CHAPTER - 1

INTRODUCTION

In very simple terms, a VPN connects your PC, smartphone, or tablet to another computer (called a server) somewhere on the internet, and allows you to browse the internet using that computer's internet connection. So if that server is in a different country, it will appear as if you are coming from that country, and you can potentially access things that you couldn't normally.

A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more.

These days VPNs are really popular, but not for the reasons they were originally created. They originally were just a way to connect business networks together securely over the internet or allow you to access a business network from home.

VPNs essentially forward all your network traffic to the network, which is where the benefits – like accessing local network resources remotely and bypassing Internet censorship – all come from. Most operating systems have integrated VPN support.

Using VPN we are providing the facility of data transferring over web.

CHAPTER - 2

PRE-REQUISITES

2.1 Windows Server 2012 r2 Installed

We installed and configured a VPN Server using Windows Server 2012 R2. Managing a VPN server running Windows Server 2012 R2 is no different than any other Windows Server. Windows system management is mature and well understood, and the server can be maintained using existing platforms, tools and procedures. A Windows Server 2012 R2 based VPN Server costs significantly less than it does to deploy dedicated and proprietary VPN hardware. The Server van be deployed in existing virtual infrastructure and has no per-user licensing requirements.

2.2 Platform Used:

VMWare Workstation 14 pro
Version: 14.1.3 build-9474260

We've used VMWare workstation 14 pro to perform the Virtual Private Network. VMware Workstation Pro enables technical professionals to develop, test, demonstrate, and deploy software by running multiple x86-based Windows, Linux, and other operating systems simultaneously on the same PC.

You can replicate server, desktop, and tablet environments in a virtual machine and allocate multiple processor cores, gigabytes of main memory and graphics memory to each virtual machine, whether the virtual machine resides on a personal PC or on a private enterprise cloud.

Some additional pre-requisites are:

- The Active Directory on Windows Server 2012.
- DHCP Configuration on Windows Server 2012 R2.

- DNS Server On Windows Sever 2012 R2
- Configure and enable Routing and Remote Access

- Configure Remote Access permissions for an AD group
- Launch NPS
- Implement IIS Server8.5
- Implement FTP

2.3 Minimum System Configuration:

The figures below are commended minimum for the default installation and most applications will benefit from more than the minimum resources.

Processor: An Intel processor

RAM: 8 GB

Free Space: 100 GB

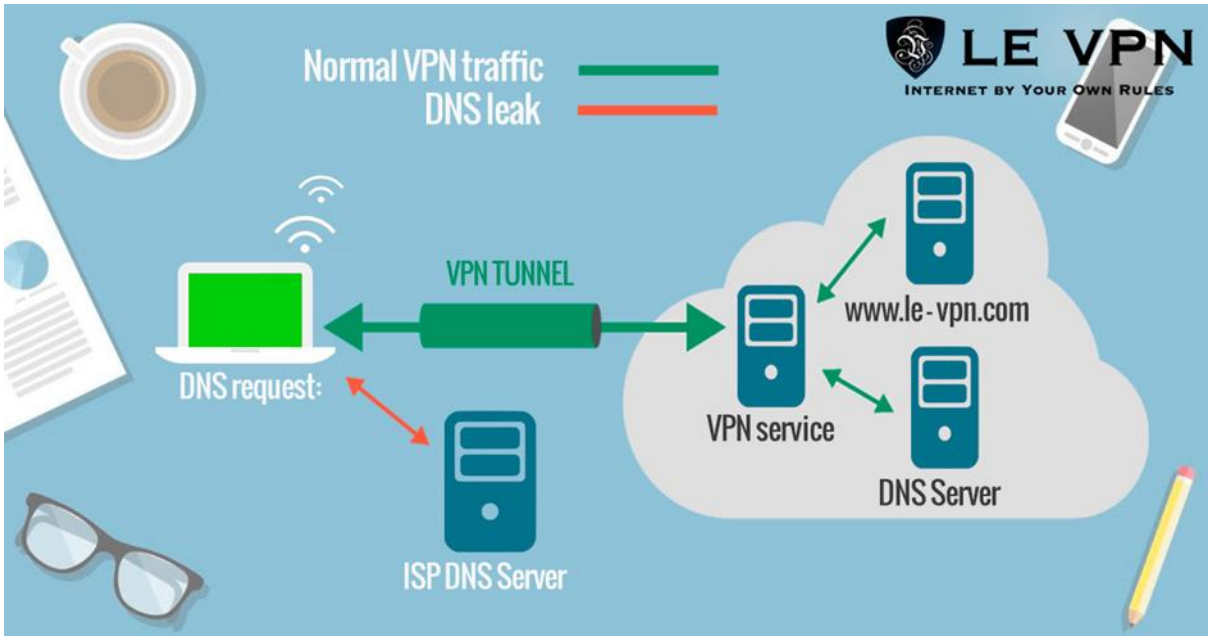
CHAPTER-3

Overview of VPN

A Virtual Private Network (VPN) is a network that uses the Internet or other network service as its Wide Area Network (WAN) backbone. In a VPN, dial-up connections to remote users and leased line or Frame Relay connections to remote sites are replaced by local connections to an Internet service provider (ISP) or other service provider's point of presence (POP). A VPN allows a private intranet to be securely extended across the Internet or other network service, facilitating secure e-commerce and extranet connections with business partners, suppliers and customers. There are three main types of VPN:

- Intranet VPNs allow private networks to be extended across the Internet or other public network service in a secure way. Intranet VPNs are sometimes referred to as site-to-site or LAN-to-LAN VPNs.
- Remote access VPNs allow individual dial-up users to connect to a central site across the Internet or other public network service in a secure way. Remote access VPNs are sometimes referred to as dial VPNs.
- Extranet VPNs allow secure connections with business partners, suppliers and customers for the purpose of e-commerce. Extranet VPNs are an extension of intranet VPNs with the addition of firewalls to protect the internal network.

.



VPNs maintain the same security and management policies as a private network. They are the most cost effective method of establishing a virtual point-to-point connection between remote users and an enterprise customer's network. This technology enables a user to discard the changes done to the operating system, allowing it to boot from a known state.

A VPN provides a means by which remote computers communicate securely across a public WAN such as the Internet.

A VPN connection can link two LANs (site-to-site VPN) or a remote dial-up user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that make up the public WAN. To secure VPN communication while passing through the WAN, the two participants create an IP Security (IPsec) tunnel.

3.1 Benefits of VPN:

The VPN (Virtual Private Network) technology came as an answer to individuals' request to protect their online activities and to maintain their online confidentiality.

Besides this functionality, the technology helps internet users access restricted content from anywhere in the world, with just a click of a mouse.

Therefore, we can say that a VPN is a secure solution that allows its users to send and receive data via the internet while maintaining the privacy and confidentiality of their data, based on its encryption level. The cherry on top is that a VPN will unblock the internet, by providing you the most-wanted Internet freedom that you deserve.

It's obvious that because of people's security need and especially because of the need for sending encrypted data over a network, the VPN technology has been developed. But beside the role of creating a "private scope of computer communications," VPN technology has many other benefits:

- Enhanced security
- Remote control
- Share files.
- Online anonymity
- Unblock websites & bypass filters.
- Change IP address.
- Better performance.
- Reduce costs.

