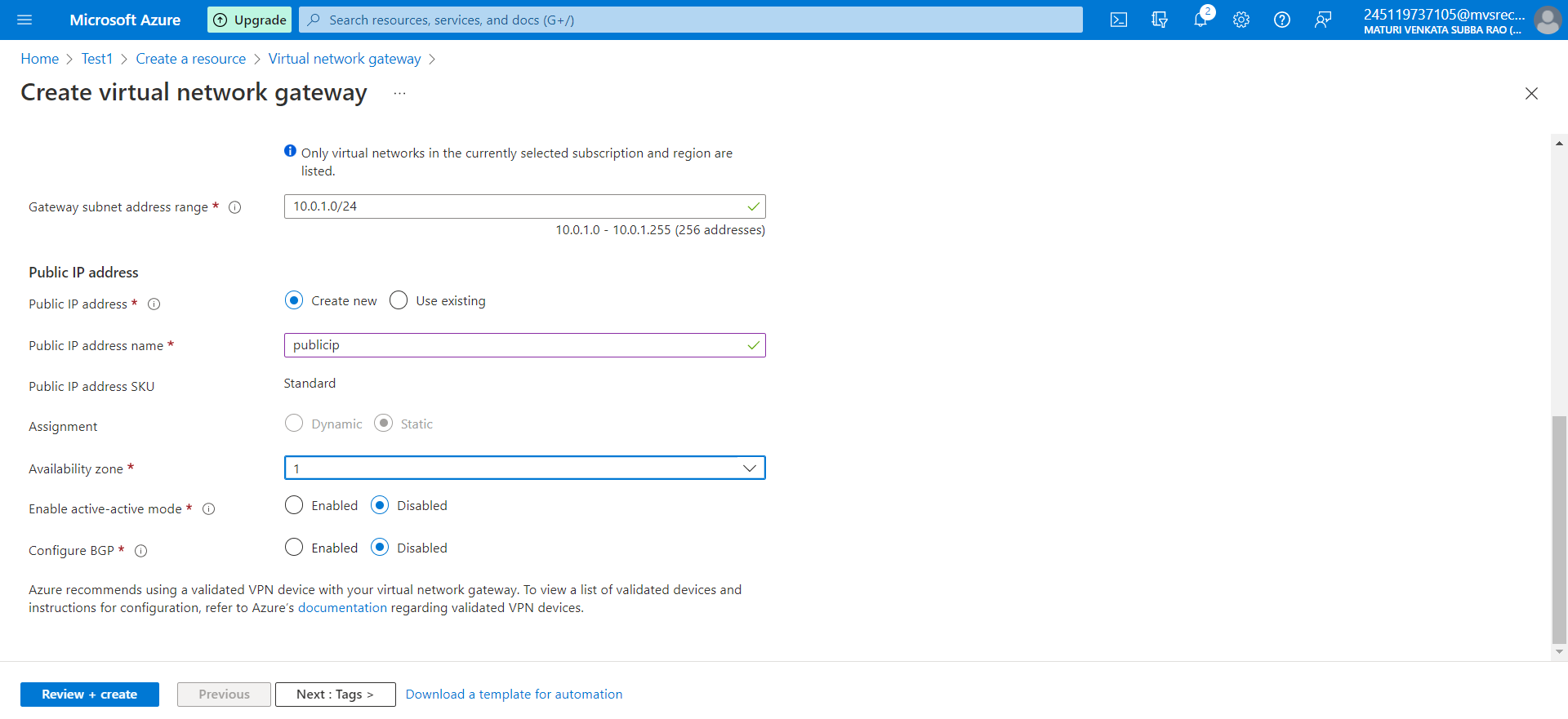
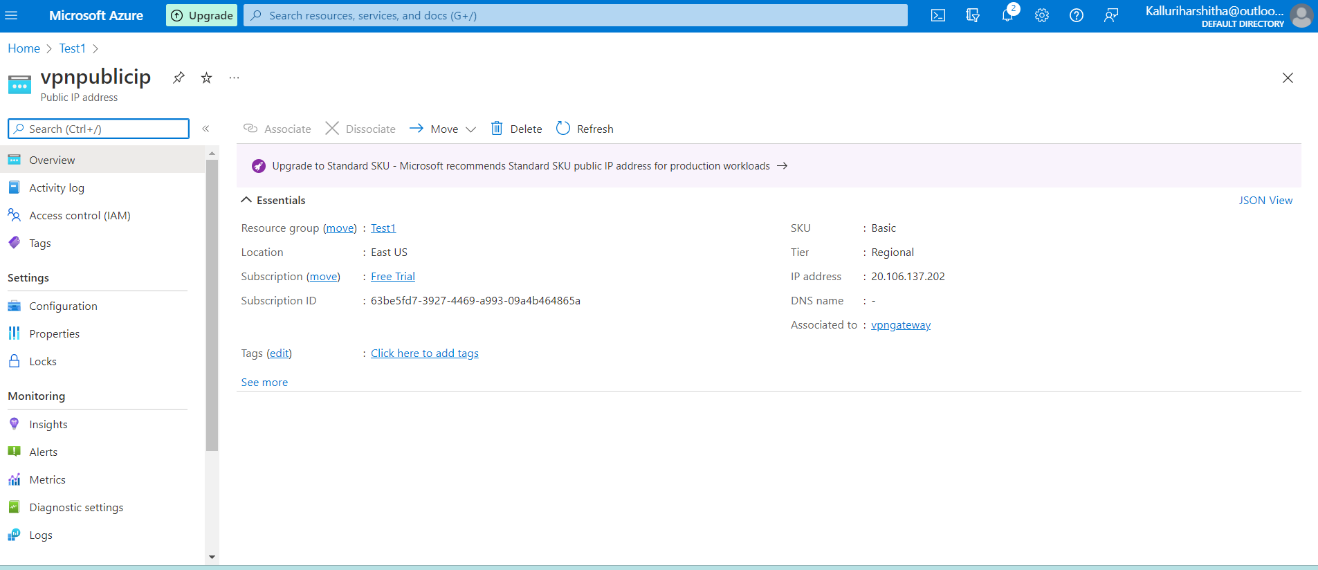


