IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SSVPN (SECURE SESSION VPN) FOR ACCESS ACCOUNTS WITH DOUBLE AUTHENTICATION PROVE

[1]Sarwar Khan Ghaznavi, [2]Mr. Dushyant Sing, [3]Mr. Sitaram Gupta

[1]Research Scholar, [2]Assitant Professor, [3]HOD of CS Department, Vivekananda Global University, Jaipur, India

[1]Department of Computer Science & Engineering,

[1]Vivekananda Global University, Jaipur, India

Abstract: Intranet access has become an essential function for corporate users. At the same time, a corporation's security administrators have little ability to control access to corporate data once it is released to remote clients. At present, no confidentiality or integrity guarantees about the remote access clients are made, so an attacker may have compromised a client process and is now downloading or modifying corporate data. Even though we have corporate-wide access control over remote users, the access control approach is currently insufficient to stop these malicious processes. We have designed and implemented the Session Security VPN network infrastructure that empowers corporations to verify client integrity properties and establish trust upon the client policy enforcement before allowing clients (remote) access to corporate Intranet services. Client integrity is measured using a Routing and Remote Access Services (RRAS), a new security technology that is becoming broadly available on client systems, and our system use these measurements for access policy decisions enforced upon the client's processes. We have implemented Microsoft Operating System along with Domain/Client prototype system that utilizes the RRAS measurement and attestation, existing network control, and existing corporate policy management tools. This prototype illustrates that our solution integrates seamlessly into scalable corporate policy management and introduces only a minor performance overhead.

Index Terms **- VPN, Tunneling, RRAS, SSVPN, Protocols, Domain.**

1. INTRODUCTION

The SSVPN connectivity and securing the session with the double authentication prove. This simulation and prove will be done practically or virtually, but in this scenario, I have already installed the VMWare for simulation as a Client/Domain site. If you want to do it practically in your office or anywhere else, so there is no difference between the simulator that I used in this project and practical work. It is completely the same as it is in any network that you are interested to configure. This authentication proves for the client site and domain site can be done through RRAS (Routing and Remote Access Services). According to network type in, we have used the domain network type for more security and proving the authentication for clients that want to access the public network (Internet) so before beginning the configuration and explaining the scenario we should know about some basic topics that we will discuss it in the below sections.

2. Routing and Remote Access Services

The Remote Access Service is applicable in any computing atmosphere that uses a Wide Area Network (WAN) link or a Virtual Personal Network (VPN). RAS makes it attainable to attach an overseas consumer laptop to a network server over a WAN link or a VPN. The remote laptop then functions on the server's LAN like the remote laptop was connected to the LAN directly. The RAS API allows programmers to access the options of RAS programmatically. Specifies the Routing and Remote Access Server (RRAS) Management Protocol, which allows remote management (configuration and monitoring) of RRAS. The RRAS implementation refers to the elements which will be organized to supply routing, remote access service, and site-to-site property. RRAS is meant to perform well as each router and an overseas access server as a result of it supports a good array of options. For the needs of this preparation, you need solely a little set of those features: support for IKEv2 VPN connections and LAN routing. IKEv2 could be a VPN tunneling protocol delineate in net Engineering Task Force Request for Comments 7296. the first advantage of IKEv2 is that it tolerates interruptions within the underlying network association. as an example, if the association is quickly lost or if a user moves a consumer laptop from one network to a different, IKEv2 mechanically restores the VPN association once the network association is reestablished—all while not user intervention. The aim of VPN is to provide secure communication by creating tunnels virtually between two host that want to communicate between each other in a VPN network, when the tunnel created, after that data moving

or transferring can take place [1]. Configure the RRAS server to support IKEv2 connections whereas disabling unused protocols, that reduces the server's security footprint. to boot, tack together the server to assign addresses to VPN shoppers from a static address pool. you'll feasibly assign addresses from either a pool or a DHCP server; but, employing a DHCP server adds quality to the look and delivers stripped-down edges. An IPSec is the good option for the secure remote access [2].

3. Workgroup Network (Peer to Peer)

The workgroup could be a peer-to-peer Windows network, wherever users will use their login credentials solely on his or her system and not others. It holds a distributed administration whereby every user will manage his machine severally. Most storage is distributed. every device has its dedicated storage.

In a workgroup: All pcs area unit peers; no pc has management over another computer

- Each pc encompasses a set of user accounts. To use any pc within the workgroup, you need to have an associate account on its pc.
- There is a unit usually no over 10 to twenty computers.
- All computers should air an equivalent native network or subnet.

A workgroup mainly implements a peer-to-peer networking model, where each computer is autonomous having its user account and permissions, memory, and are equally important. Also, these computers are not so secure. They have local security, i.e., each device maintains its security. It may also happen that one computer in the workgroup may not have access permissions to all the computers in that particular workgroup. Every computer has to maintain its user accounts and access permissions.

4. Domain Network

The domain could be a client/server network wherever users will login from any device of the workplace. conjointly called Remote login. it's a centralized administration and every one device will be managed from a centralized device. It prefers centralized storage and every one of the user's knowledge is hold on at a centralized device which might be NAS or SAN.

In a domain:

- One or additional computer area unit servers.
- Network directors use servers to regulate the protection and permissions for all computers on the domain.
- This makes it simple to create changes as a result of the changes area unit mechanically created to any or all computers.

If you've got a user account on the domain, you'll be able to go online to associate pc on the domain with no need for an account on it pc. There will be lots of or thousands of computers. The computers will be on totally different native networks.

Due to the rise security and flexibility in an exceedingly domain atmosphere Techtronic perpetually recommends implementing a website atmosphere for our purchasers

5. Propose Work

Before set up the propose connection we should have the scenario and the diagram of our connection that we want to configure and install the VPN and set up our network. in us propose network connection.

Scenario: in this scenario for the purpose network connection for the SSVPN is to connect two site which is located remote from each other. They want to have connection between each other, as we know they can connect it without VPN configuration as well, but the main point is the security of the users which want to connect between each other, here we want to secure their session which the new and advance encrypting technique which is not possible in the existing (simple connectivity between users) network connectivity. The main aim of IPSec is to secure the Internet Protocol (IP) by authenticating and encrypting IP packet of a data stream. Inside IPSec there is some protocol working for establishing the session and negotiation of cryptographic keys to be used during the session [3].

Suppose here we have two branches, Branch A and Branch B, each of them has its own user and domain, our task is to connect them through VPN connection securely with double authentication prove, it means one authentication is done in VPN configuration and the second authentication can be done in the domain site. The domain site specifies the user's validation, using username and password.

In the propose topology which is shown in Fig 1, Branch A and Branch B is connected over ISP (Internet Service Provider) with public Internet Protocol (IP). Each Branch has its own domain; the domain is from Microsoft vendor. Before starting the set up the SSVPN connection we should have already done the following configuration for the domain Branch A and Domain Branch B.

1. Server Operating system
2. Server machine (PC with advance technology)
3. DNS (Domain Name System)
4. Active Directory
5. DHCP (Optional)
6. Two Interface (one for public IP and second for Private IP)

After configuring these setting, we should go through the VPN configuration which is included in RRAS role. This configuration is necessary for both side of the branches and the client can just set up the VPN connection using the specified username and password for establishing connectivity.