3.2 Risk & Limitation of VPN:

Many users find the benefits outweigh the costs of Virtual Private Networks, however there are a few disadvantages inherent to VPNs include security, performance and complexity. Organisations should objectively consider these limitations and take them into account, as they can translate into hidden costs.

The limitations of a VPN service

At first glance, there appear to be many business advantages to running VPNs – business mobility, scalability and a reduction in telecommunication costs. The following article compares traditional Virtual Private Network technologies with newer Private MPLS networks (known as Secure Private Networks).

VPN and security

VPNs are flexible; companies are able to connect many locations, both locally and overseas using this technology. However, if the VPN is not configured and managed correctly, serious security issues can arise. Despite the popularity of VPNs, there are security risks if stringent procedures are not followed. Based on the fact that security is a major concern for businesses, this implies significant risks.

Tips for securing your VPN include:

- Using secure authentication methods with strong passwords. Passwords should be longer than eight characters and containing a mixture of upper case and lower case letters, as well as numbers.
- Change your passwords on a regular basis; at least every two months. System administrators should be able to set passwords to expire after a certain period.
- Use a minimum of 256-bit encryption or as strong a type of the Advanced Encryption Standard as your internet speed will allow. The higher the encryption, the longer the time required for that type of encryption to complete.

Exposure risks with VPNs

By utilising the public internet and using it to form a private tunnel, VPNs are vulnerable to security breaches, performance degradation and network failures. In contrast, Private MPLS networks protect against online and external threats as traffic is independent of the internet and utilises the service provider's own network, which is entirely segregated for your business' exclusive use. Your business data will never traverse the internet.

VPN reliability & availability

A significant disadvantage, especially for large businesses, is that the reliability of an organisation's VPN is outside their direct control due to the fact it uses the internet. In contrast, Secure Private Networks (SPN) provide guaranteed performance and availability for business-critical operations. In addition, a SPN also provides the advantages of centralised control; therefore an MPLS (Multiprotocol Label Switching) based private IP network dramatically reduces complexity and removes the need for additional skilled engineers.

VPN and performance:

In contrast to traditional Private Networks, VPNs are only as fast as the slowest internet connection between two end-points. Unpredictable internet performance creates disruption and inconvenience. Moreover, with the increasing use of real-time and interactive applications, network performance issues with VPNs become much more noticeable.

Complexity and incompatibility

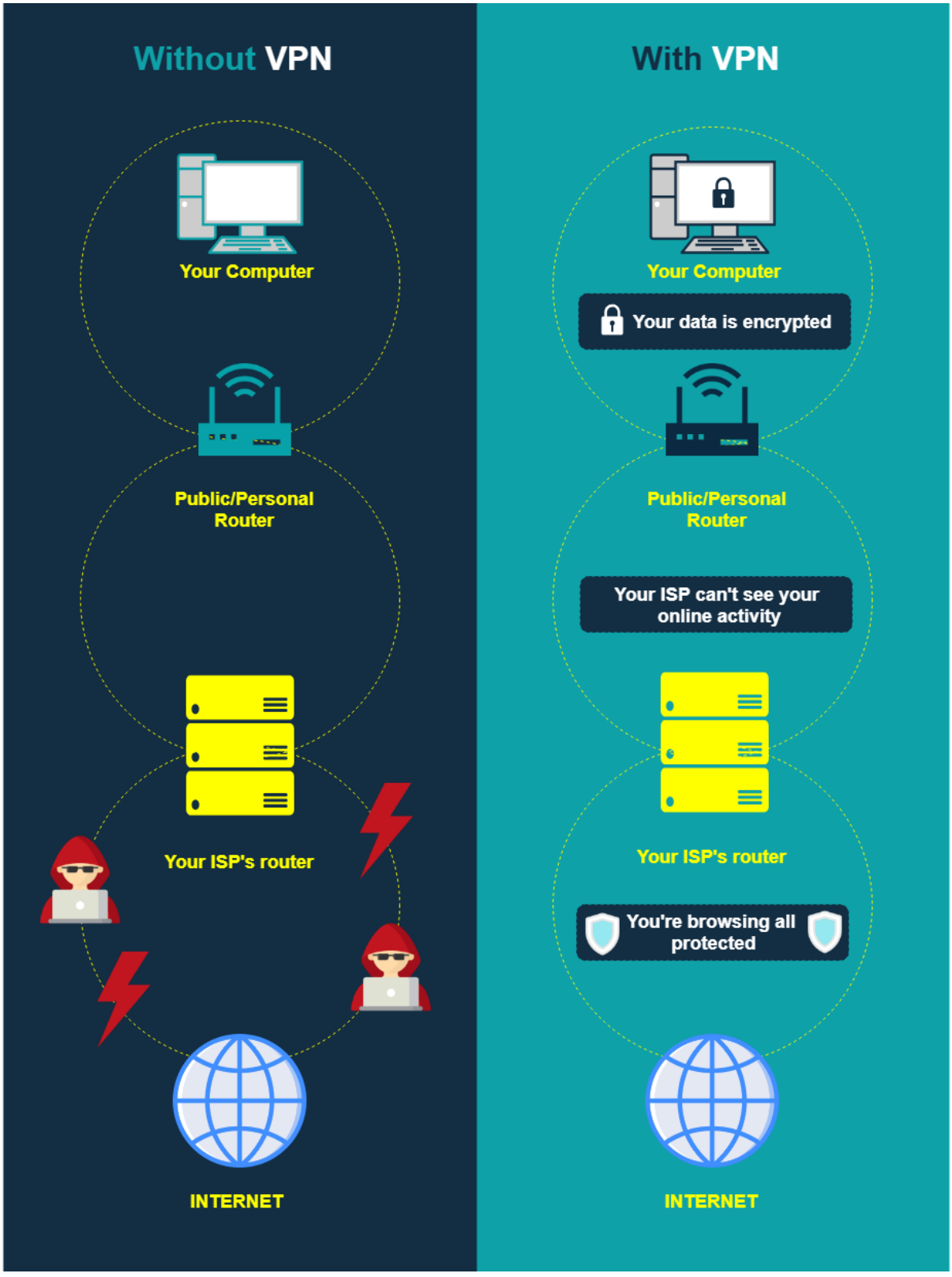
VPNs work using equipment from many different manufacturers, which all too often work poorly together. The incompatibility of equipment from different vendors can have the effect of making things more complex. Your business may need to employ additional network engineers to configure and administrate these devices, all of which may make the VPN solution more costly to implement and maintain.

VPN Quality of Service (QoS)

VPNs do not offer complete guarantees. In addition, packet loss is variable and can be very high. Unlike VPNs, MPLS-based Secure Private Networks provide solutions to these problems, with much greater redundancy and scalability.

As the curiosity and demand for private network solutions has increased, concerns have been raised over the limitations of VPN-based solutions. With the evolution of Private MPLS networks over the past decade, the availability and associated costs have reduced the original appeal of VPNs.

As outlined above, a Private MPLS solution will provide better performance, enhanced reliability and the ability to run QoS over the network. Unless you require the ability to connect to your company's LAN while travelling internationally, or you view price as a greater priority than performance, the benefits of a Private MPLS-based Secure Private IP Solution, outweigh those of a VPN.