Fig 6: virtual network gateway

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet





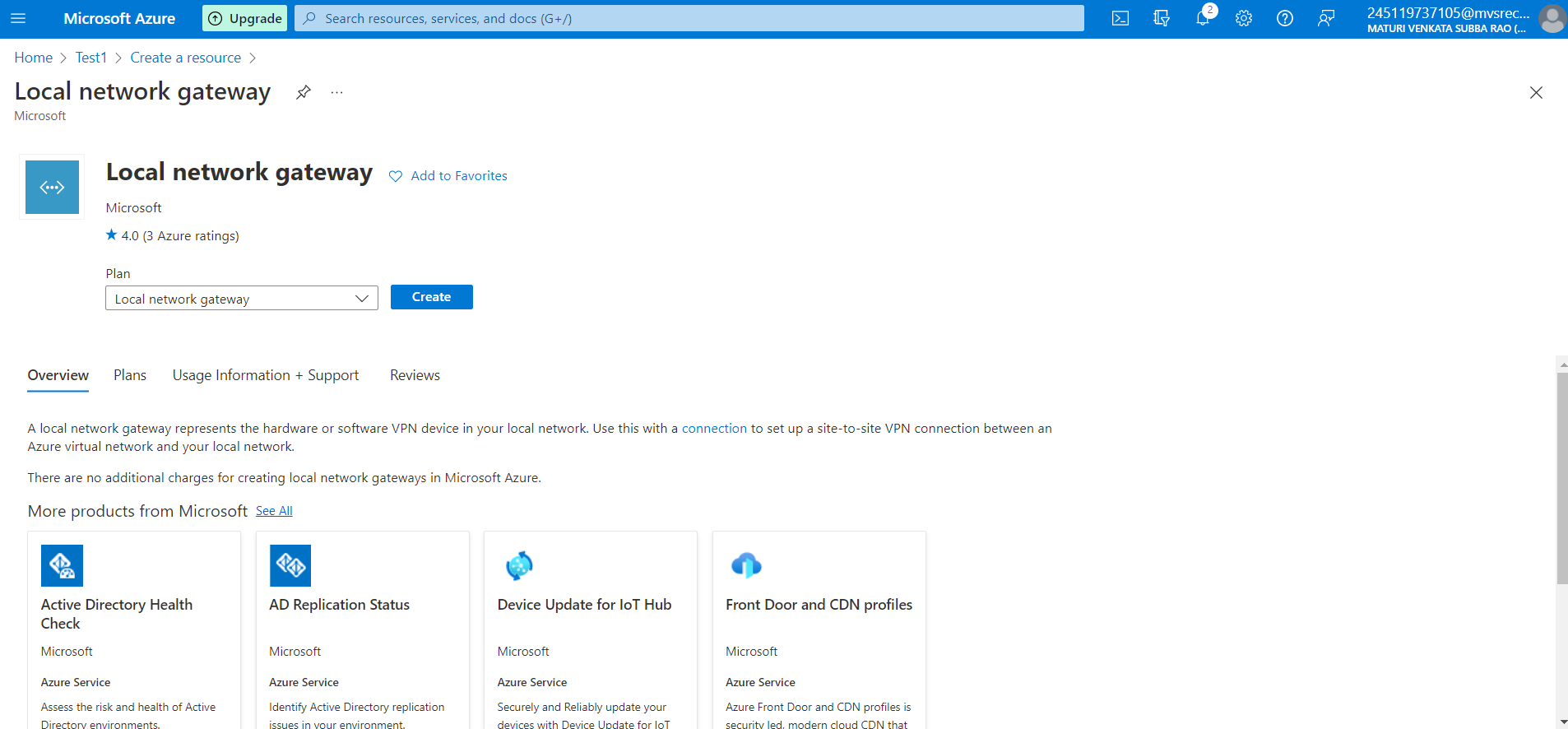