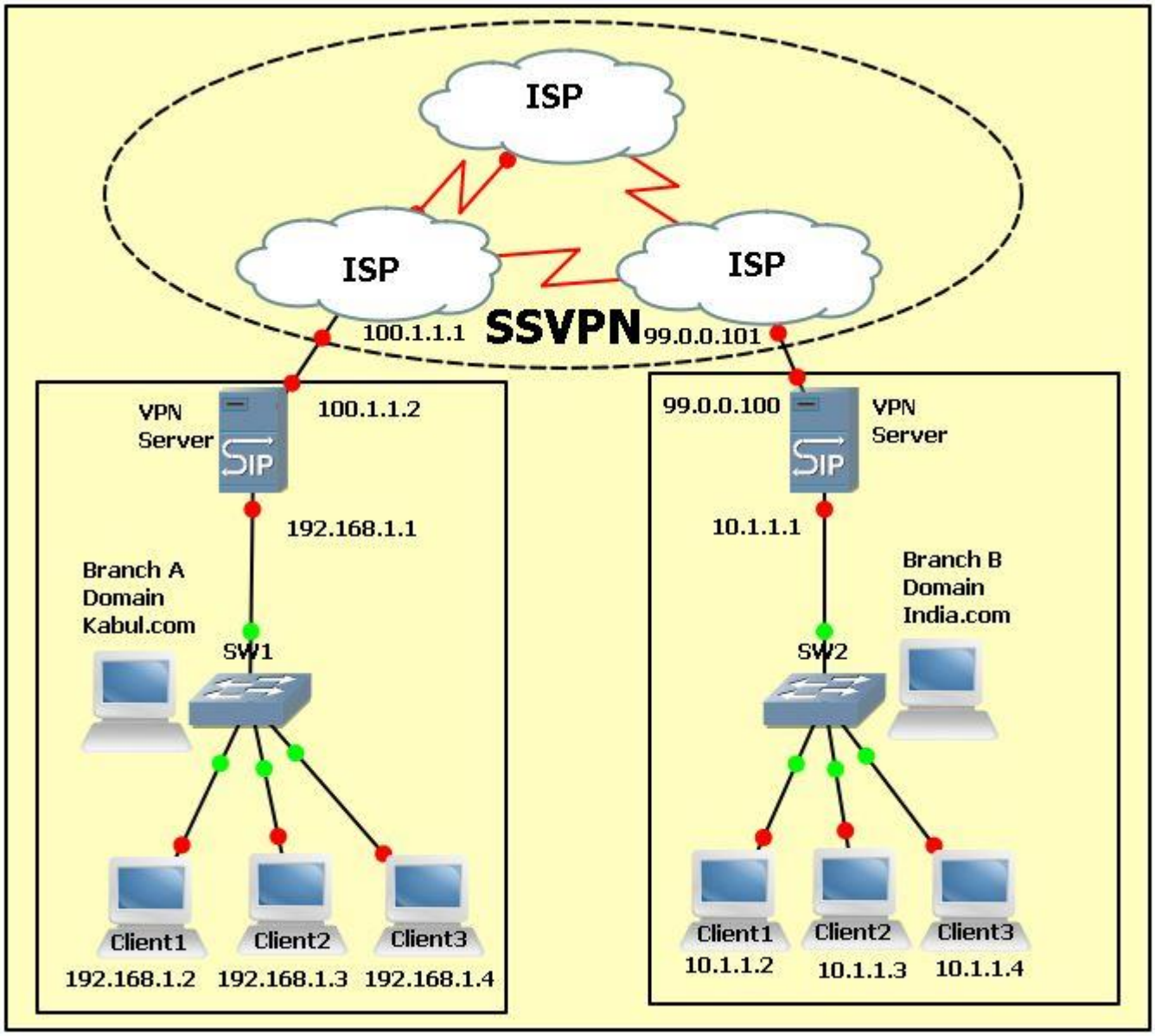

Figure 1: propose Topology for Site-to-Site SSVPN

5.1 Branch A (Kabul.com) Configuration

This branch has already done the requirement to configure the domain and installed the RRAS role to configure the VPN. In the first step, assign the IP for the both side of the interface as shown in the Figure 1.

After that open the RRAS role using shortcut in "Run" (winkey+R) and write *"rrasmgmt.msc"*. The RRAS page will open as shown in the Figure 2.

