Chapter 5

Configure Routing and Remote Access

Testing VPN : 26. How to configure SSTP VPN on Windows Server 2019 - YouTube

VPN Installation and Configuration: Server 2019 VPN Installation and configuration - YouTube

24. Install and Configure Remote Access VPN on Windows Server 2019 - Bing video

Outline

- Configure Routing and Remote Access
  - Routing and remote access in Windows
  - Routing and remote access in Linux

Introduction

- **What is routing and remote access in network administration?**
  - **to do remote access between client and server.**
  - **In order to do that, we need a to install and configure software.**
  - **In windows server using Routing and Remote Access Service (RRAS)**
  - **In Linux using Secure Shell (SSH) via PuTTy.**

  **** PuTTy is a free and open-source terminal emulator, serial console and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection. It can also connect to a serial port. The name "PuTTY" has no official meaning.**

Routing and remote access in Windows

- Routing and Remote Access Service (RRAS) is a Microsoft API and server software that makes it possible to create applications:
  1. to administer the routing and remote access service capabilities of the operating system,
  2. to function as a network router.
  3. to implement routing protocols.

- ** application programming interface (API) is a web service that provides the connection between the application and the data sources.

Definition

- **Routing and remote access service (RRAS):**
  - **is a suite of network services in the Windows Server family that enables a server to perform the services of a conventional router.**
  - **It provides connectivity for remote users and remote offices to the corporate network.**
  - **RRAS includes an application programming interface (API) that facilitates the development of applications and processes for administering a range of network services.**
  - **It provides a remote access connection enables services such as file and print sharing to be available to remote users.**
- **To access network resources, remote access clients can use standard Windows tools.**

Ref: https://www.tech-faq.com/routing-and-remote-access-service.html

Services included in the RRAS suite include:

- **Remote access**
- **Dial-up remote access server**
- **VPN remote access server**
- **IP router for connecting subnets of networks**
- **Network address translation services**
- **Other router-specific services**
- **Dial-up and VPN site-to-site demand-dial router**

Ref: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11)

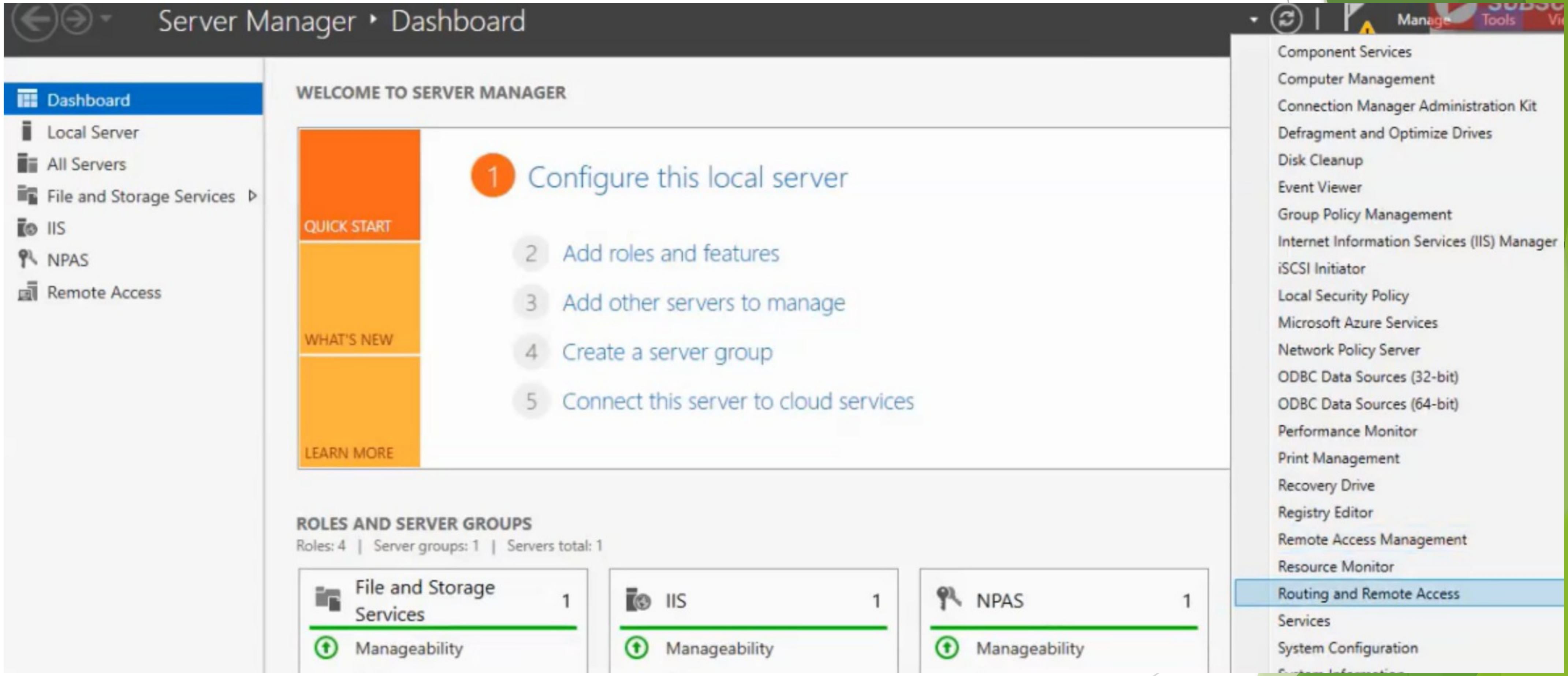
- The Routing and Remote Access service (RRAS) includes integrated support for the following dynamic routing protocols:
  - Routing Information Protocol (RIP) version 2
  - Open Shortest Path First (OSPF)
  - Routing and Remote Access service can be configured for:
  - LAN-to-LAN routing
  - LAN-to-WAN routing
  - Virtual private network (VPN) routing
  - Network Address Translation (NAT) routing
  - Routing features, including
    - IP multicasting
    - Packet filtering
    - Demand-dial routing
    - DHCP relay