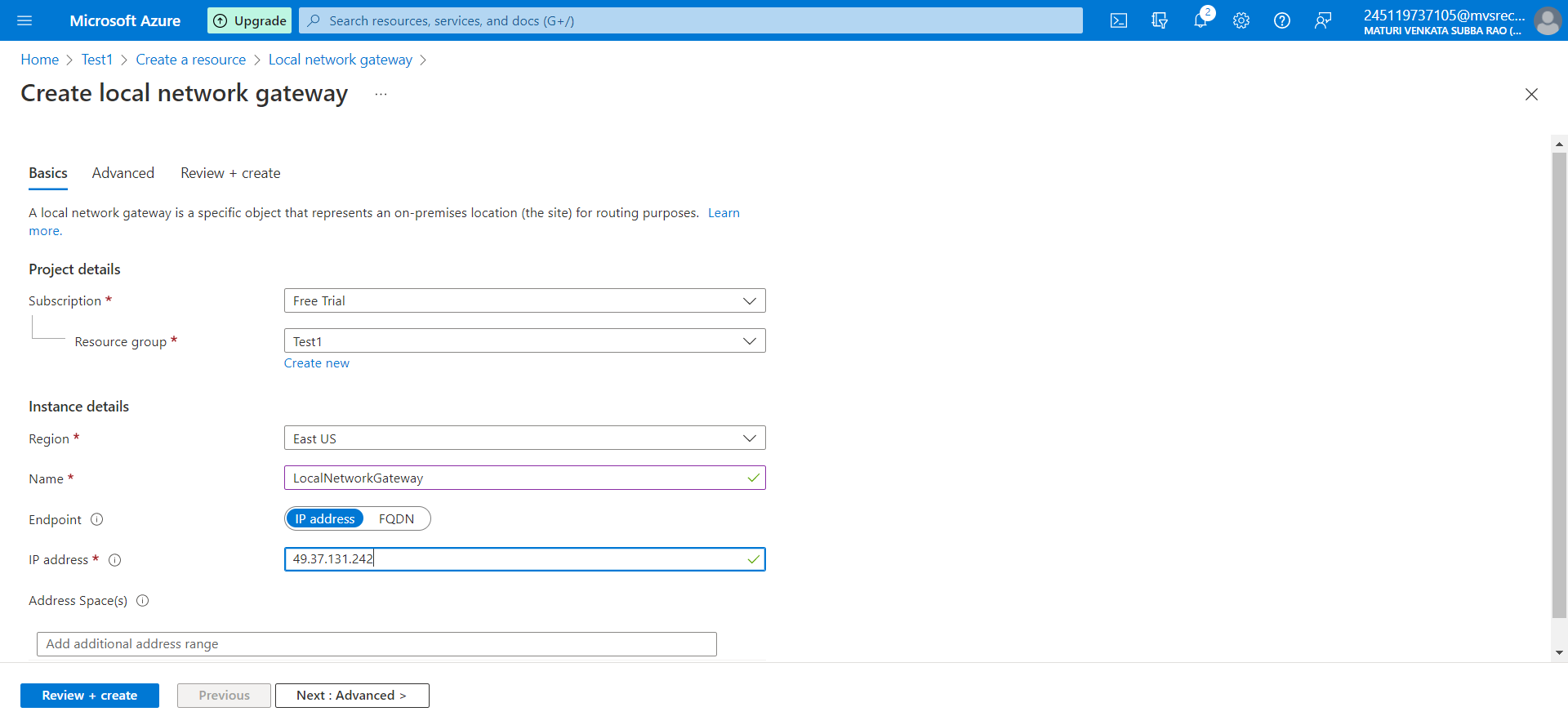
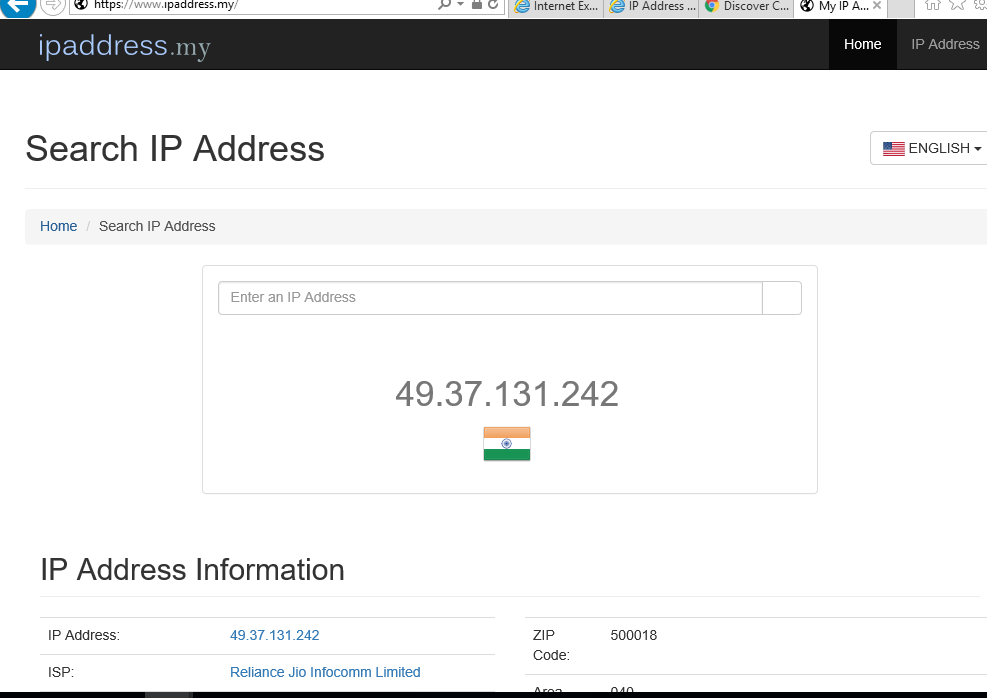
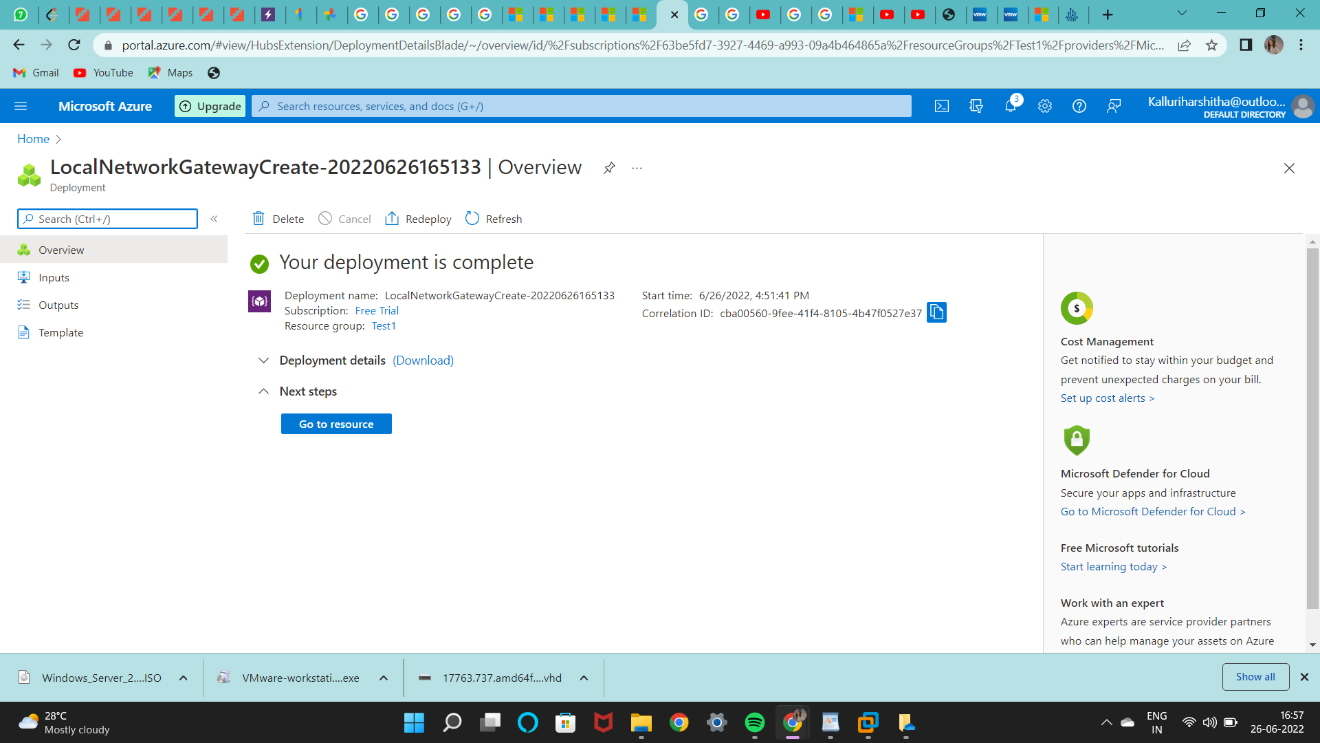