Without VPN
Your Computer
Public/Personal Router
Your ISP's router
INTERNET
With VPN
Your Computer
Your data is encrypted
Public/Personal Router
Your ISP can't see your online activity
Your ISP's router
You're browsing all protected
INTERNET

CHAPTER - 4

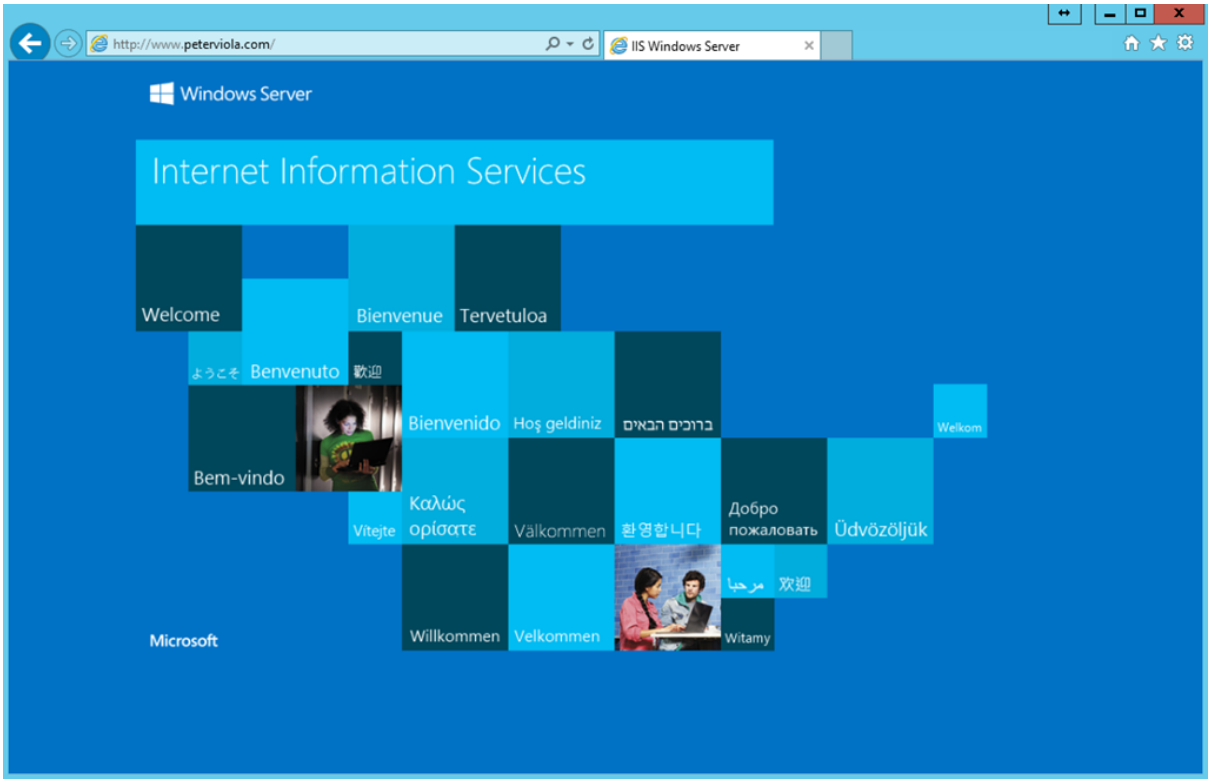
IIS SERVER

Internet Information Services (IIS) is a flexible, general-purpose web server from Microsoft that runs on Windows systems to serve requested HTML pages or files. An IIS web server accepts requests from remote client computers and returns the appropriate response. This basic functionality allows web servers to share and deliver information across local area networks, such as corporate intranets, and wide area networks, such as the internet.

A web server can deliver information to users in several forms, such as static webpages coded in HTML; through file exchanges as downloads and uploads; and text documents, image files and more.

Web servers provide portals

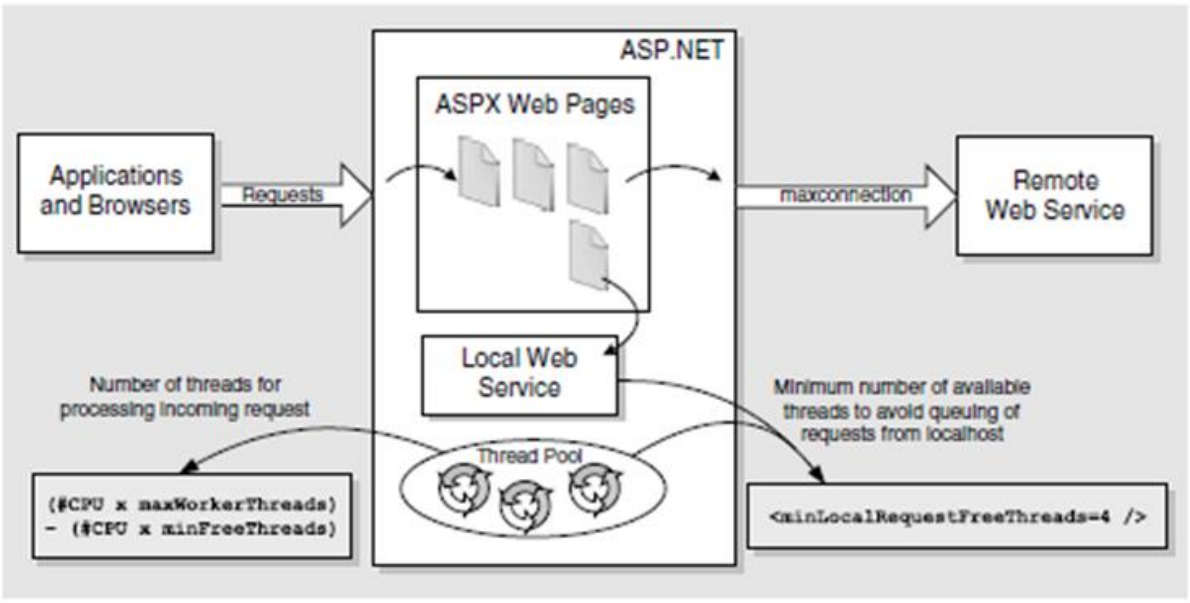
Modern web servers can provide far more functionality for a business and its users. Web servers are often used as portals for sophisticated, highly interactive, web-based applications that tie enterprise middleware and back-end applications together to create enterprise-class systems. For example, Amazon Web Services allows users to administer public cloud resources through a web-based portal. Meanwhile, streaming media services, such as Spotify for music and Netflix for movies, deliver real-time streaming content through web servers.



4.2 How IIS works?

IIS works through a variety of standard languages and protocols. HTML is used to create elements such as text, buttons, image placements, direct interactions/behaviors and hyperlinks. The Hypertext Transfer Protocol (HTTP) is the basic communication protocol used to exchange information between web servers and users. HTTPS -- HTTP over Secure Sockets Layer (SSL) -- uses Transport Layer Security or SSL to encrypt the communication for added data security. The File Transfer Protocol, or its secure variant, FTPS, can transfer files.

Additional supported protocols include the Simple Mail Transfer Protocol, to send and receive email, and the Network News Transfer Protocol, to deliver articles on Usenet.



In contrast, the diagram below shows Hyper-V with nested virtualization enabled. In this case, Hyper-V exposes the hardware virtualization extensions to its virtual machines. With nesting enabled, a guest virtual machine can install its own hypervisor and run its own guest VMs.