f: https://www.tech-faq.com/routing-and-remote-access-service.html

- **The Routing and Remote Access service (RRAS) supports remote user or site-to-site connectivity by using virtual private network (VPN) or dial-up connections.**
- **a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together.**
- **Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee**
- **A VPN (Virtual Private Network) is a concept which helps enterprise companies with distributed offices to connect to each other securely over the Internet**

Ref: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11)
https://www.communicat.com.au/wp-content/uploads/2013/04/how_vpn_work.pdf
https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

Window Server 2019



WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

ROLES AND SERVER GROUPS

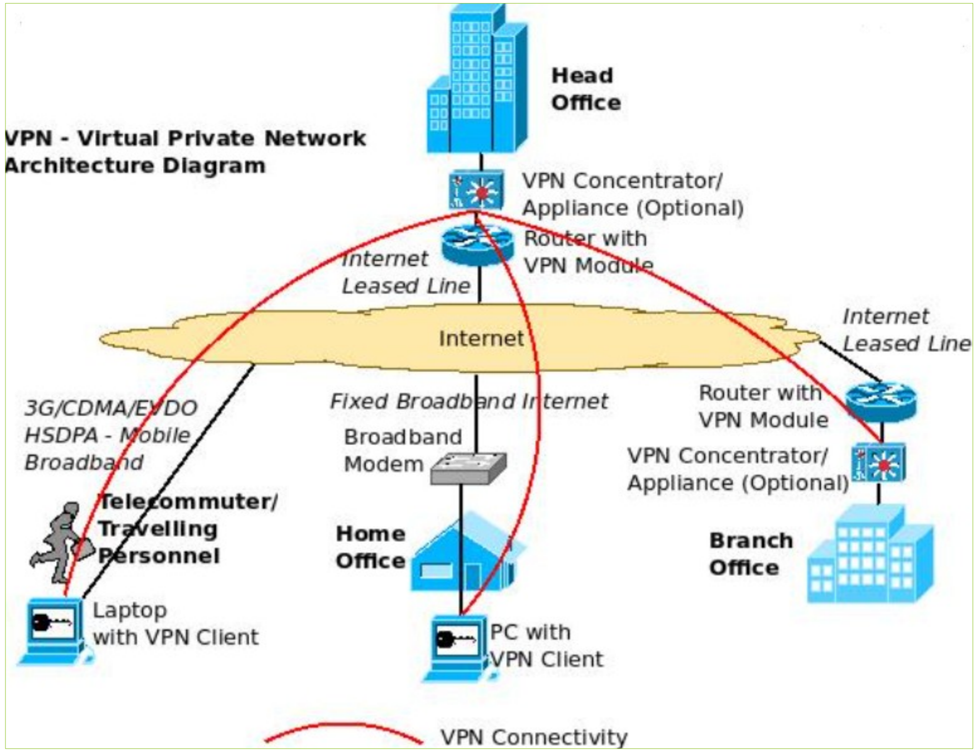
Roles: 4 | Server groups: 1 | Servers total: 1