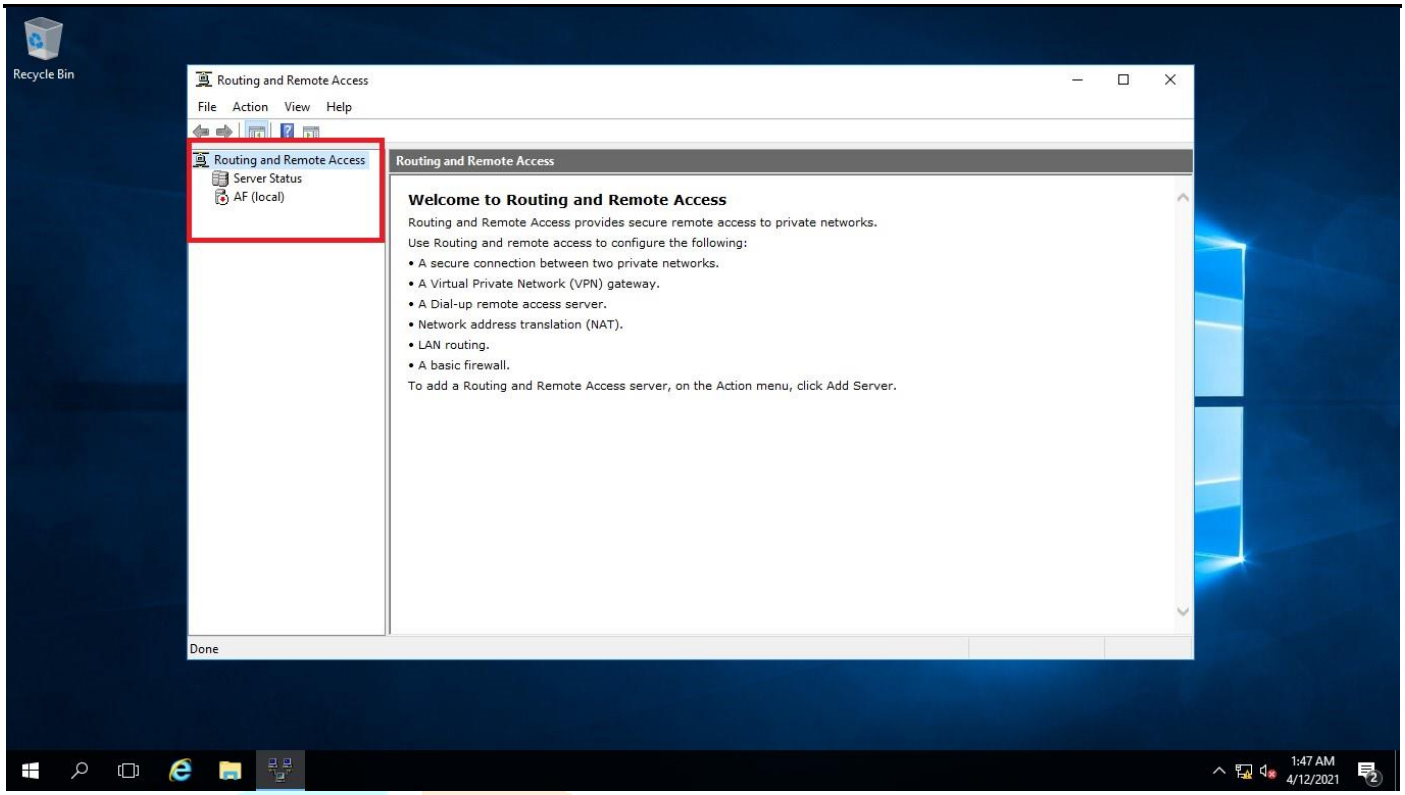

Figure 2:RRAS Interface in Microsoft Server 2016

This page that is shown in the Figure 2, shows that the initial step of RRAS configuration for the VPN. To configure VPN, just right click on the "AF (local)" and select the "Configure and enable Routing and Remote Access". In the next step you will see a list of services to be configured in this server. As show in the Figure 3. Here we select the "Virtual Private Network (VPN) access and NAT" --→ Click on "NEXT" to configure our VPN between one branch and another branch (site-to-site). The next step will show us the interfaces which is connected to the VPN server, as we know the VPN server has two interfaces, one is for the external (connect to the Internet) and the second one is Internal (connect to the Local Area Network).

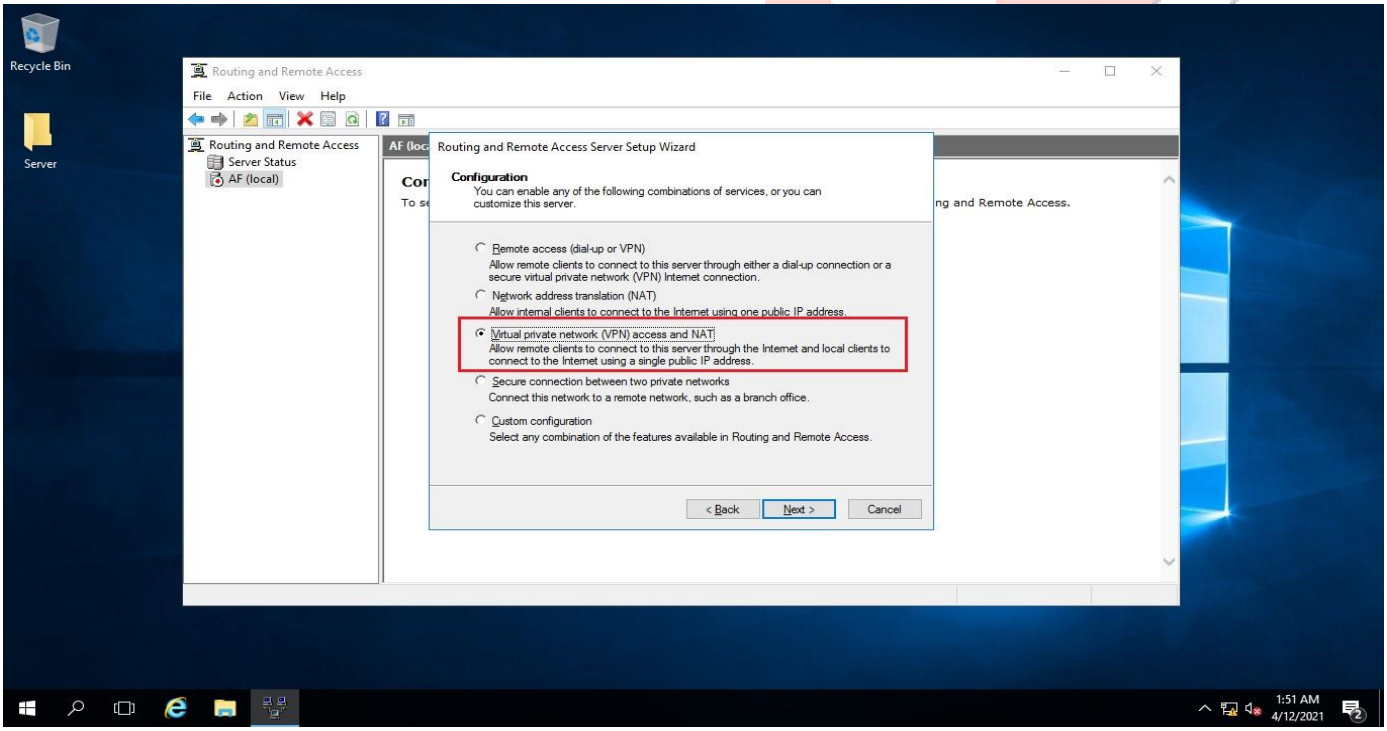

Figure 3: VPN Services Selection

For the VPN configuration select your external port which is connected to Internet and click on the "NEXT" button. Here will show you the connection for the remote access of VPN created but with zero connection (no connection establish yet). As shown in the Figure 4.