Fig 7: local network gateway

The local network gateway typically refers to your on-premises location.







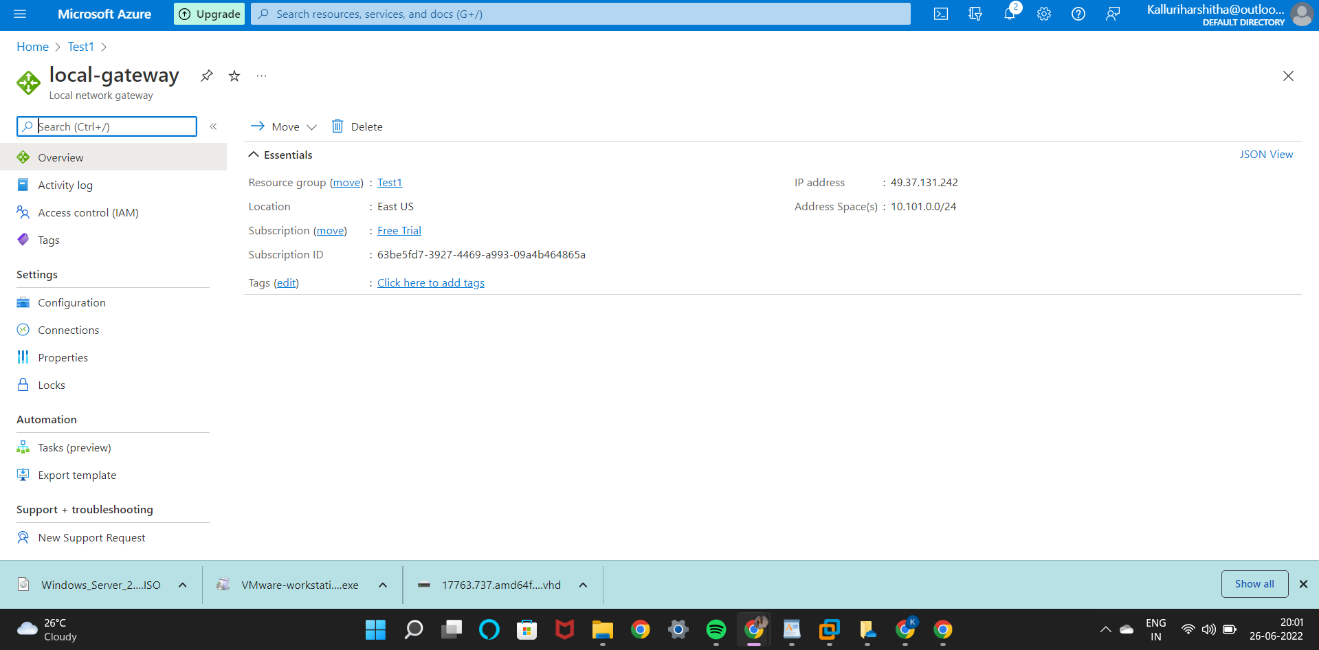
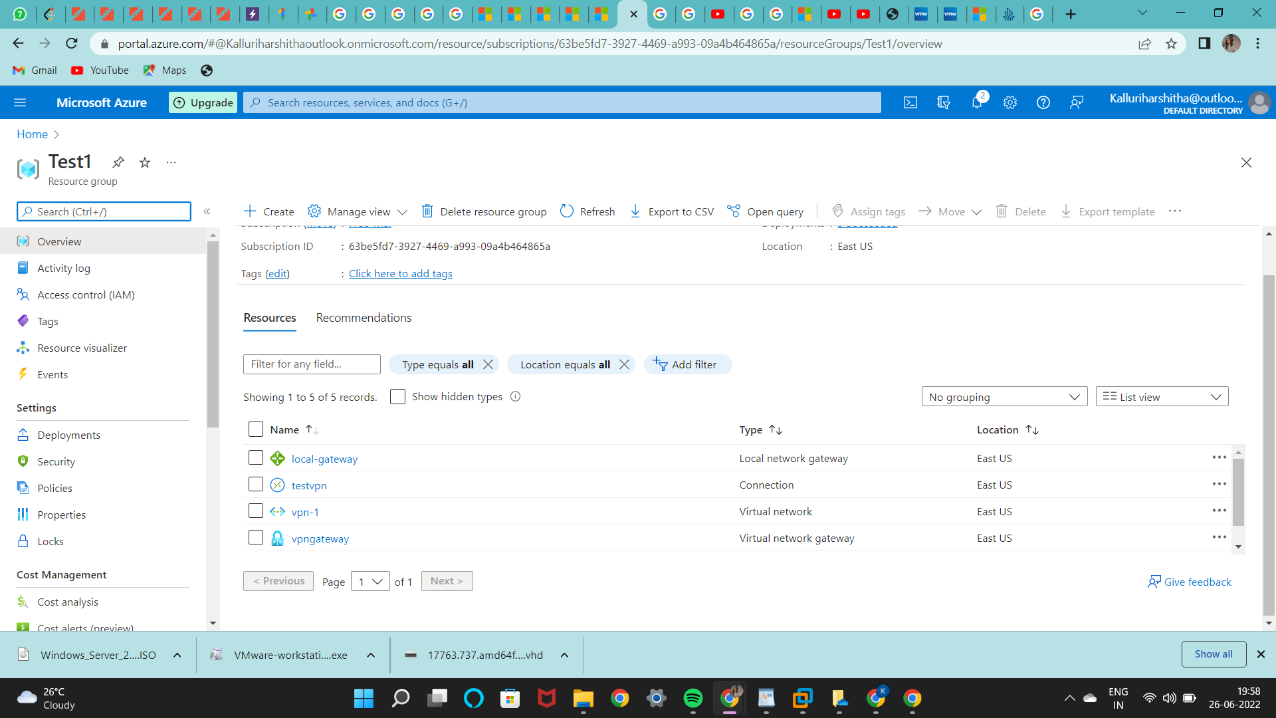


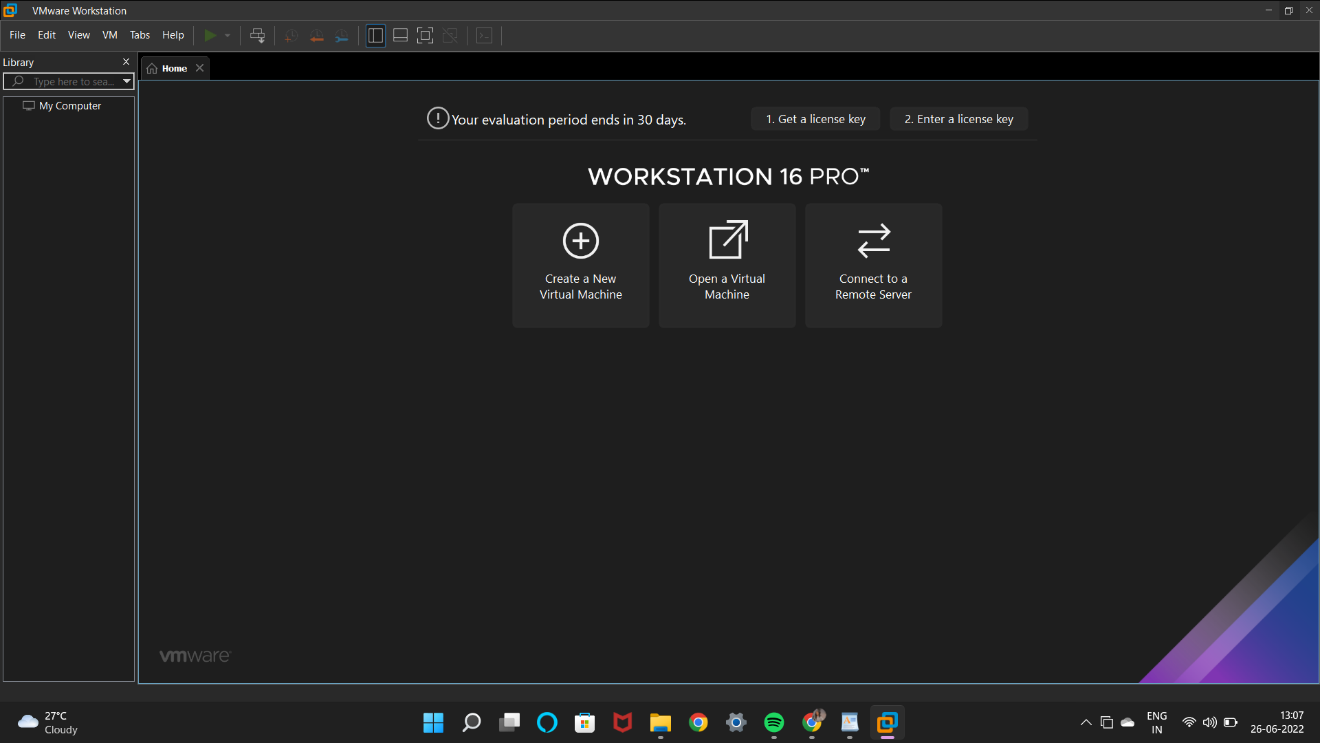
Fig 7.2: status of local network gateway