Versions of IIS

IIS has evolved along with Microsoft Windows. Early versions of IIS arrived with Windows NT. IIS 1.0 appeared with Windows NT 3.51, and evolved through IIS 4.0 with Windows NT 4.0. IIS 5.0 shipped with Windows 2000. Microsoft added IIS 6.0 to Windows Server 2003. IIS 7.0 offered a major redesign with Windows Server 2008 (IIS 7.5 is in Windows Server 2008 R2). IIS 8.0 came with Windows Server 2012 (Windows Server 2012 R2 uses IIS 8.5). And IIS 10 arrived with Windows Server 2016 and Windows 10.

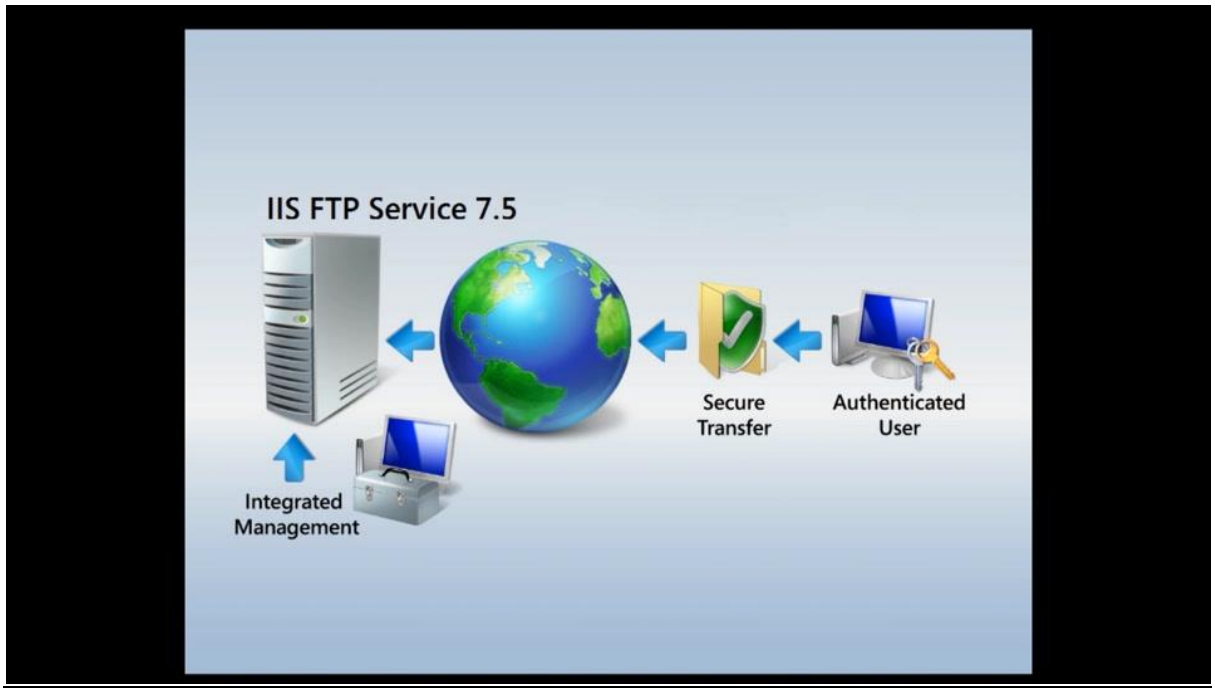
4.2 Benefit of IIS Server:

- Manageability - Logging Enhancements
- Manageability - ETW Events
- Scalability - Dynamic site activation
- Scalability - Idle Worker Process Page-out
- Certificate Rebind
- Dynamic Registration Threshold (system application Host/web Limits)

CHAPTER - 5

FTP

Microsoft rewrote the FTP service for Windows Server® 2008 and above. This updated FTP service incorporates many new features that enable web authors to publish content better than before, and offers web administrators more security and deployment options.



5.1 Configuring FTP:

1. Enable Web Server (IIS) role and FTP Server role service.

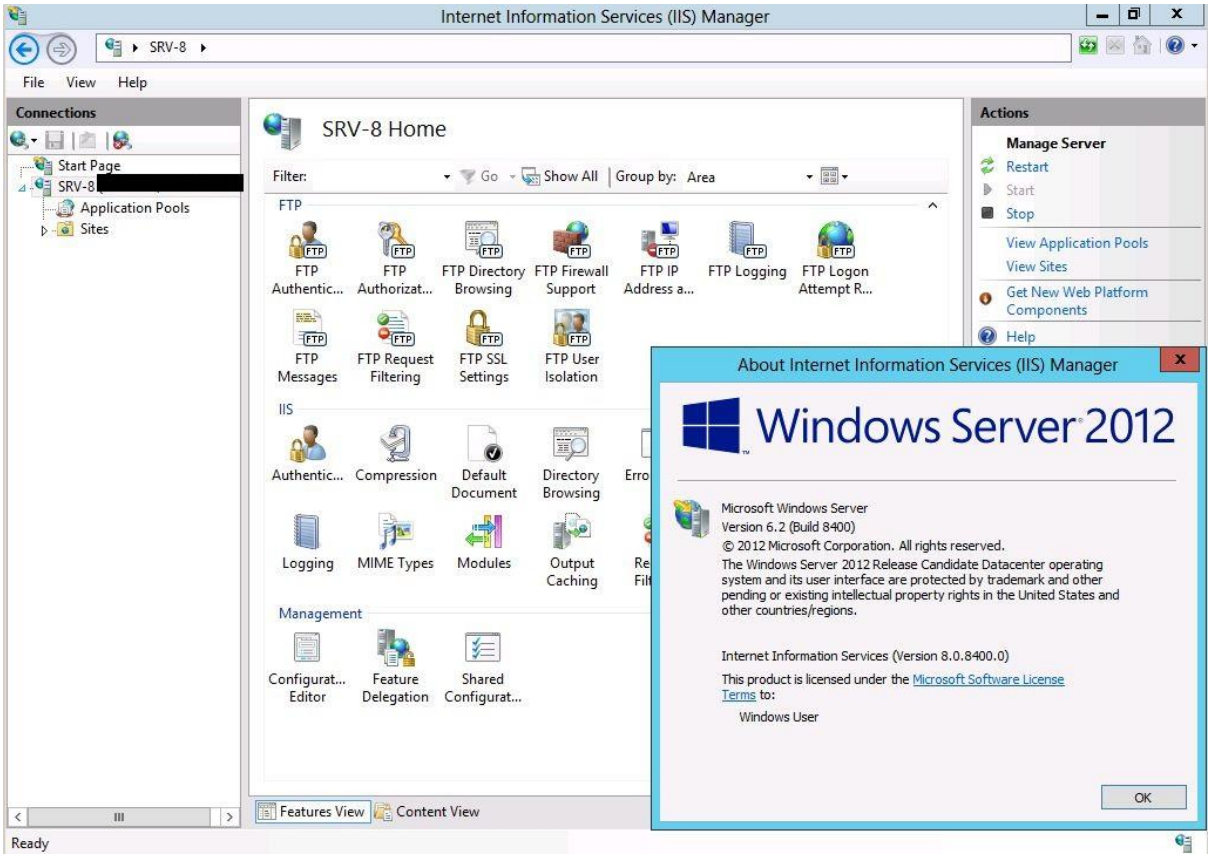
1. Log in to the server by using an administrative account
2. Open Server Manager
3. Go to Manage > Add Roles and Features
4. Click Next
5. Select Role-based or feature-based installation
6. Click Next
7. Select Select a server from the server pool, and select your server
8. Click Next.