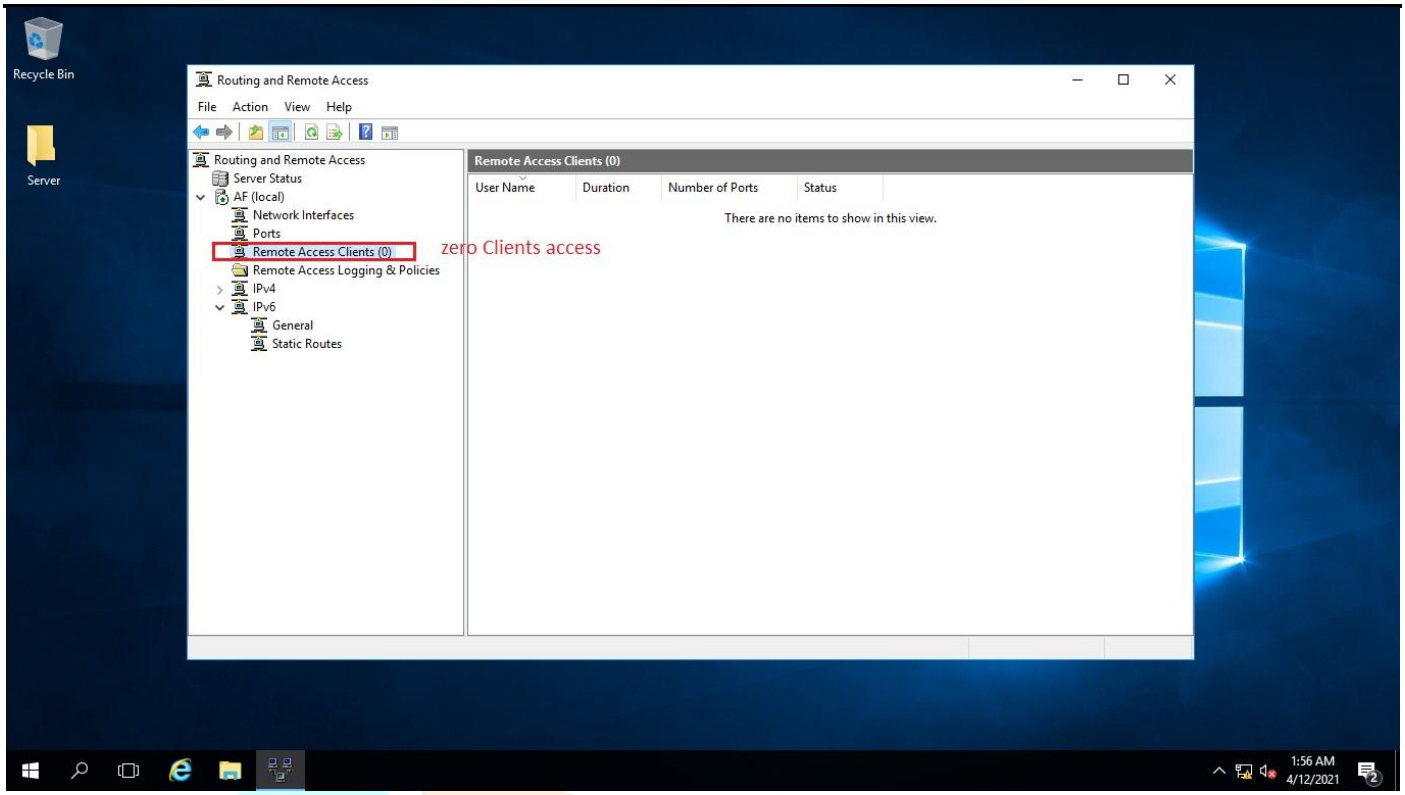

Figure 4: The Remote Access Client interface created with zero connection

The Kabul branch Remote access is being created without any connection, it will shows connected while the India branch configure the VPN connection and one of the client establish connection toward Kabul branch VPN server.
The next step is Right Click on "*Network Interface"* and select *"New Diamond-dial Interface"* to specify the source and destination network along with their encryption protocols. Shown in Figure 5.

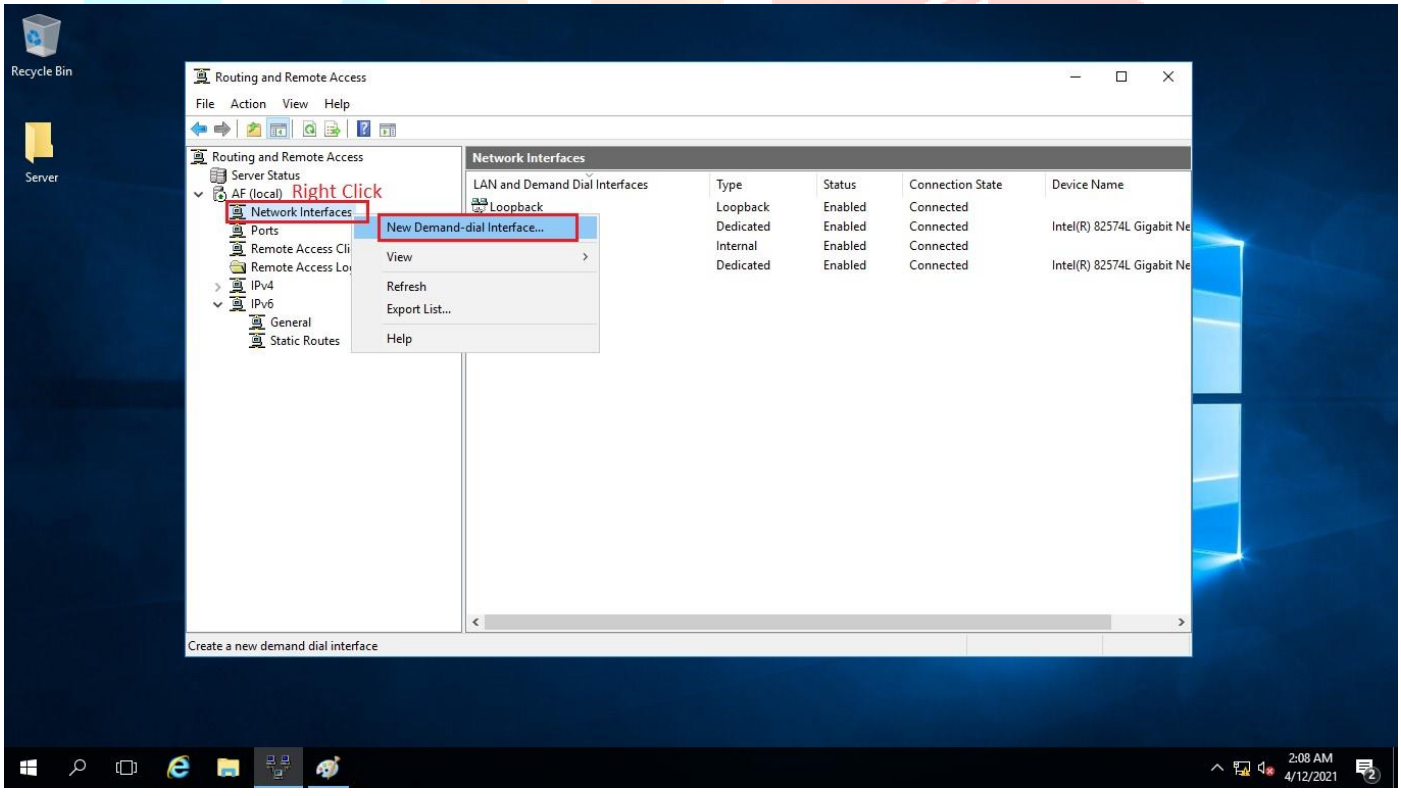

Figure 5: establish VPN network Connection

The next step will appear to write the *"Interface Name",* it may be any name but remember that, as same name a user will create for the client to connect while using VPN connection for the authentication to the VPN server. Then Click on "*NEXT"* to select the VPN types, as shown in Figure 6.

