Research proposal on san system architecture network proposal

Law, Security

ABSTRACT

SAN Solutions Inc., is a multinational company with over 500 employees distributed across headquarters and remote offices. The organization is involved in a significant Department of Defense project and thus need seamless connectivity across its branches, and the headquarters to enhance productivity. Because of the nature of the project, the company forbids any external access of its details outside the U S. As the Director of IT, I am tasked with the responsibility of recommending a secure and efficient network solution to remote branches located in Denver, New York, Los Angeles, Chicago, Colorado. The main areas of concern include accounting, sales, engineering, production and executive management departments. In this respect, a site-to-site virtual private network is the ultimate solution for SAN. With site-to-site VPN, the company employees will communicate with the headquarters through a subnet of the internet that guarantees greater security and privacy. VPNs vast capabilities such as corporate network telecommuting, secure collaboration and private browsing will ensure that employees access the necessary resources to execute their work securely across all branches. Management of projects from the headquarters will also be simplified as DoD projects will only be handled by the United States branches.

As part of the overall mandate of creating a comprehensive network infrastructure that provides a solution to SAN connectivity issue, this paper is going to provide an all round analysis of the components of the network. This is especially the IPv4/ IPv6 implementation, and configuration plan, DHCP options. There is also a complete DNS design for a seamless web, and active

directory, secure and feasible routing, file server configuration, backup and restoration mechanisms, DFS implementation, remote file sharing, and recommended disk quotas and allocation.

INTRODUCTION

In the corporate world, mobility and remote access are the business drivers with companies opting to open, as many, branches as possible to gain a considerable market share. The ability to felt around the globe and connect seamlessly to the headquarters is the paramount concern. Remote branches need to convey their operations to the headquarters with less difficulty than before. Likewise, the top managerial echelons need to pass crucial decisions and board directives to the branches in real time and with greater ease. As a result, the headquarters and branch connection must be pervasive and available no matter the location. Productivity in the branch offices can be improved through seamless network integration with the main branch. The fundamental key to corporate business is making the remote access as easy to access and use as the corporate network, with additional capabilities to support more than just the traditional data devices.

Traditionally, companies use to connect with branch offices using Wide Area Networks. WANs connect many LANs situated in many disparate offices. The installation of LANs and WANs is expensive. This is in addition to security issues that are introduced. The advent of internet and the many associated benefits it has brought about has made it easy to connect via VPNs –run over the internet and achieve privacy, as well as, enhanced connectivity.

OPERATING SYSTEM

The organization requires deploying Windows Server 2012 on the main location as well as five remote locations. In order to achieve these objectives, it will choose between Windows Server 2012 Datacenter and Standard versions. This is because Windows Server 2012 Datacenter and Windows server 2012 standard are the most fully functional editions of Windows Server 2012. They operate in almost the same processor and memory support features and functionality. The only difference is that they run on a diverse number of virtual machines, but no additional license cost is incurred from Microsoft. Datacenter Edition is meant for virtualization and private cloud deployment. Virtualization and cloud computing are undoubtedly the new front desired by every vendor in the market. It offers efficiency in performance and minimal resource consumption. The standard Edition is applicable for hosting and physical server deployment with minimal virtualization. The standard license entitles the user to run up to two virtual machines on a maximum of two processors.

VPN

VPN provides a host of upsides in an organization. Its implementation in SAN will guarantee security as well as performance. VPN connects via Internet to the outside world securing the internet traffic and the corporate assets of the organization. Most of the VPN networks are encrypted so that computers and other devices communicate with them through encrypted channels. Employees in all the branches will be able to access the network resources such as files, applications, and printers through local area networks without compromising on the security and privacy. The LANs will be connected to the WAN, and the VPN to concentrate all the servers and other networked resources among them all.

VPN provides advanced connectivity between disparate organizations branches over the Internet. The site-to-site connections and the ability to transfer data faster than WANs make it more preferable in instances such as those of SAN.

VPN SECURITY

Advances in internet features and technologies such as Quality of Service, network performance and cheap technologies have made it possible to achieve a range of services via the internet. Virtual Private Networks is one of them. VPN Internet Protocol security IPSec is one complete, safe and commercial feature developed to aid the transportation of data. In a VPN network, the data is segmented so that the intended recipient receives the data alone. Encryption technologies are used abundantly to safeguard the passage of data across the network. The implementation of IPSec based VPN, for instance in the organization will enhance the networks resistance to data attackers, tampering or theft. IPSec can be deployed over the Internet or MPLS with the former being ubiquitously cheaper. Internet has become a global presence utility that needs to be utilized. Implementing the VPN through the internet will add safety, interoperability between the individual SAN branches as well as quick and efficient services. Above all, it will empower SAN to extend their network services to all branches and remote partners and suppliers. Travelling employees, telecommuters and strategic partners will be in contact with the company all the way.