9. Scroll down and put a check mark in Web Server (IIS)
10. An Add features window pops up. Put a check mark in the Include management tools (if applicable) option
11. Click Add Features button
12. Click Next
13. Scroll down and put a check mark in: FTP server, FTP Service and FTP Extensibility.
14. Click Next
15. Click Install
16. When installation is finished, click Close

2. Create FTP users

You need to create users in Windows in order to be able to use FTP services. You can use either local or domain users. In this case, I will create some local users. The only thing that changes if you use domain users is, when you log in to FTP, you must use the domain/ account format.

1. In Server Manager go to Tools
2. Click Computer Management
3. Click Local Users and Groups
4. Click Users
5. In the centre pane, right-click a blank area and then select New User
6. Enter the username information and click the Create button
7. Create as many usernames you need here.



5.2 Benefits of FTP:

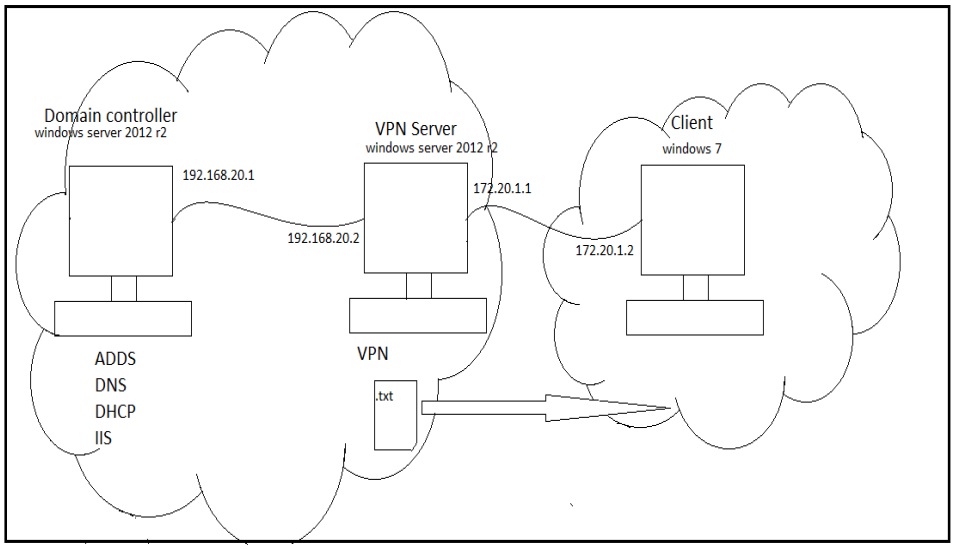
- Allows you to transfer multiple files as well as directories
- The ability to resume a transfer if the connection is lost
- The ability to add items to a “queue” to be uploaded/downloaded
- Many FTP clients have the ability to schedule transfers
- No size limitation on single transfers (browsers only allow up to 2 GB)
- Many clients have scripting capabilities through command line
- Most clients have a synchronizing utility
- Faster transfers then HTTP
- Supported on almost all hosts (per Randy Downs at Downs Consulting Services)

Those are just a few of the advantages of using an FTP client. While the clients help make transfers easier.