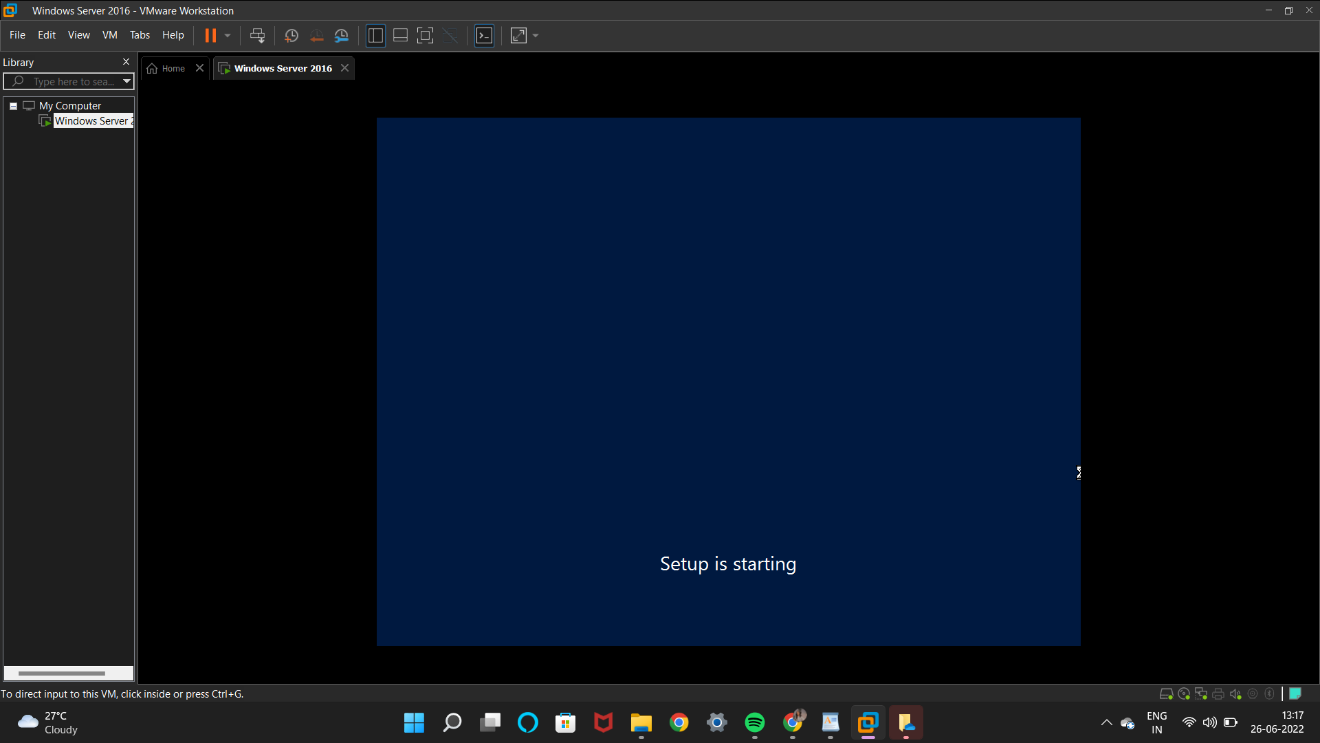
## **Configure your VPN device**

Site-to-Site connections to an on-premises network require a VPN device. Here we need to configure the VPN device. When configuring VPN device:

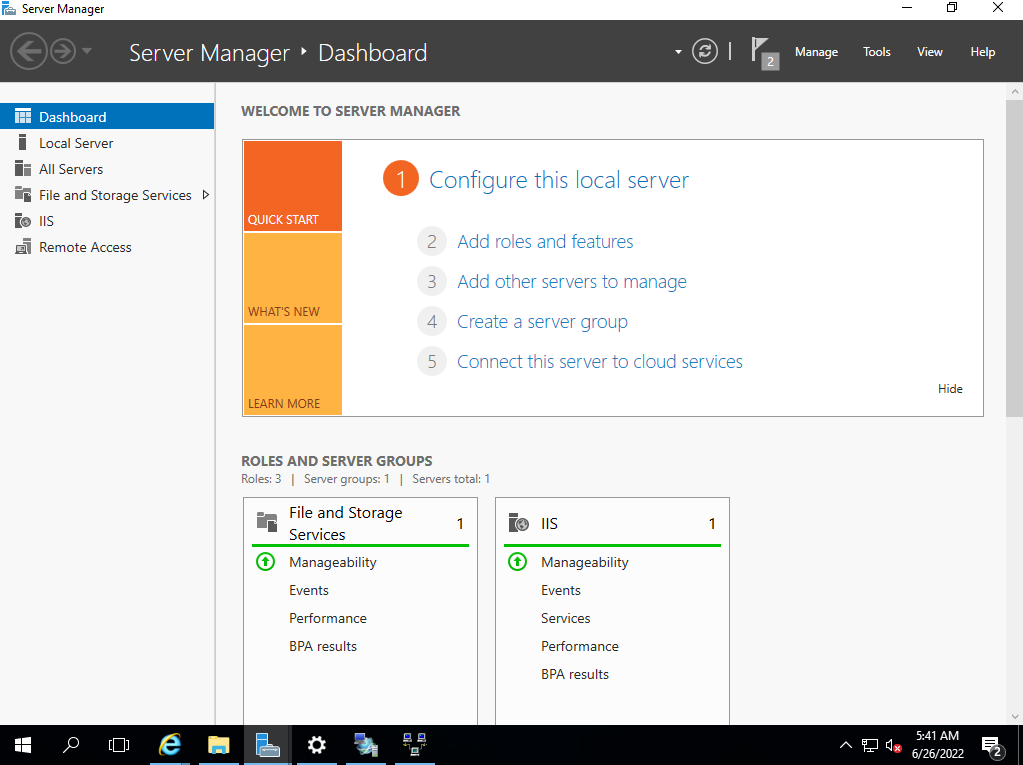
* A shared key. This is the same shared key that you specify when creating your Site-to-Site VPN connection. In our examples, we use a basic shared key. We recommend that you generate a more complex key to use.
* The Public IP address of your virtual network gateway. You can view the public IP address by using the Azure portal, PowerShell, or CLI. To find the Public IP address of your VPN gateway using the Azure portal, navigate to **Virtual network gateways**, then click the name of your gateway
* The shared Key is given while configuring the on site to on premises that is on our vmwareworkstationwindow server.