File and Storage Services	IIS	NPAS
1	1	1
Manageability	Manageability	Manageability

virtual private network (VPN)

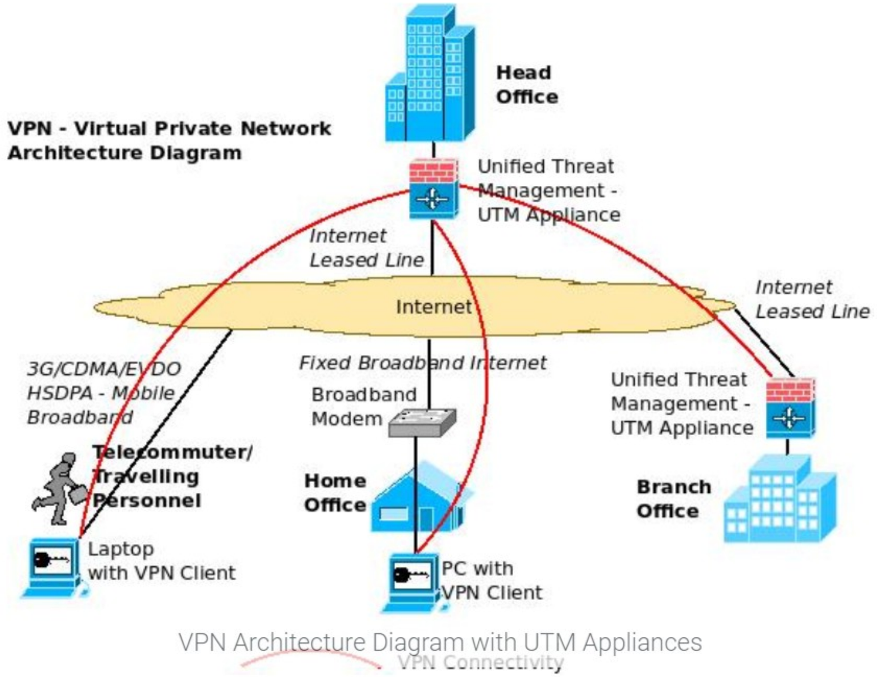
- **is an encrypted connection over the Internet from a device to a network.**
- **The encrypted connection helps ensure that sensitive data is safely transmitted.**
- **It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.**

Creating the site to site VPN between the head office and branch office using routers (or VPN Concentrators)



- The diagram shows a scenario where there are four locations (From top, clockwise)
- One is the head office (accessing Internet through Internet Leased Lines),
- the branch office (accessing Internet through Internet Leased Lines),
- a home office (accessing Internet through Fixed Broadband connection)
- telecommuter/ traveling personnel (Accessing Internet through mobile broadband technologies like CDMA/ EVDO/ 3G/ HSDPA etc).