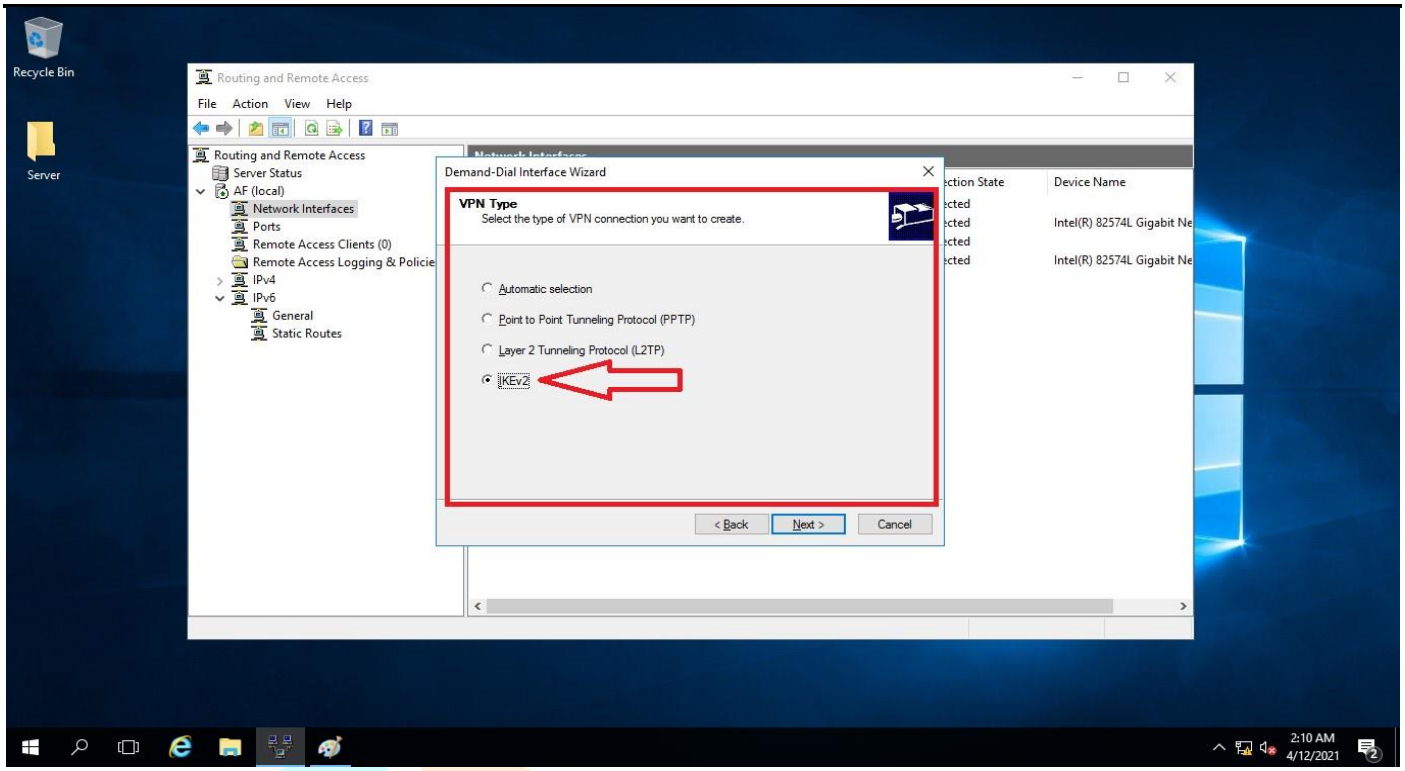

Figure 6: Selecting the VPN type for encryption

This is the important part to select the IKev2 VPN types. This VPN types is not supported in the simple or exiting VPN connection that is discussed in Chapter 3. The more details and advantage about the IKev2 VPN types will discuss in Chapter 5 in more details. To go one step more just click on the *"NEXT"* button that is shown in Figure 6.

The next step for the configuring VPN connection is to specify the public IP and Private IP of the both side should be clarifying to each other, it means in Kabul branch we write the public IP and Private IP of the India.com server and in the India.com should write the public and Private IP of the Kabul.com VPN server. Currently we want to configure the Kabul.com branch so we should write the India.com public IP (99.0.0.100) and also route the private IP that is shown in Figure 7.

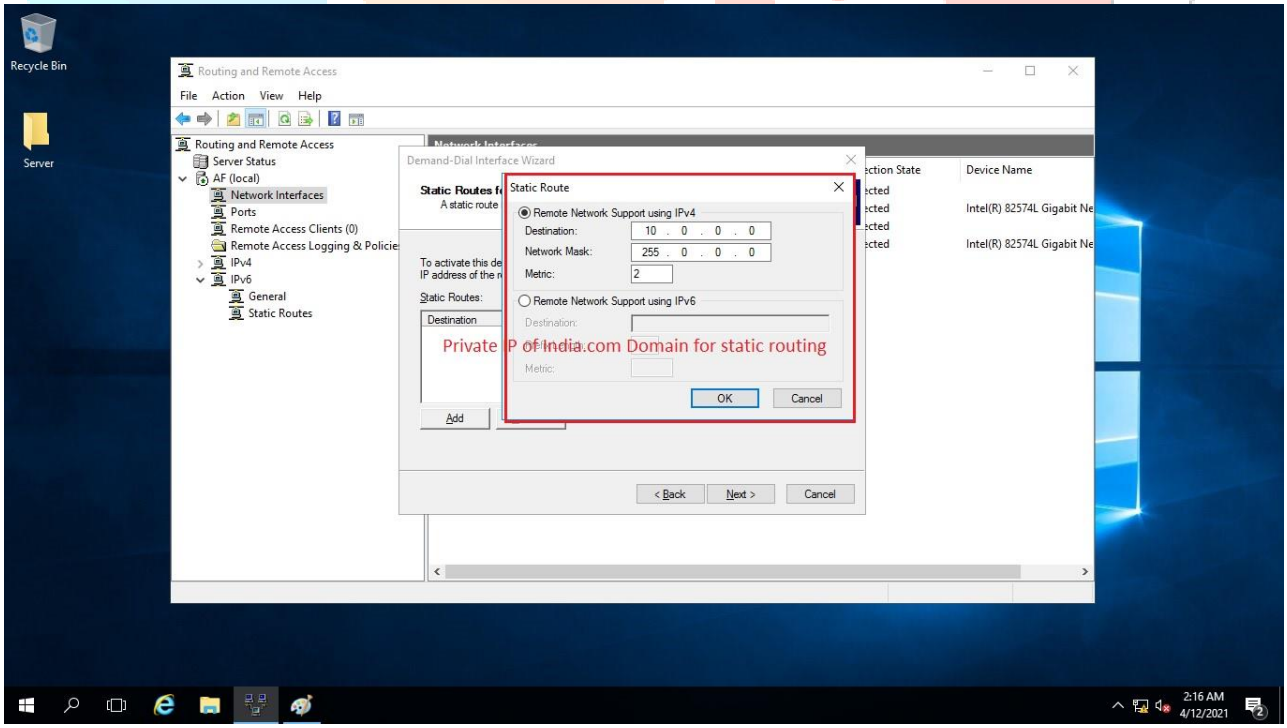

Figure 7: Static Route toward India.com Domain

The private IP of India.com should be routed for the communication of the Kabul.com Clients and the metric specify number of routers which they want to pass. The metric is also kind of security for the network connection. Next step a password should be clarify for users from the India VPN server want to connect to the Kabul.com domain.as shown in Figure 8.