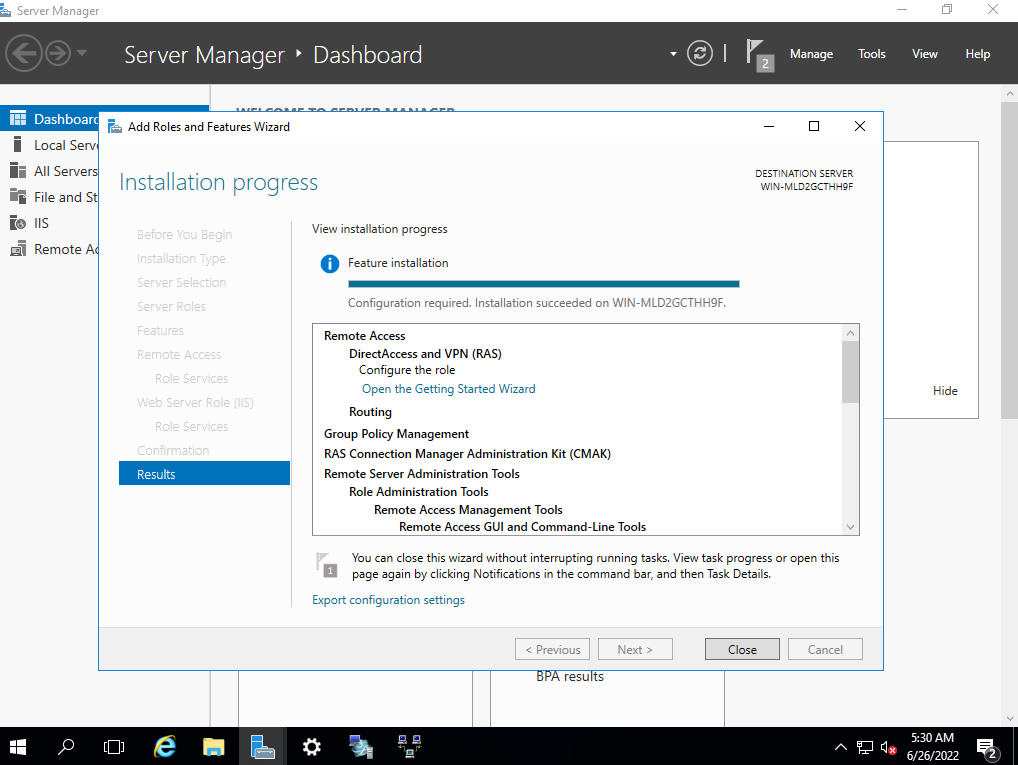
Vmware Workstation Environment

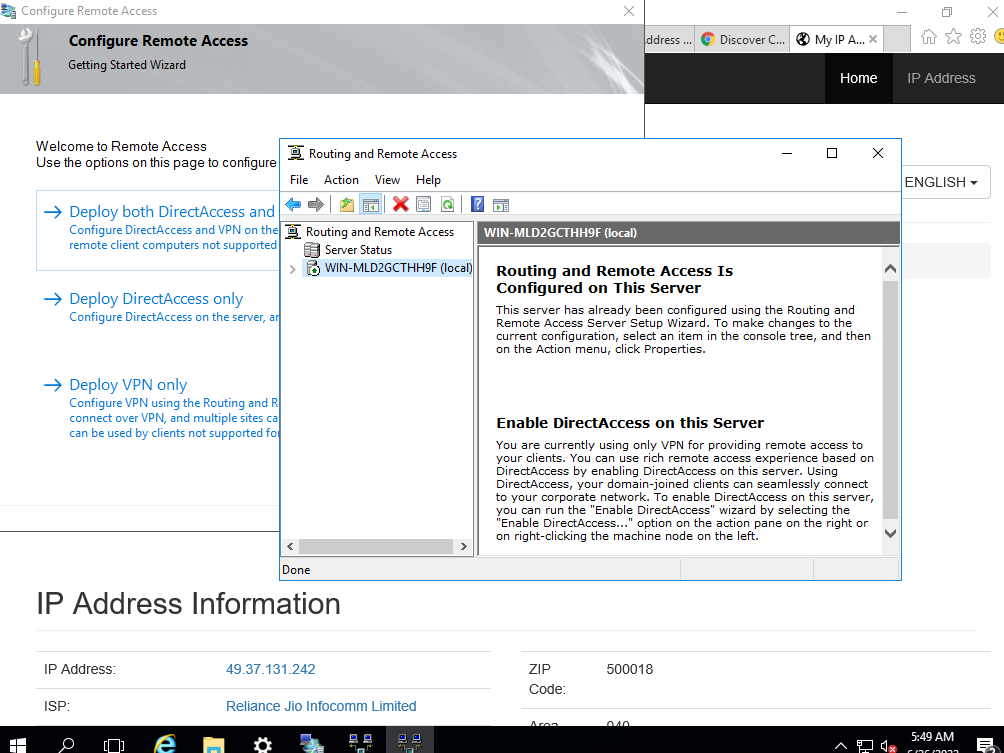


Creation of the roles and features on the server manager -Enable the routing and remote access for establishing the connections