CHAPTER - 6

DATA TRANSFER OVER WEB OVERVIEW

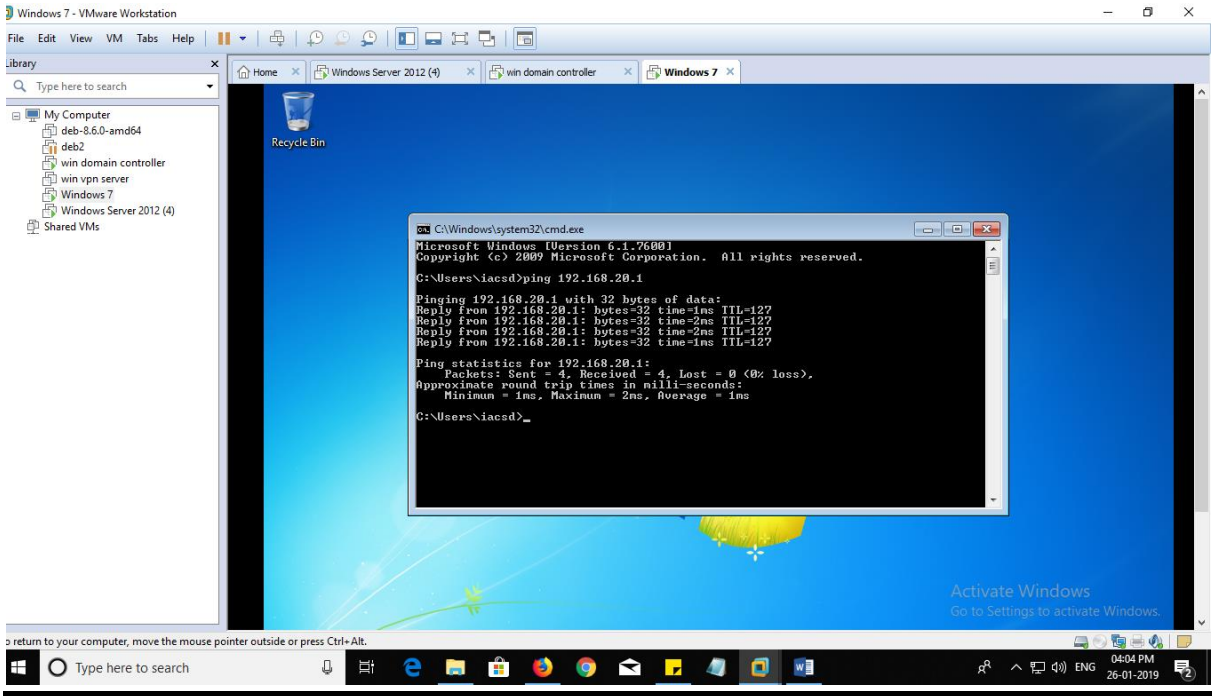
6.1 Data Flow Diagram



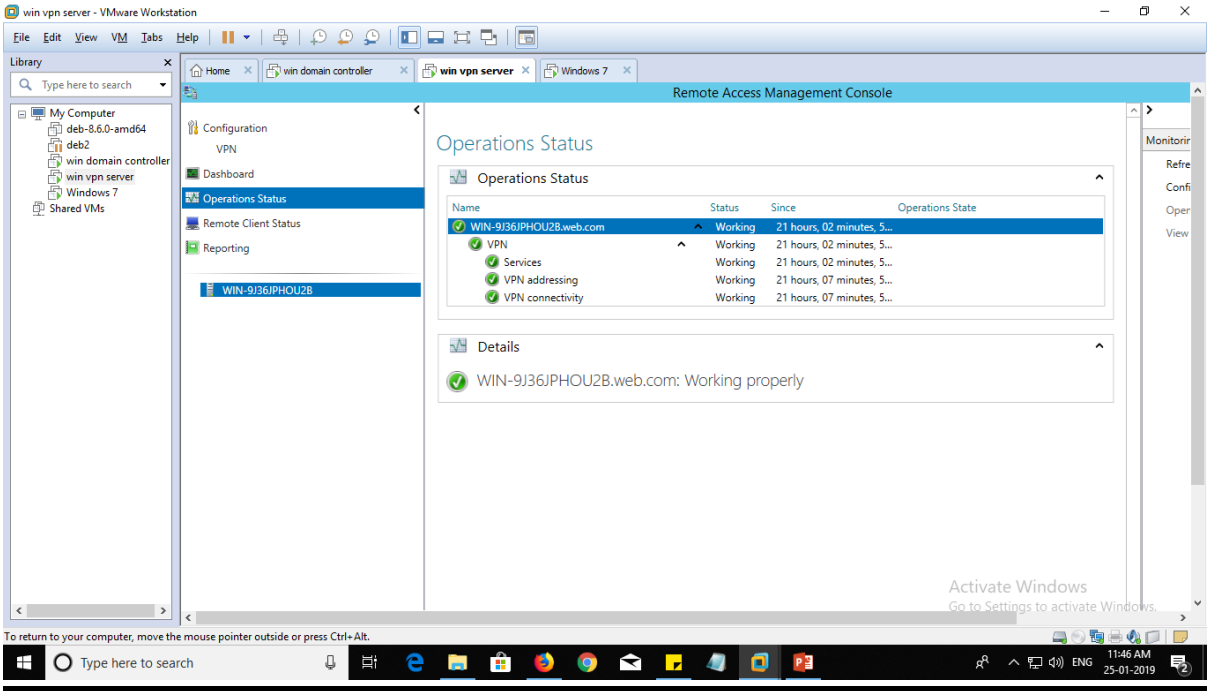
CHAPTER- 7

SCREENSHOTS

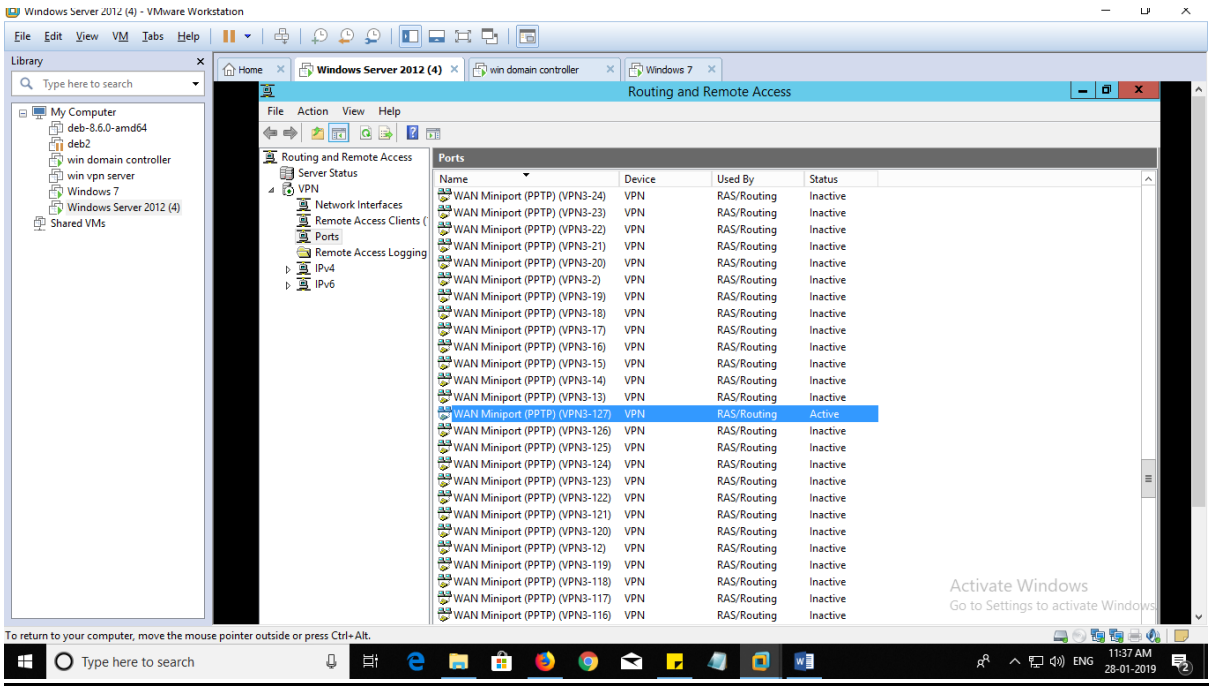
Three Machine communicate with each other