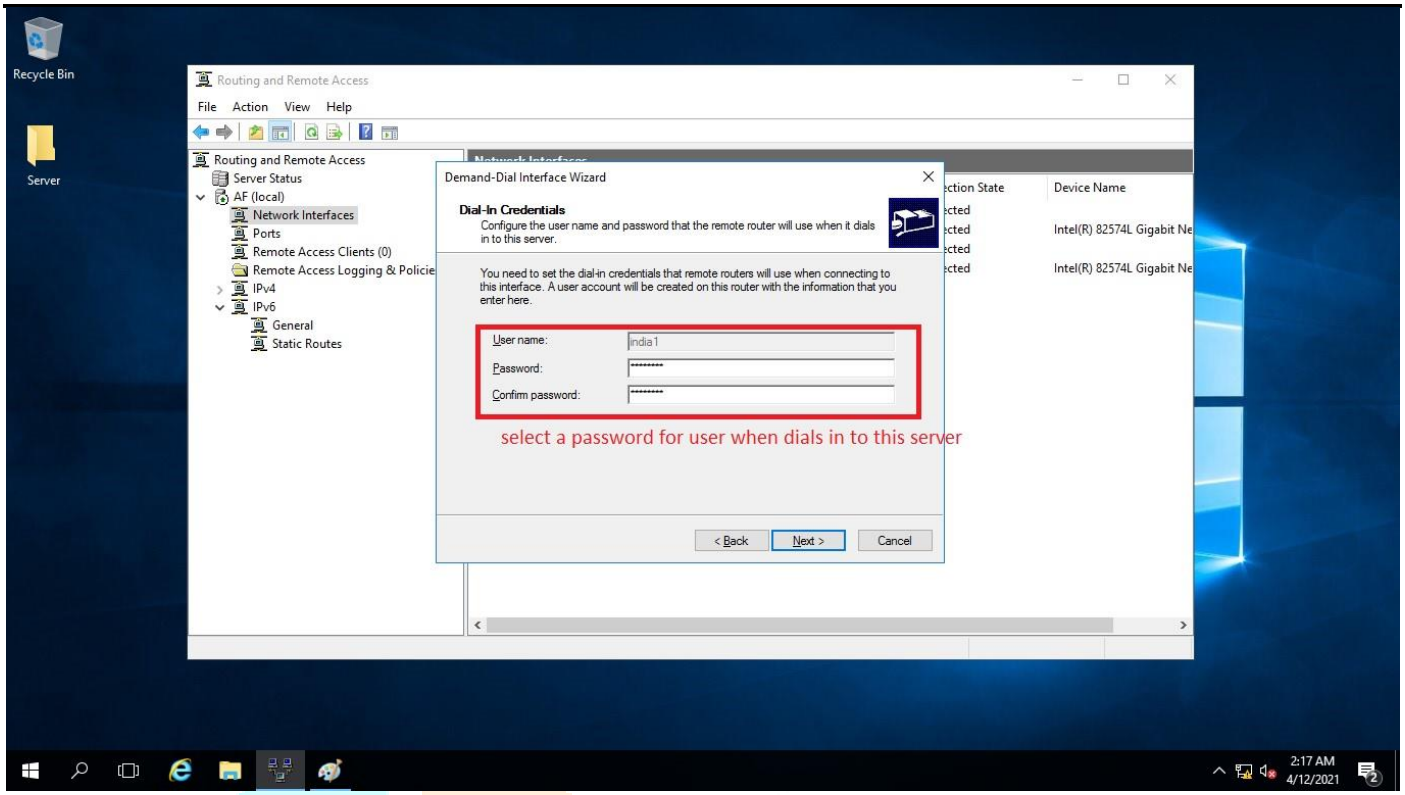

Figure 8: Username and Password for the Inida1 user

In the next step the credential is needed to confirm yourself, the username, Domain, Password, reconfirm the password is need to specify that the valid user want to create the VPN connection. As shown in Figure 9.

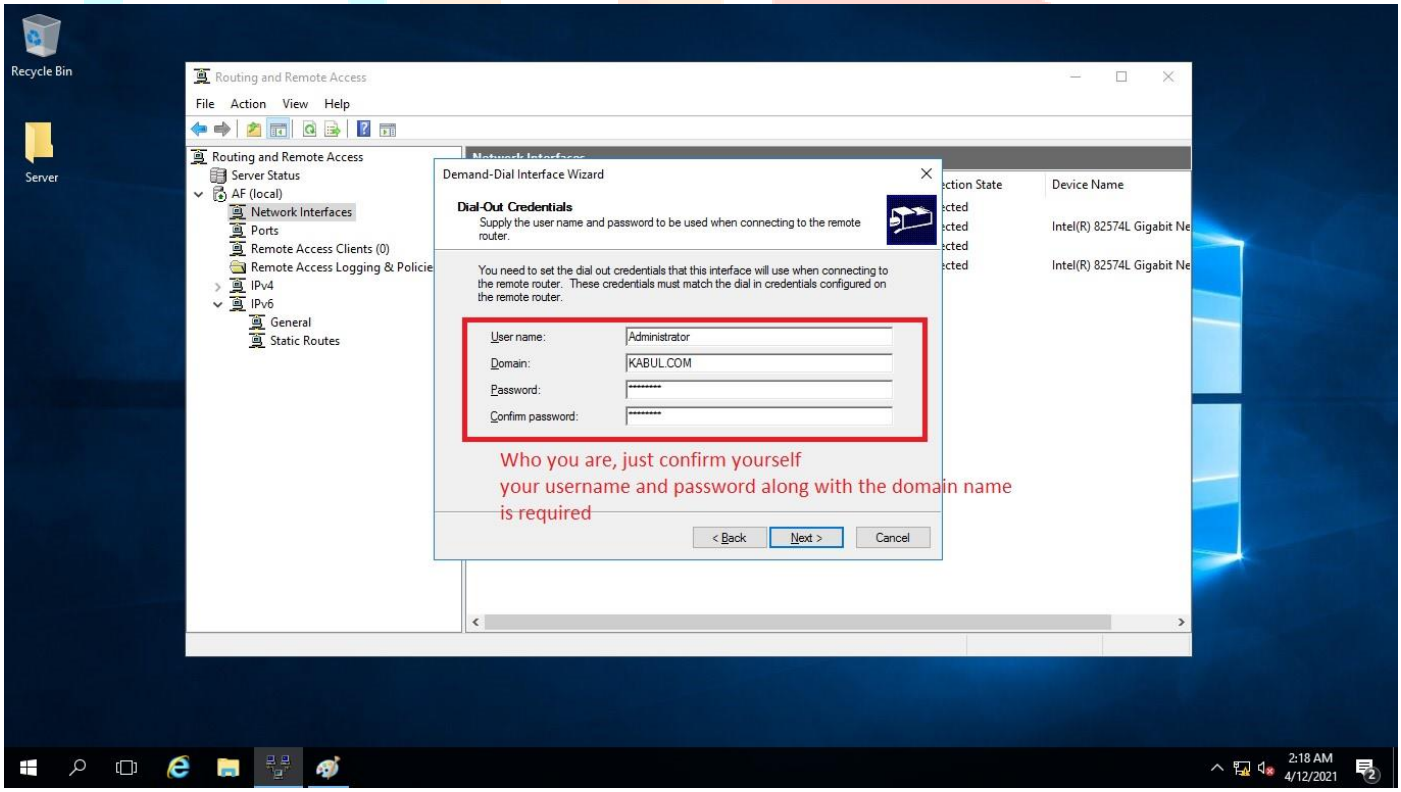

Figure 9: Credential step for the Valid user

Client Connectivity to India VPN server: the client1 in Kabul.com which has Microsoft windows 7 Operating System want to connect to India VPN server and access to the user's Remote access. Just click on the "*Network and sharing center"* and click on "*Set up a New Connection"* and select the "*Use my Internet Connection VPN" as* shown in Figure 10.