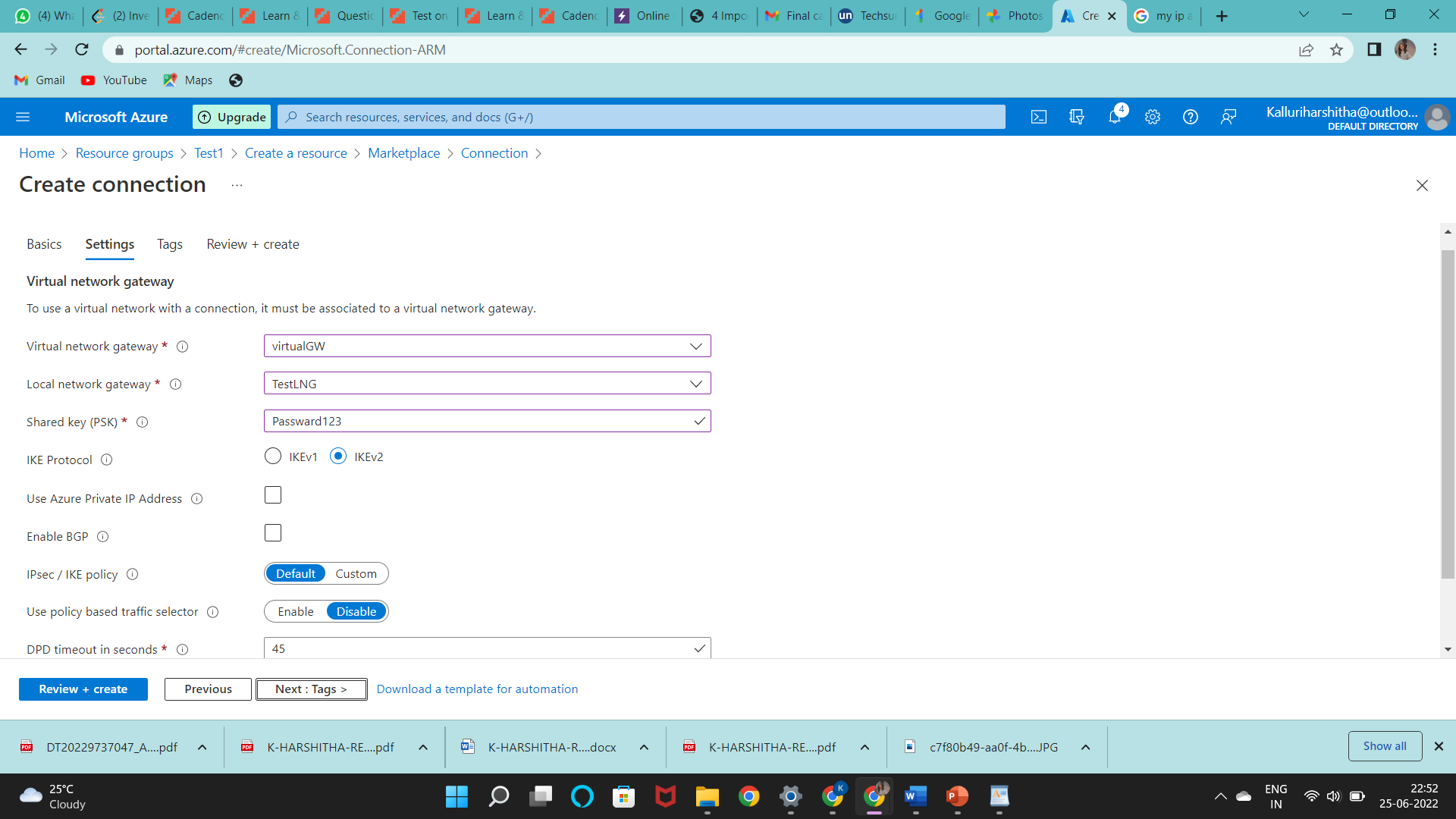


* Creating roles and features





* Enabling the routing and remote access on premises.



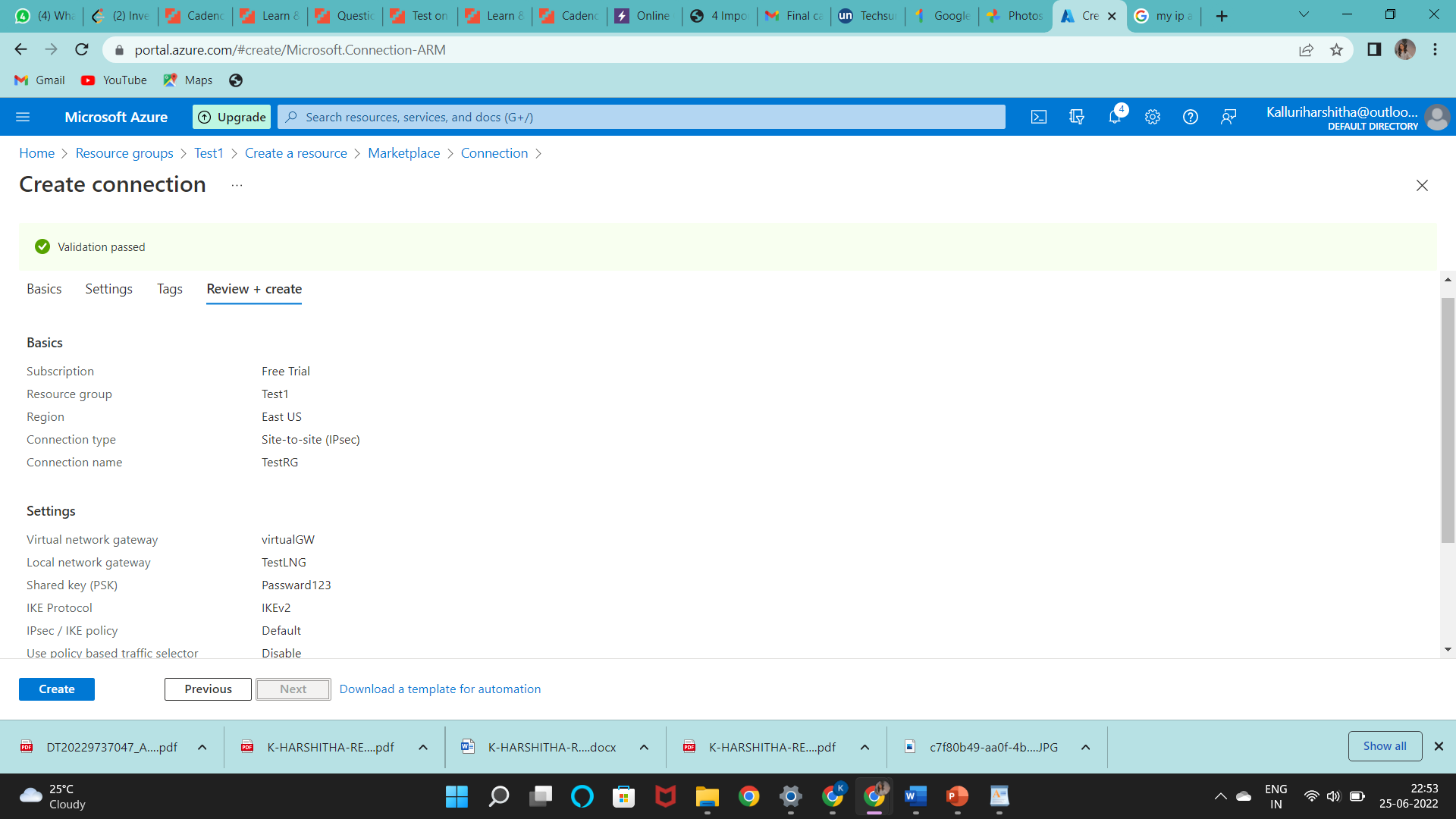
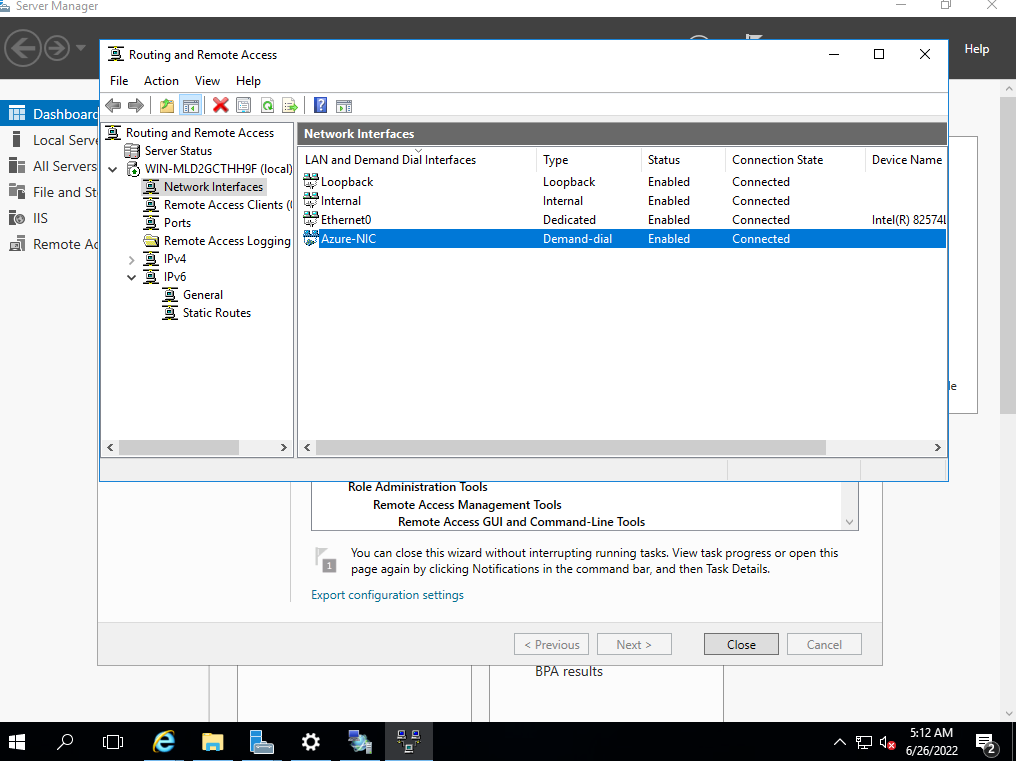


