Free term paper about network technology

Business, Company

OVERVIEW

An international pharmaceutical company is headquartered in New York, NY and has other six operational locations. The corporate headquarters in New York has 1000 employees while the other centers have a considerable number of employees and remote workers. San Diego has 250 employees, Houston has 750 employees in central research, Madrid has 500 employees, India has 50, and London has 150 while China has 300 employees and 500 remote sales workers. There is a diverse computing department with no universal standard. There is a combination of devices and operating systems in place. There are also different data center centers in operation. The data center in New York is used as the main corporate data center. There are email, file, print, database and intranet web services in this server while that in San Diego has high-performance computing, technical application servers and video-streaming services for R &D. Finally a data center in Houston TX is used for disaster recovery. The company engages in large file transfer and there is one internet connection located in the corporate data center that services all company locations.

This paper proposes a network design for local and wide area network. The network should be able to service both internal and remote users of the company effectively. The network should span seven cities and accommodate more than 3, 500 users. Background information concerning this company is that it was formed through a number of acquisitions via venture capitalists. The data center in New York is used as the main corporate data center.

A virtual private network is preferred in this case. A VPN is a wide area

networking technology that is facilitated by global interconnectivity. It is made up of hardware and software that are configured to allow access for internal and external organizational resources. In this case, users can share the pooled resources no matter how far their location is from the corporate headquarters. VPN is facilitated by the internet protocol. The pharmaceutical company has been formed by acquisitions and the only viable option to connect the seven regional and international locations sufficiently is by using a virtual private network. The wide area networking technologies in place today include MPLS, Ethernet and VPN Tunneling. Considering these technologies, VPN Tunneling is the only relatively cheap and secure option. VPN is characterized by its carrier agnostic nature and makes it compatible across multiple networks. Notably, the pharmaceutical setting comprise of a diverse number of technologies, standards and frameworks. It is this consideration with the ability to work with private networks while utilizing the same hardware infrastructure like the internet that makes it suitable for this option.

Media

Fiber is preferred as the best media to be used for networking. In this large network, fiber is appropriate given its ability to deliver optimally under long distances and high bandwidth. For example, the two multimode media with transmission speeds of 1GB/s and 50/125 OM2 and OM3 laser optimized cable may be used in this case given its compatibility will all the network fiber equipment. Internally, OM3 will be utilized for gigabit networks within the department while single mode fiber will be used for long distances where high speed is anticipated.

The installation of fiber optics will consider future expansion mechanisms such as high-speed network. Fiber will be installed within the premises but not terminated as a future proof for high-speed networks. It is anticipated that in the future, a high-speed network might be required and hence, this design strategy will ensure minimal alteration of the original network.

Network devices

The proposed diagram for the network is as shown.

Devices

A VPN router is used to connect the various locations to the VPN tunnel. A VPN router such as the Yamaha RTX810 support 50 locations or tunnels. It is recommended that four connections be used for every router in the PPTP protocol. In this case, an FTTH model is adopted. Fiber to the Home will provide the required high-speed connectivity and sufficient bandwidth to the seven locations.

Protocols

A point to point connection between a VPN client and the VPN server or a site-to-site connection two VPN servers is referred as a virtual private network. A connection between the corporate headquarters and branch office could be a permanent site to site VPN connection. For telecommuting users, there is a possibility to create an on-demand VPN connection to the VPN server located at the branch office or headquarters.

There are three VPN tunneling protocols available; point-to-point tunneling protocol PPTP, layer two tunneling protocol L2TP and secure socket tunneling protocol SSTP. PPTP, L2TP and SSTP are founded on the point-to-point

protocol. PPP is a protocol developed to send data trans-dial-up or even in PPP which are dedicated. Tunneling process allows the encapsulation of a packet from one type of a protocol to another. PPTP protocol is the protocol of choice in this case because it involves encapsulation of IP packets over a public network such as an internet. PPTP functions by allowing the encryption of traffic to take place and then followed by encapsulation in the IP header for it to be able to be sent over the network. The multinational company require remote access to allow many of its employees and sales force to connect to company resources. Also there is need for large file transfer between San Diego and Houston. To serve this need, the cprotocol choice is PPTP. PPTP support remote access as well as site-to-site VPN connections. Because the internet will be used as the default public network to connect users in the geographically dispersed locations, then PPTP server will be incorporated. PPTP enabled VPN server will have one end facing the internet and the other end facing the intranet.

Encapsulation of PPP frames so that they can be transported over the network. It will be led by TCP connection and Generic Routing Encapsulation (GRE). This way, the payloads of the encapsulated PPP frames are encrypted and compressed in a manner suitable for transmission. The encryption process is done using an assistant such as the Microsoft Point-to-Point Encryption. MPPE utilizes encryption keys which is got from MS-CHAP V2 and EAP-TLS authentication procedures. It is recommended that VPN use MS-CHAP v2 or EAP-TLS authentication protocol in order for the payloads of the PPP frames to be encrypted. PPTP leverages the underlying PPP encryption and encapsulation of previously encrypted frames.