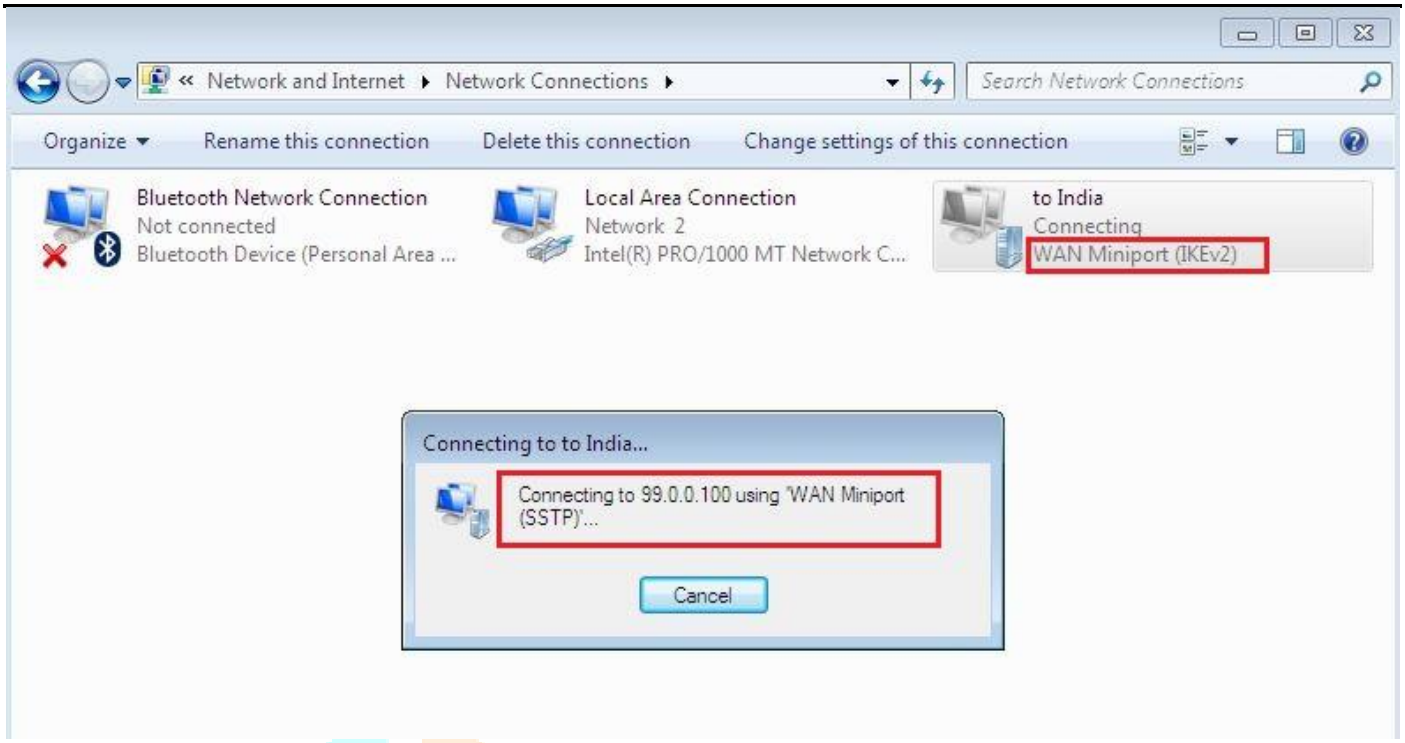

Figure 10: Creating Tunnel between user and VPN server

in the Figure 10 shows that the VPN is connecting to the Public of India VPN server 99.0.0.100 and the Secure Socket Tunneling Protocol is use to create tunnel between the Kabul branch and India branch. The SSTP is commonly use to form a Virtual Private Network tunnel that provides a mechanism to transport PPTP, L2TP and IKev2 traffic through an SSL/TLS provide transport-level security with key negotiation.

After forming the tunnel, the user should authenticate with the VPN server (username and password). If the username and password is correct then authenticate with the domain that whether this account is registered in domain or not. As shown in Fig 11,12.