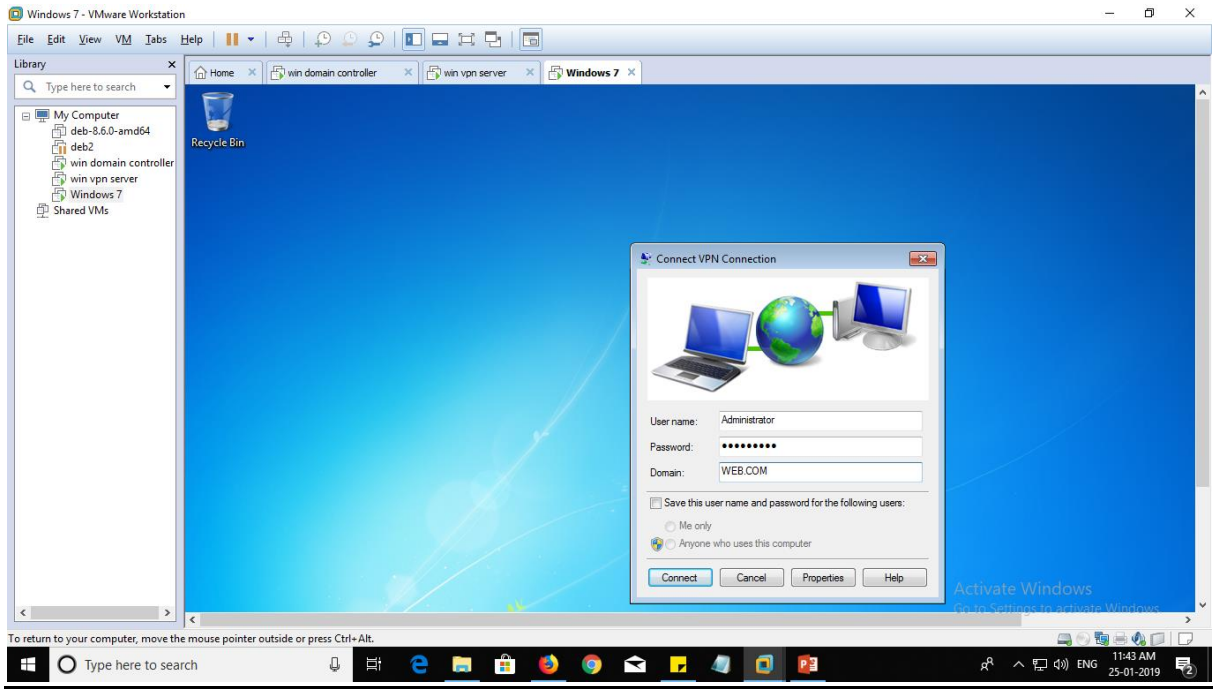
VPN Server Implementation



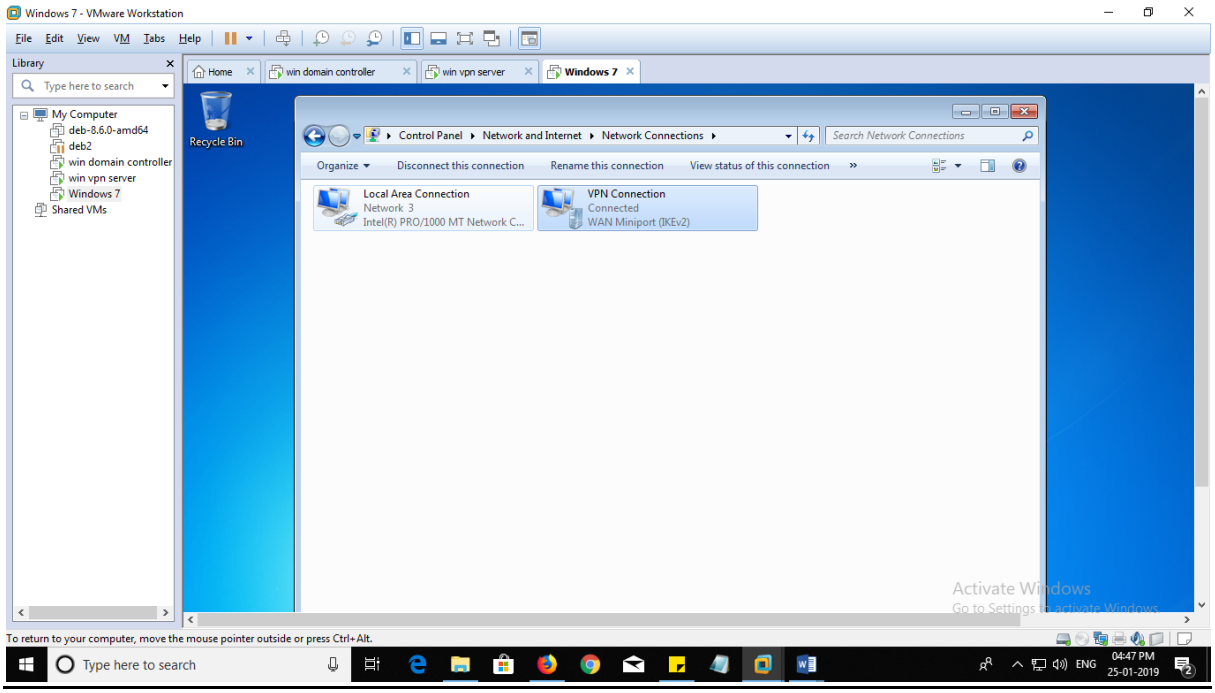
WAN Miniport (PPTP) (VPN3-127) is active



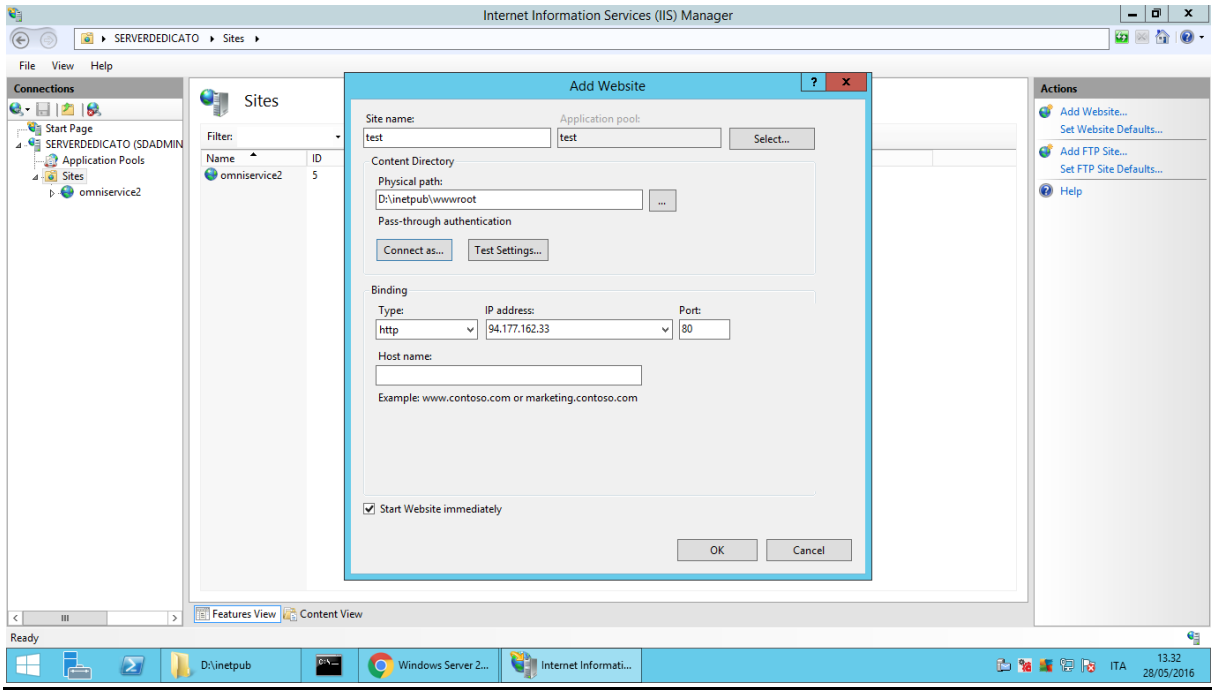
Authenticate Username and Password for VPN connection