WAN circuit and connectivity

MPLS is preferred for site to site connectivity. There are three reasons why MPLS is preferred for connecting geographically dispersed sites. One, it provides guaranteed performance for real time IP-based applications that includes video and audio. Two, it flattens the network and diminishes dependence on hub and spoke designs, and three, it saves money. MPLs are de facto network protocol for wide area networks because of reliability, flexibility and controls.

Remote access method and authentication

A VPN is an extension of a private network and comprises of links across public and shared networks internet included. The point-to-point protocol in VPN allows users to send data securely between two locations in the network. Mobile users in China, London, Madrid and other locations have the capability to send data to the headquarters in a secure manner similar to a point-to-point process synonymous with private networks. The remote user will be able to access the entire network by dialling internet connection. The VPN server behaves like a router to provide a connection to the entire network for which the server is connected to. In order to get connected, the VPN client must authenticate itself to the VPN server and vice versa. Once mutual authentication process is completed, the user can access the resources in whatever location in the network. Company’s sales force in China will be able to file sales and other details remotely through intranet and extranet based networks. Intranet applies to users within the company while extranet is applicable to those outside the company resources.

In order to standardize operations, it is recommended that the company

deploy similar software in all its locations. An operating system such as Windows Server 2012 comes with functionality that control authentication. Network Access Protection is a good functionality for issuing health certificates of the organization’s IPsec peer intranet tunnels. NAP is managed by the HRA that issue certificates based on System Health Object Identification. NAP health checks allow some users to the network while denying others. It uses the Remote Access Setup Wizard. The policies used by NAP allow telecommuting users such as those in China to log in to the company’s network and execute their mandates using extranets. The user must provide their credentials to a VPN network and these credentials are exchanged based on administrator's rules. Administrators will define group object policies that determine who accessed which network. For instance, R&D department will be restricted to those working in this department alone. Hence, through group user policies, administrator will deny telecommuters such as the sales force from accessing their information.

Fault tolerance

VPN data networks are critical for business operations and success. There is a need to ensure that VPN provides a reliable service to users and their applications. In this discussion of fault tolerance, we base our analysis on Windows platform. Windows Server 2012 provides a favorable platform for solving network issues for remote, mobile and on-site users. There are two functionalities in Windows framework that ensure that organizations do not loose network connections. DFS Namespace is the first. DFS Namespace allows folders to be shared publicly in multiple sub-folders across the network. A user looking for a file in the namespace will be redirected to the

source server. The namespace locates the file and directs the user to where the file is located for efficient retrieval. Another reliable way of ensuring that remote users connect securely to company resources is by installing controls. The controls ensure that remote users connect to VPN and use application virtualization to permit screen sharing of an application running on a server while restricting direct access of the remote computer to the network.

DFS replication is the next phenomenon used for establishing fault tolerance in Windows based VPN network. With replication, folders are multiplied and stored in different locations. Data is spread uniformly across the organization and any changes introduced in one location will be effected in the rest locations. A file slightly changed in the headquarters will have its changes updated in all other locations in a mechanism referred to as remote differential compression.

Security

IPsec VPN is a favorable medium for establishing a permanent connection between locations. IPsec works at the network layer and makes its application agnostic. It means that any IP-based protocol can be tunneled through it. However, the application agnostic design introduces weaknesses related to security. Security measures incorporate in the IPsec VPN include authentication, authorization and encryption. These are insufficient to restrict access to any remote user, and for that matter, Network Address Translation is used in addition to setting up the appliance to terminate insecure tunnels. Special configurations are applied to ensure that IPsec functions well with NAT. Additional security measures include granular

access control limitations and missing-host check functionalities designed by the administrator to augment with Network Access Control capabilities. Another reliable way of ensuring that remote users connect securely to company resources is by installing controls. The controls ensure that remote users connect to VPN and use application virtualization to permit screen sharing of an application running on a server while restricting direct access of the remote computer to the network. It largely eliminates the risk of a connection originating from a remote computer and spreading to systems on the network.

References

(CCIE.), M. L. (2013). Comparing, Designing, and Deploying VPNs. Adobe Press.

Alex Shneyderman, A. C. (2003). Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems. John Wiley & Sons.

Hooper, H. (2012). CCNP Security VPN 642-648 Official Cert Guide. Cisco Press.

Syngress, D. L. (2012). Firewall Policies and VPN Configurations. Syngress.

Tomsho, G. (2011). Guide to Networking Essentials. Cengage.