The nature of contracts SAN executes is of top priority in terms of security. The internet is also a public network that is susceptible to all manner of attacks. As a result, the implementation of a VPN network needs strong security credentials to prevent unwelcome access to the network and subsequent compromise. SAN values the security of its resources and data and endeavors to provide the same degree of safety when it comes to internet. The unfortunate fact is that the transmission of data from one branch to the other or from the headquarters involves more than 30 server located at different locations. The magnitude of vulnerabilities increases at the level involving so many preying eyes. The data should, therefore, be encrypted before it is delivered and subsequently decrypted at the destination.

DATA ENCRYPTION

With the involvement of security agency’s contracts such and those with Department of Defense, data privacy is of principal concern. Without an explicit method to conceal the data en route over the internet, its privacy will be compromised. Data transmitted in public networks such as the internet exist in clear text format. It can, therefore, be viewed or stolen using sniffing programs that monitor its convergence over the network. Unencrypted data transmitted over a network may display IP headers containing IP addresses of the sender and the receiver. Hackers can capture such information and use it for future attacks among other things.

It is, therefore, paramount that VPN network use encryption techniques to prevent valuable data against man-in-the-middle attacks. Encryption techniques scramble the clear text format into cipher text that cannot be deciphered by the attacker. The cipher text is transmitted to the recipient who, in turn decrypts the cipher text to clear format (Hooper, 2012).

VPN server file configurations contain the setting details within its memory. They also, simultaneously, save them to disk settings VPN configuration files are similar to windows registry files and are provided in an excellent configuration data format.

Config files are created under the file name " vpn_SANserver. config" located in the same directory as VPN s server processes executable files. The config settings are saved in any instance the VPN server settings are changed, or its internal structure is modified. The VPN server reads the contents of the vpn_server. config when booted and returns them to the initial values prior to termination. Thus, the config settings will allow the structural settings of the VPN to be restored to the initial state prior to booting regardless of when it was shut down. In case the configuration settings are not available on the disk when the VPN server is launched, default settings are used .

DISK QUOTA INFORMATION

Disk quota implementation is managed through the File Server Resource Manager templates. SA custom quota will be created for each branch of the SAN business as well as the headquarters. Through file screen management, certain types of information can be stored while others can be restricted from being saved in certain locations. For instance, employees would be restricted from uploading some kinds of files in the servers such as music files. File screens prevent saving of some authorized files in the servers. The server administrators are tasked with determining the files to be accommodated. Other disk management practices available to server administrators include disk usage monitoring, warning and usage enforcement.

Disk quota configurations are achieved through a per-volume basis. This is where production and engineering departments will be allocated more space as compared to sales and accounting departments.

VPN DATA BACKUPS AND DISASTER RECOVERY

Including a VPN in a data backup, and disaster recovery plan is beneficial as it safeguards the availability of SAN data. SAN will set up backup service designed to provide employees with secure data backup from remote locations. The backup services are limited to the SAN VPN network in order to ensure that backups and restore are strategically completed in a timely manner. The organization provides backup and restores functionality globally via the VPN service primarily intended for each branch of business and telecommuting employees. A customized solution known as SAN VPN client is installed on employee computers together with a login account for each user. The solution will provide backup of daily activities in servers located at strategic locations outside the organizations premises. The System Administrators in each branch will advise on the configuration settings for each location as per workload capacity .

VPN allows users to log in remotely and continue to serve the customers as if they are working at their branch office. Currently, the company uses

Windows 2012, and Linux servers that best implements IPSec VPN hence their choice for backup and restoration in case of uncertainties. IPSec provides an excellent enterprise routing equipment and public facing servers that give VPN a distinct competitive advantage. IPSec capable router permits the establishments of failover strategies with excellent levels of availability and redundancy.

DNS CONFIGURATION

The intranet resources can be accessed by the VPN clients using the names http://branchname/SAN. net. Name resolution can be achieved through DNS based resolution using the IPv4. DNS based resolution, as well as windows based resolution, require the server address to be provisioned on the VPN client. DNS server resolution will allow both IPv4 and IPv6 based network. The IP address of the DNS based server is located at the VPN client through static configuration inside the VPN client or dynamic configuration from the VPN server. Dynamic configuration will enable the handshake process to be initiated through the IKEv2 based VPN reconnect and is thus recommended in this case. IKEv2 based tunnel DNS servers IPv4 and IPv6 address is picked from the VPN server private interface and passed through the IKEv2 tunnel establishment phase.

SAN Network diagram

DATABASES

With the use of a relational data warehouse, analyzing data for the purpose of providing insightful decisions becomes simplified. The support tools associated with a warehouse provide a means to convert raw data into operational data. Thus, a data warehouse is more superior to management information systems and decision support systems.

References

Carvalho, L. (2012). Windows Server 2012 Hyper-V Cookbook. Packt Publishing Ltd.

Gary B. Shelly, T. J. (2010). Systems analysis and design. Cengage Learning.

Jose Garrido, R. S. (2011). Principles of Modern Operating Systems. Jones & Bartlett Publishers,.

Ralph Stair, G. R. (2011). Principles of information systems. . Cengage Learning.

System. (2010). Network and System Sciences , . International Journal of Communications , 815-824.