Fig 8: Adding connections

Create the Site-to-Site VPN connection betweenvirtual network gateway and on-premises VPN device.



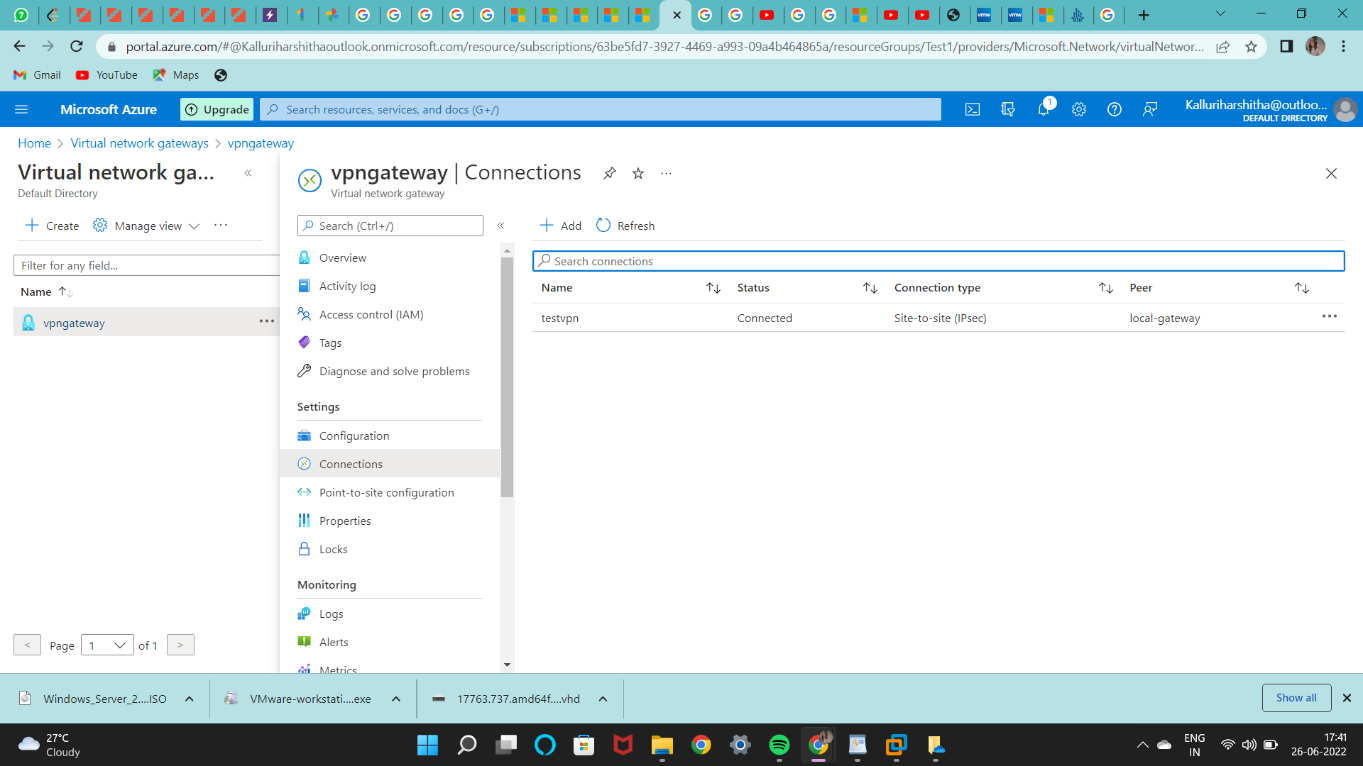


Fig 9: overview or status

**CONCLUSION AND FUTURE ENHANCEMENT**

**Limitations of existing system**

Organizations are stretched while managing a greater number of physical units, and when trying to set up and maintain them, the networking devices and applications in distributed sites, support time needed by organizations are coupled and will be increasing their cost gradually.

“Vnet peering is a mechanism that connects two virtual networks (VNets) in the same region through the Azure backbone network’’. When two virtual networks are peered, they appear as one for connectivity purpose. When two vnet’s are peered through remote gateway, we cannot configure local network gateway.

**Drawbacks:**

* Good security is not seen by vnet peering over internet.
* A single virtual network can have only one gateway. It can either be a local gateway or a remote gateway
* Every Virtual network peer must reside in same region

**PROPOSED SYSTEM:**

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsecVPN tunnel. Once a site-to-site VPN is setup you have IP level connectivity between your premises and virtual networks in Azure. Site to site VPN enables us to build hybrid azure applications.

**ADVANTAGES**

* A Secure connection will be established.
* Usage of too many physical machines can be reduced.
* The S2S VPN is the fastest way to establish a trusted private connection
* Cloud organizations will be able to reduce expenditures and increase productivity.
* Extra investment for physical and hardware infrastructure can be optimized by using Azure cloud computing

**CONCLUSION**

Here, by we conclude that the existing system do not have security,and a single virtual network can have only one gateway.Our proposed system Site-to-Site VPN gateway connection provides IP level connectivity between on premises and virtual networks in Azure. Andreduce expenditures and increase productivity, in azure site to site VPN can have multiple gateways i.e., both local network gateway and virtual network gateway

**REFERENCES**

1. Fundamental of azure by **Michael collier and Robin Shahan 2nd edition**
2. A Comparative Taxonomy and Survey of Public Cloud Infrastructure Vendors [**Dimitrios Sikeridis, Student Member, IEEE ,Ioannis Papapanagiotou, Senior Member, IEEE 2017**]

3. Virtual Networking with Azure for Hybrid Cloud Computing in Aneka **[Adel Nadjaran**

**Toosi, Rajkumar  Buyya 2017**]

4. Implement Virtual Networks by [ **Dan Patrick, Rick Rainey, Michael Washam**

**(4-10-2018)]**

5. VNet Peering in Microsoft Azure [**Rick Donato 2016**]

6.Cloud Computing and WindowsAzure [G**. CARUTASU1, M. A. BOTEZATU1, C.**

**BOTEZATU** Aug 13, 2018]