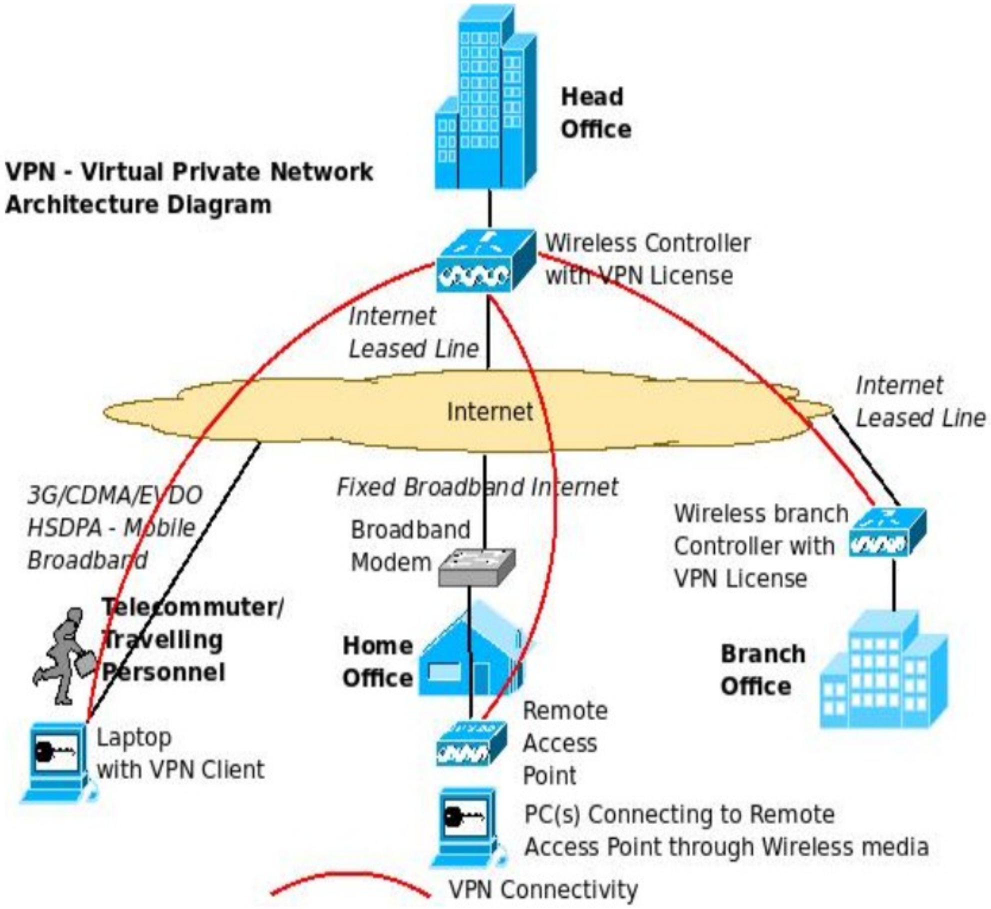
Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/



VPN Architecture Diagram with UTM Appliances

- **Creating a VPN with UTM (Unified Threat Management Appliance):use certain UTM appliances (which come with inbuilt VPN Licenses) for establishing site to site VPN.**
- **The home office/ traveling personnel can establish a VPN similarly by connecting to the UTM appliances in the head office (through the VPN Client).**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/



Creating a VPN using Wireless Controller:

•Use centralized management of multiple wireless access points in the enterprise) can itself act as a VPN concentrator (with appropriate licenses) and establish VPN Tunnels with other controllers, remote access points (home office) and VPN Clients (telecommuters/ traveling personnel).

•The VPN connections need not always be from the head office to the branch offices / traveling personnel etc as shown in the diagrams.

• It can be established from one site to another site, one site to multiple sites and multiple sites to multiple sites depending upon the configuration, models and connection types supported by the various VPN devices.

•Both Site to Site as well as Site to Client VPN's can be established.

f: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

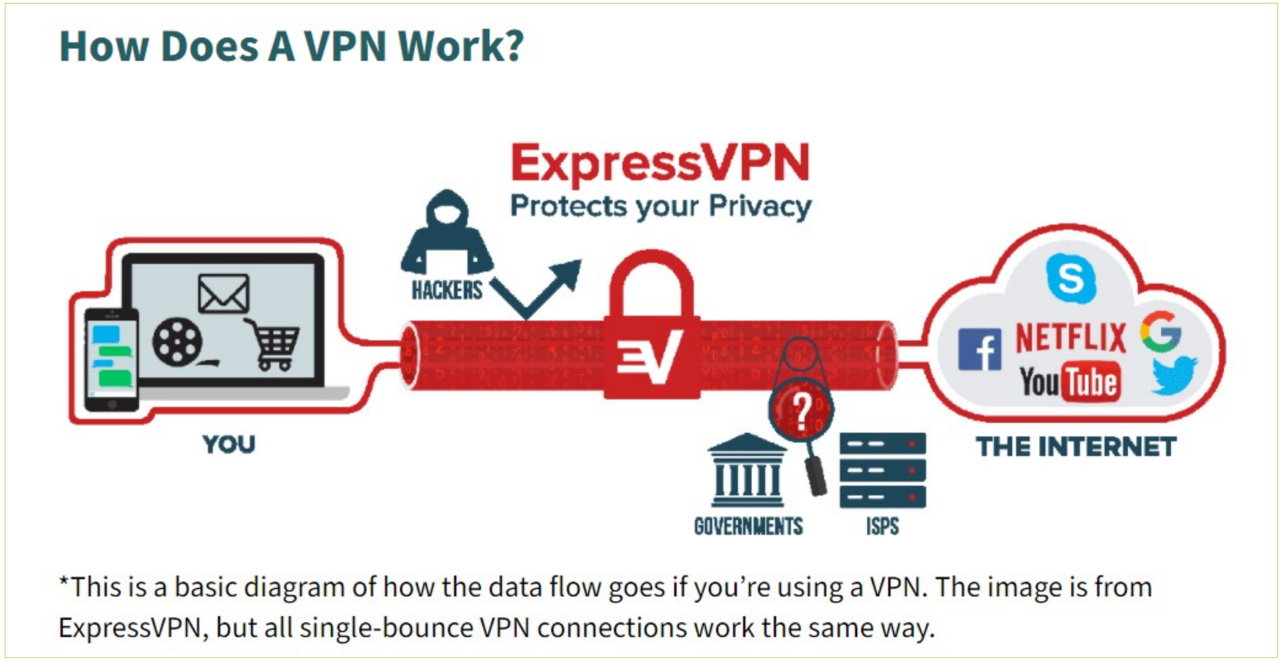
- **Two types of Virtual Private Networks**
  - **IPSec VPN**
  - **SSL/TLS VPN.**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