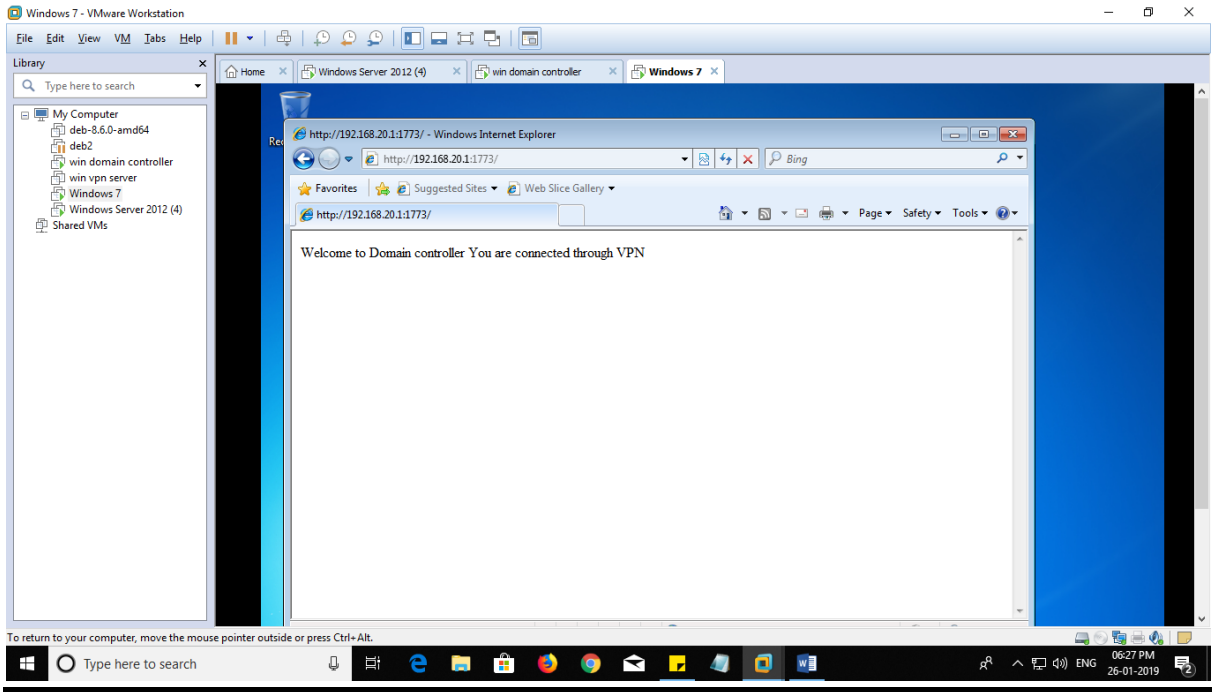
Successfully Established VPN Connection



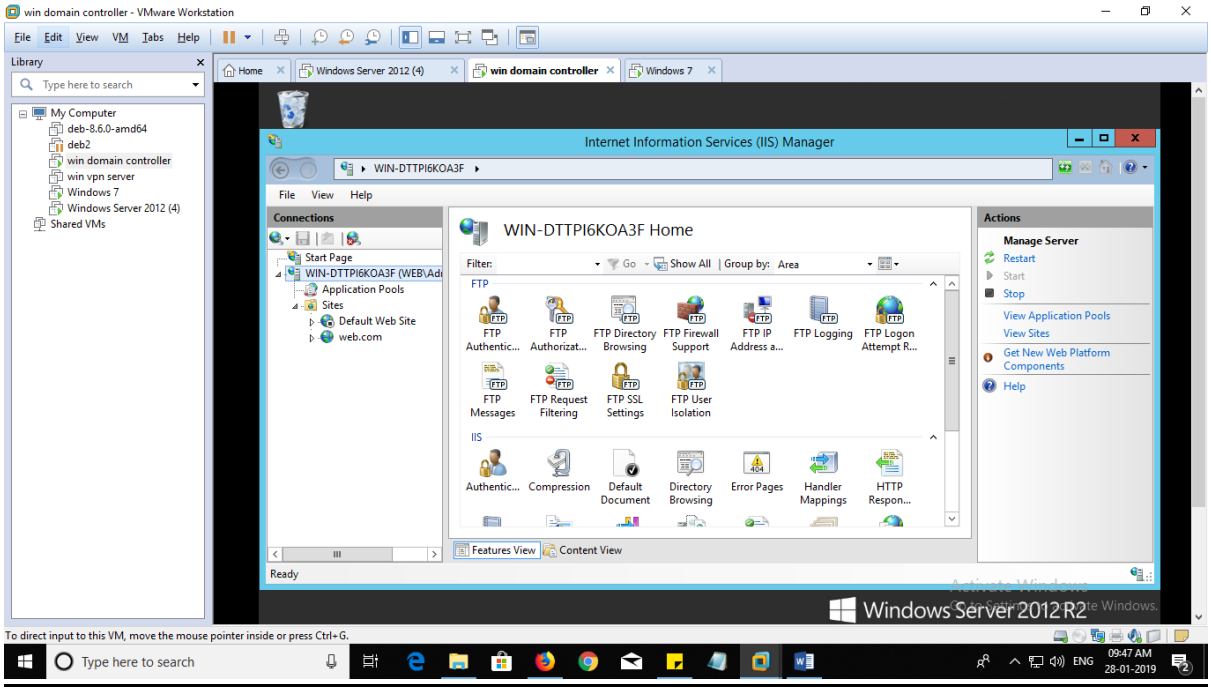
IIS Server



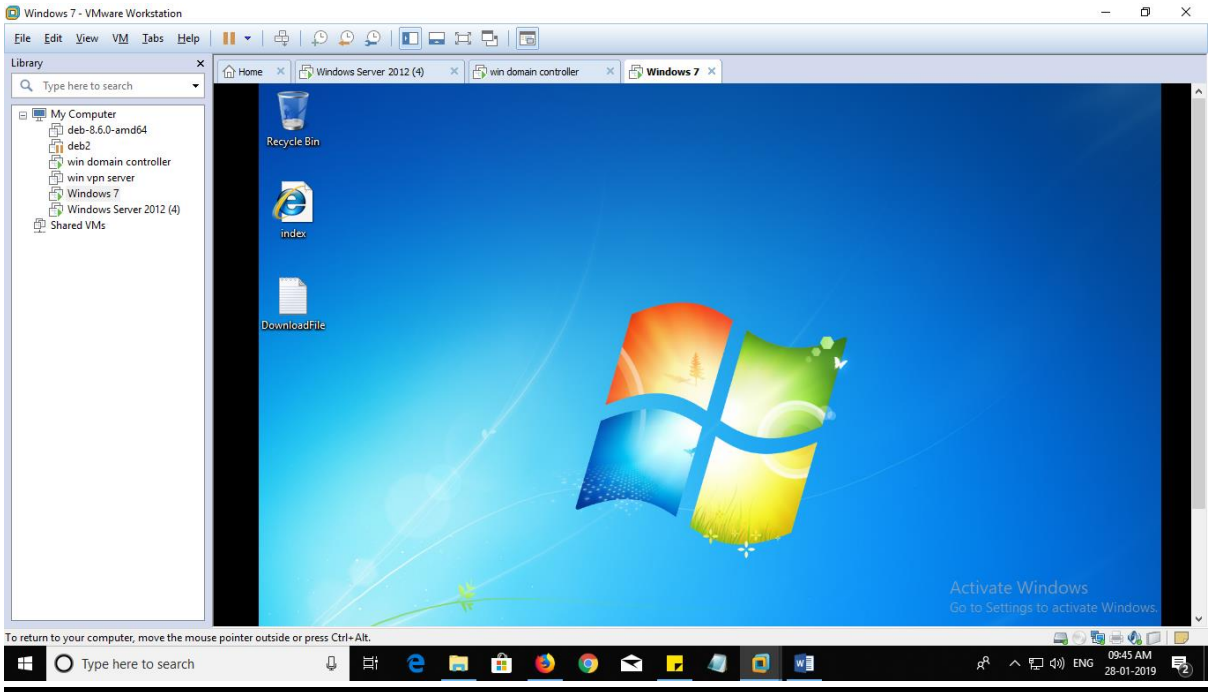
Website host On Client Machine through IP address



FTP Setup



File download on Client Machine through VPN



CONCLUSION

Our project is an approach to implement scenario of data transfer over web using VPN. Provide functionality that helps internet user's access content from anywhere in the organization, with just a click of a mouse. Therefore, we can say that a VPN is a secure solution that allows its users to send and receive data via the internet while maintaining the privacy and confidentiality of their data, based on its encryption level.

BIBLIOGRAPHY

The references used in the project are:

http://techgenix.com/configure-vpn-windows-server-2012-r2/

http://enterprise.arcgis.com/en/web-adaptor/latest/install/iis/enable-iis-2012-components-server.html

https://vpsie.com/knowledge-base/how-to-setup-ftp-server-users-on-windows-2012-r2/

https://www.youtube.com/watch?v=icmnmqRHO9s

https://www.youtube.com/watch?v=-E1GvdJCoX0