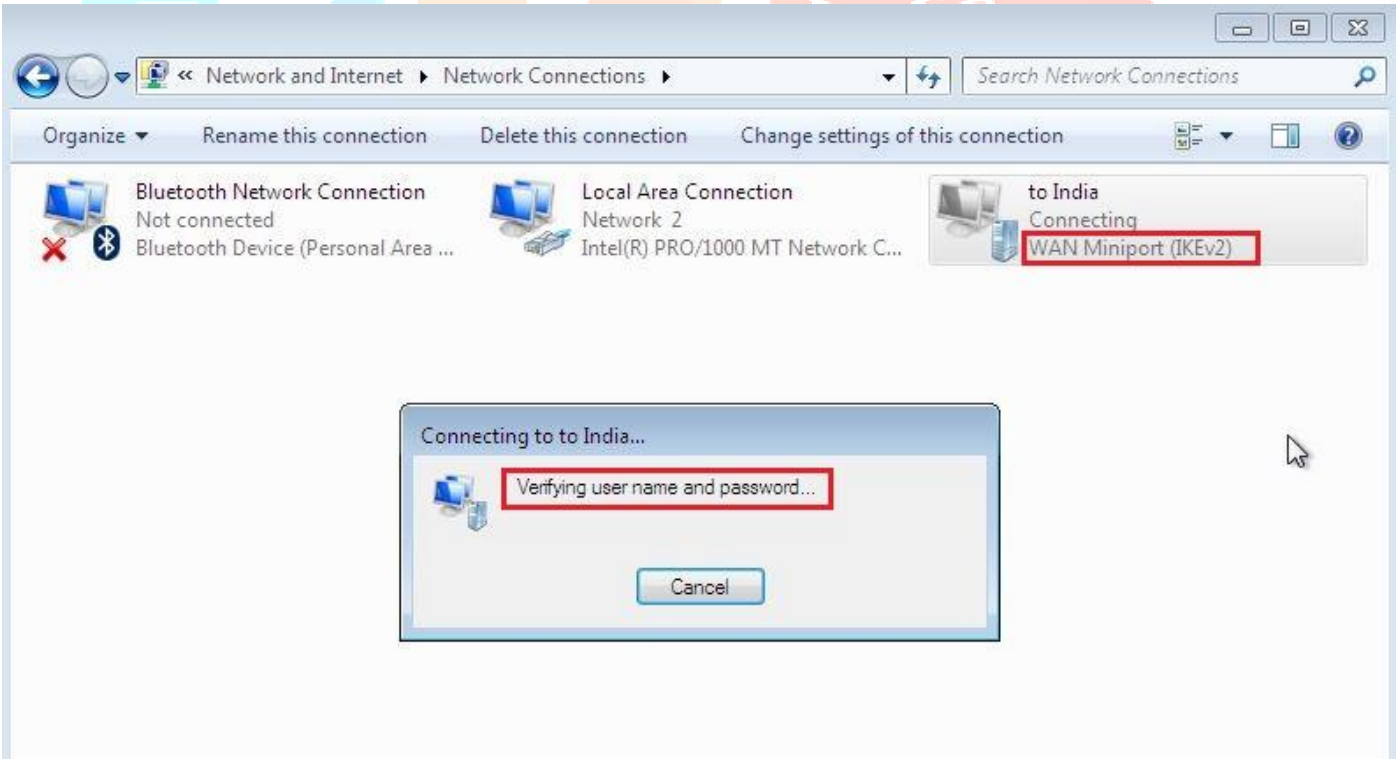

Figure 11: Authentication with the VPN server

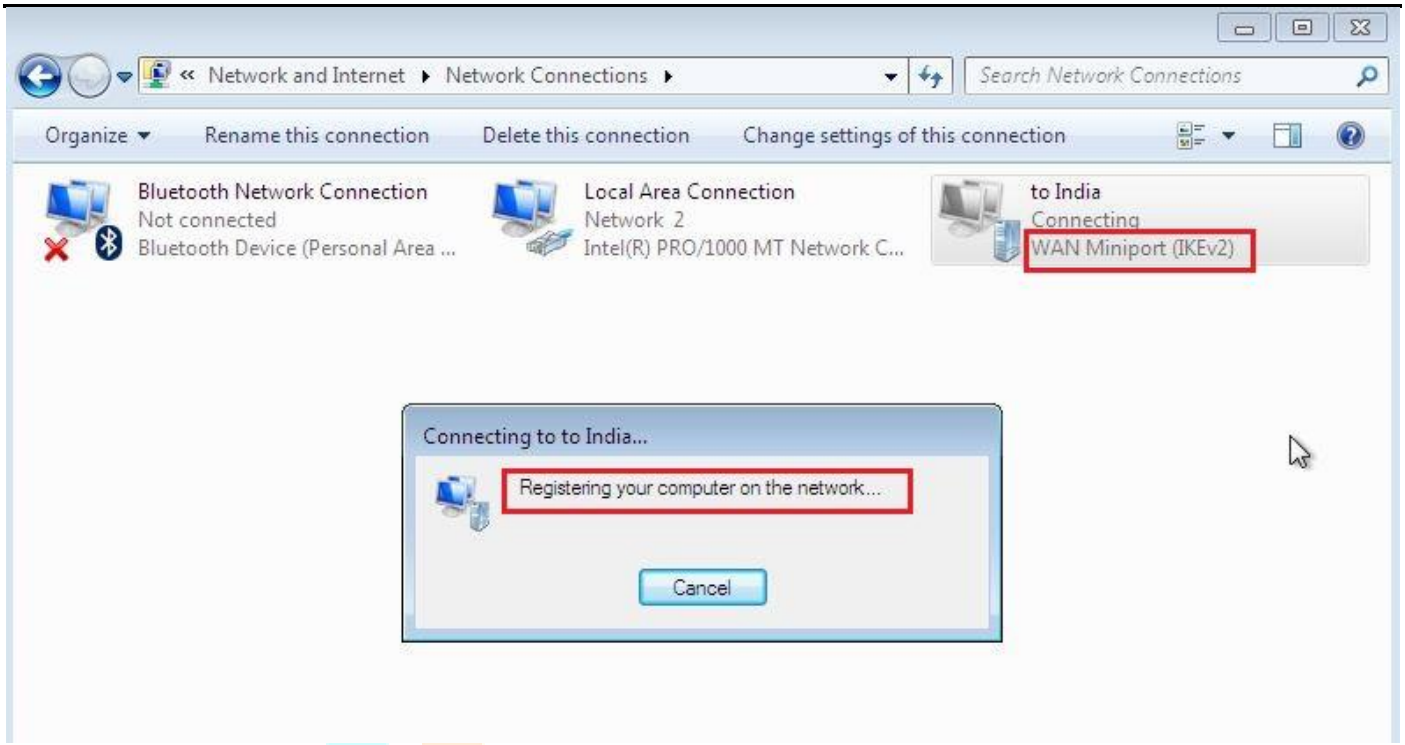

Figure 12: Authentication with the Domain for Registering

6. RESULTS AND DISCUSSION

Virtual Private Network (VPN) is commonly use for the security reason in public and private network. currently the usage of the VPN is increasing day by day, due to the free services and providing good security method for the users. VPN use tunneling mechanism between source to destination for the transferring the packet and their tunneling protocol which is use to secure our data is getting advance nowadays. The network administrators use VPN for various purposes, such as Remote Access VPN, Site-to-Site VPN and PC to PC VPN in their network. as we analyze, draw and configure the existing VPN configuration between hosts and realize some vulnerabilities, weak encryption tunneling protocol in a public network is risky and it is an easy way for the attacker to fetch their data. For the prove of the existing VPN communication and authentication technique. In these Figures shows when the existing system want to connect with the destination host, there is not any authentication or registering to the VPN. And the highest tunneling protocol is L2TP and PPTP. In the existing VPN connectivity, the IKev2 tunneling protocol is not possible to configure. It needs a special VPN server to support the all functionalities and feature for the IKev2.

With compare to the existing VPN connection and propose SSVPN, we have found some good functionalities that is not possible in the existing VPN. The SSVPN is the combination of VPN server and Domain registering mechanism that use to provide more security for the host that want to connect through it with double authentication prove. While configuring the SSVPN in Chapter 4, we prove that, the first authentication is happened with VPN server and the second authentication goes to Domain to check the valid username and password (Figure 11 and 12). And the IKev2 support by the VPN server (Fig 10). As we know the IKev2 protocol is become more popular over the last few years and it also support the IPsec latest encryption algorithm. It consumes less bandwidth compare to L2TP and PPTP. currently The IKev2 is one of the speediest VPN and has stable and consistent connection.

7. Compare the Existing and Propose VPN Connection

Table 1: Existing and Propose Connectivity

No	Description	Existing System	Propose System	Positive Affect
1.	Easy to Configure	YES	NO	0
2.	High Security	NO	YES	1
3.	Support L2TP	YES	YES	1
4.	Support PPTP	YES	YES	1
5.	Support IKv2	NO	YES	1
6.	Multiple User Connection	NO	YES	1
7.	Double Authentication	NO	YES	1
8.	compatibility between vendors.	NO	YES	1
9.	Support EAP Authentication	NO	YES	1
10.	Mobility and Multi-homing Protocol (MOBIKE)	NO	YES	1
11.	Asymmetric authentication	NO	YES	1
12.	supported on many platforms	YES	NO	0
13.	Open source Implementation	YES	NO	0
14.	Fast establishing	NO	YES	1

Conclusion

Utilizing VPN leads to a major increase in network secure session security. This is, however, a tiny low value to obtain the safety and privacy offered by a virtual non-public network. VPN is that the handiest and versatile kind of secure communication across long distances. additional information measure is needed to handle the extra network load. A VPN could need a component upgrade or maybe further hardware. If network resources don't seem to be developed and distended to satisfy the new VPN needs; companies could expertise slower response times in e-mail, file delivery, and information inquires. vital delay is additionally intercalary to e-mail and FTP transactions. leased lines and frame relay networks were the first big-ticket answer for personal networks. Their higher expenses and bigger hardware needs cause the unfold of VPN technology. As we analyze, explain and configure and existing VPN server configuration in Microsoft using site-to-site VPN connection vs the propose VPN connection we found that that vulnerabilities that include in the existing VPN connection, vanish in the propose connection so the secure of the session with double authentication prove that is discussed in the previous chapter has been tested and the result was positive about our scope or area in SSVPN. In Future it is possible to extend the VPN session security using the different technique for the encryption methods and its tunneling protocol.

REFERENCES

[1] Robin Kr Gupta, Virtual Private Network, School of Computer Science and Engineering, International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211, Volume 9, Issue 5, May 2017

[2] Elena lanos – Schiller, Defta (Ciobanu) Costinela – Luminita, Virtual Private Network and its Protocols, ISSN 12-234, 2018, 3-4

[3] Oluwatomisin Oluwafemi Opemipo Abiodun, Implementation of Internet Protocol Security (IPSec) on a Site to Site Virtual Private Network (VPN), Department of Computing, University of Northampton, England, United Kingdom

[4] K. Karuna Jyothi, Dr. B. Indira Reddy, Study on Virtual Private Network (VPN), VPN's Protocols and Security, IT Department, Sreenidhi Institute of Science and Technology, Ghatkesar, Telangana, India, 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN: 2456-3307

[5] Diyar Salah Fadhil,Ababakr Ibrahim Rasuland YounusAmeenMuhammed, IPSec on a Site to Site VPN Network, Faculty of Science, Soran University, Kurdistan Region, Iraq, I S S N 2319 – 1236