- **IPSec VPN:**
- **IPSec VPN or Internet Protocol Security VPN is one of the most popular technologies available for establishing VPN over the Internet.**
- **It establishes this by using technologies like tunneling, encryption and authentication.**
- **This type of VPN assumes that a trusted relationship is present between the various sites or individual computers forming the VPN and it defines procedures to provide data integrity, authenticity and confidentiality across the public network (Internet).**
- **IPSec VPN operates in the Network layer.**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

- **What is a VPN "tunnel"?**
- **A "tunnel" is the encrypted connection a VPN establishes so that traffic on the virtual network can be sent securely across the Internet. VPN traffic from a device such as a computer or smartphone is encrypted as it travels through the VPN tunnel.**



How Does A VPN Work?

*This is a basic diagram of how the data flow goes if you're using a VPN. The image is from ExpressVPN, but all single-bounce VPN connections work the same way.

ps://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-does-a-vpn-work.html

- **Advantages of IPSec VPN:**
- **IPSec VPN is an established and field tested technology and has been in use by majority of the customers for a long period now.**
- **IPSec VPN is a client based VPN technology and connects to only those sites/ devices which can prove their integrity (This is more applicable for home offices and remote offices where the VPN software client needs to be installed before-hand to establish a secure connectivity back to the head office). So, administrators can be quite sure that the devices connecting to the network are trusted ones.**
- **Since IPSec VPN inspects and drops a packet at a lower level in the protocol stack (network layer), the packet drop performance is better thereby enabling smooth functioning even in a high capacity usage scenario.**
- **IPSec VPN's are the preferred choice of companies for establishing Site to Site VPN and IPSec has found more implementations in this segment. IPSec VPN's can also establish a Site to Client VPN with devices installed with IPSec clients.**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

- **Advantages of IPSec VPN:**

- **IPSec VPN gives full access to all the head office Intranet applications to branch office/ remote personnel establishing the VPN to HO. So, the user feels as if they are at the office even though they may be working from home. Certain solutions allow selective blocking of certain applications/ devices from being accessed over a remote network.**
- **IPSec supports multiple authentication methods and demonstrates flexibility on choosing the appropriate authentication mechanism, making it difficult for intruders to perform attacks like 'Man in the Middle' attacks.**
- **Centralized management options for VPN settings are available with IPSec VPN.**
- **IPSec can implement automatic failover to another VPN device in case the original one fails**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

- **SSL/TLS VPN:**
  - **An SSL VPN uses the Secure Sockets Protocol (SSL) technology to create a virtual private network between various sites and sites to clients using encryption and authentication over the network.**
  - **Much of this protocol was adapted to Transport Layer Security (TLS) standard as well and hence it is some times referred to as TLS VPN.**
  - **SSL VPN can provide authentication, authorization, accounting and network access. SSL VPN can provide secure access through standard web browsers enabling VPN's to be established from any computer connected to Internet. SSL VPN can also provide Site to Site VPN.**
  - **SSL/TLS VPN operates in the Application Layer.**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

Advantages of SSL/TLS VPN:

- **Since SSL/TLS VPN’s support browser based access, corporate resources can be accessed by employees/ partners from any computer with Internet access after proper authentication.**
- **SSL/TLS VPN’s allow for host integrity checking (checking if the computers trying to establish a VPN connection subscribe to certain standards – like latest OS version with patches, latest version of anti-virus software etc) and remediation (if required) to ensure secure network access.**
- **Easier to deploy and maintain across a large number of traveling personnel/ remote users as there is no need to install and maintain a VPN client for each machine connecting to the network.**
- **SSL/TLS VPN can provide granular network access controls for each user/ group of users to limit remote user access to certain designated resources or applications in the corporate network.**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

Advantages of SSL/TLS VPN:

- **SSL/ TLS VPN supports many types of end point devices like mobile phones, PDA's, smart phones etc and multiple operating systems.**
- **Supports multiple methods of user authentication and also integration with centralized authentication mechanisms like Radius/LDAP, Active Directory etc.**
- **It is possible to have secure user customized web-portals (Extranets) for partners etc with SSL/TLS VPN, as the basic characteristic of SSL/TLS VPN is to provide restricted access to certain applications only, and adding more applications when required, thereby providing granular network access controls.**
- **SSL/TLS VPN's are basically designed for Internet browsers and hence do not have any NAT/Firewall traversal issues.**
- **SSL/TLS VPN's have exhaustive auditing capabilities which is crucial for regulatory compliance. Log information (regarding which user accessed which resources at what time over which period/date etc) can be taken, stored and analyzed with detailed querying and reporting mechanisms.**
- **SSL VPN's can cluster VPN devices both within the LAN as well as across the WAN for improved performance, scalability and redundancy.**
- **SSL VPN's are better for disaster recovery/ business continuity as it allows for anywhere anytime access to the corporate networks for authorized users.**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

- **Most users don't need to install client software**
- **SSL VPN uses SSL protocol and its successor, Transport Layer Security (TLS), to provide a secure connection between remote users and internal network resources.**
- **Because most web browsers now have SSL/TLS, users do not typically need to install client software to use SSL VPN. That's why SSL VPN is also known as "clientless VPN" or "web VPN."**

os://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-does-a-vpn-work.html

Differences between SSL and IPsec VPN

- **SSL VPN is flexible for end users**
- **SSL VPN is also easy to use.**
- **SSL VPN only requires users to have a modern web browser. Users may even choose their favorite web browsers without being restricted by the operating system.**
- **Different IPsec VPN vendors may have different implementation and configuration requirements.**

ps://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-does-a-vpn-work.html

- **Open source VPN:**
  - **Apart from many commercial products available for VPN, there are also free open source alternatives to establish a VPN between two places like OpenVPN and OpenSSL.**
  - **You may need a hardware device for running the open source software at both the places.**

Ref: https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

- VPNs are a cost-effective way to connect remote users to corporate network securely while also improving connectivity speeds.
- With VPNs, businesses can use high-bandwidth, third-party Internet access instead of expensive, dedicated WAN (wide-area network) links or long-distance, remote-dial links.
- Secure remote access is a method for connecting remote users and devices securely to a corporate network.
- It includes VPN technology, which authenticates users or devices, confirming that they meet certain requirements—also known as "posture"—before they can connect to the network remotely.

ps://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-does-a-vpn-work.html

Best VPN Service Providers for Use in Malaysia

- The following 5 VPN service providers offer the best protection and enhancement for your online activities while residing in or visiting Malaysia. The condensed version is:

1. NordVPN: NordVPN ranks as #1 thanks to its top-notch connection speeds, solid security and privacy protections, excellent app support and more. The provider offers its premium service for a reasonable price.
2. Surfshark: Surfshark charges a pittance for its fast connection speeds, a wide global server network and unlimited simultaneous connections policy, making it best for budget-minded users.
3. ExpressVPN: ExpressVPN offers fast, well-encrypted connections on its extensive global server network. You'll want to check out this provider if you especially want access to geo-blocked content around the world.
4. CyberGhost: If you're new to VPNs or don't have much experience online, I strongly suggest you opt for CyberGhost for your VPN service. The provider's easy-to-use app provides quick access to server locations around the globe, including streaming- and downloading-optimized servers.
5. PrivateVPN: While this provider's global server network is lacking when compared to others on this list, it does a good job of working with what it has. The provider offers fast connections that deliver reliable access to geo-blocked content.

Ref: https://pixelprivacy.com/vpn/best-vpn-malaysia/

- When ranking the providers, the following factors are:
  - Global server locations with servers in Malaysia
  - Security and user privacy protection offered
  - Speed of provided connections
  - Native app support
  - Customer support features offered

ref: https://pixelprivacy.com/vpn/best-vpn-malaysia/

Routing and remote access in Linux

- **SSH, Telnet and Rlogin are three ways of doing the same thing: logging in to a multi-user computer from another computer, over a network.**
- **SSH, Telnet and Rlogin are *network protocols* that allow you to do this. On the computer you sit at, you run a *client*, which makes a network connection to the other computer (the *server*). The network connection carries your keystrokes and commands from the client to the server, and carries the server's responses back to you.**

Ref: http://the.earth.li/~sgtatham/putty/0.53b/htmldoc/Chapter1.html

- **SSH Basics 2020 - Set-up SSH, Connect to a remote server, create a SSH config Mac, Windows and Linux**
- **https://www.youtube.com/watch?v=B_IZt9_9UCc**
- **SSH Crash Course | With Some DevOps**
- **https://www.youtube.com/watch?v=hQWRp-FdTpc**

SSH or Secure Shell is a network communication protocol that enables two computers to communicate (http or hypertext transfer protocol, which is the protocol used to transfer hypertext such as web pages) and share data.

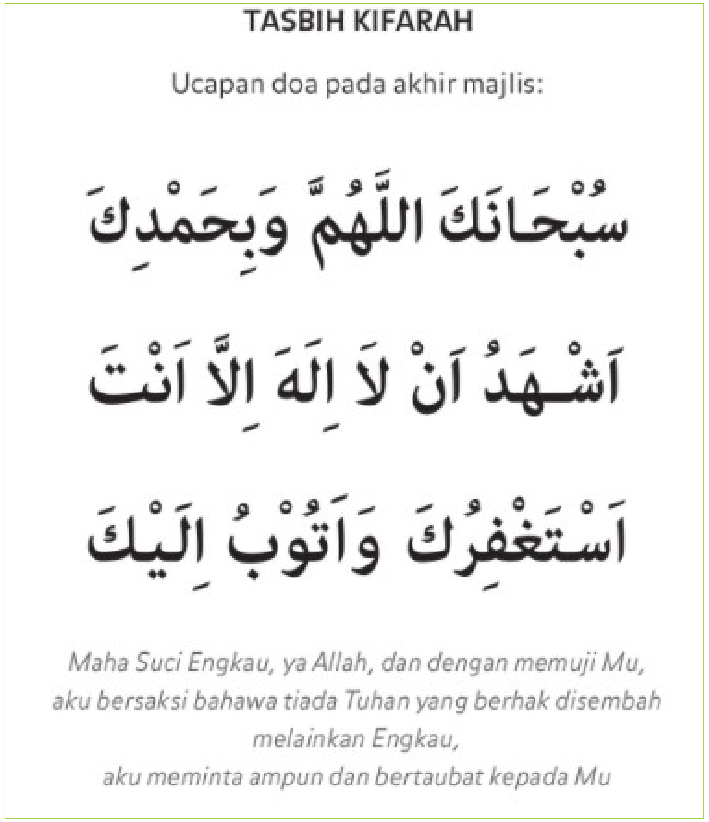
Additional info:https://searchsecurity.techtarget.com/definition/Secure-Shell

- **PuTTY is a versatile terminal program for Windows.**
  - **It is the world's most popular free SSH client.**
  - **It supports SSH, telnet, and raw socket connections with good terminal emulation.**
  - **It supports public key authentication and Kerberos single-sign-on.**

PuTTY/SSH Intro Tutorial

https://www.youtube.com/watch?v=9CZphjhQxIQ

The End



TASBIH KIFARAH

Ucapan doa pada akhir majlis:

سُبْحَانَكَ اللَّهُمَّ وَبِحَمْدِكَ

اَشْـهَدُ اَنْ لاَ اِلَهَ اِلاَّ اَنْتَ

اَسْتَغْفِرُكَ وَاَتُوْبُ اِلَيْكَ

Maha Suci Engkau, ya Allah, dan dengan memuji Mu,
aku bersaksi bahawa tiada Tuhan yang berhak disembah
melainkan Engkau,
aku meminta ampun dan bertaubat kepada Mu