WAN Encryption

Soumen Maity

A Prospectus Presented to the Information Technology College Faculty
of Western Governors University
in Partial Fulfillment of the Requirements for the Degree
Master of Science in Cybersecurity and Information Assurance

07/16/2017

Abstract

ACME is a small-sized financial services company based in South Carolina. The headquarter is located in Columbia, and other branch offices are situated in Charleston, Greenville, Florence, and Orangeburg. The data center is located in headquarter, and it has one 100 Mbps Internet link and one 10 Mbps MPLS (Multiprotocol Label Switching) host link for branch office WAN (Wide Area Network) connectivity. All the branches are connected with the data center using 1.5 Mbps service provider's MPLS T1 link. Also, all the branches are accessing the Internet services through the headquarter data center Internet link. The data transmission over the MPLS link is an unencrypted plain text communication. The current MPLS technology for the organization does not provide the data encryption over the WAN link (Haran V., 2012). Due to this, there is a huge risk involved in data security and unauthorized capturing of data over the MPLS link. Nowadays they are losing their business because of several cyber-attacks like Man-in-the-middle attack, IP spoofing attacks from their competitors and disgruntled employees. Due to the dropping of the business performances, the management team is planning to cut the IT budget for the organization.

Therefore, the IT department has decided to implement the cost-effective, data encryption technology for branch offices WAN connectivity with enhancing performances. The best cost effective solution for addressing this issue is the replacement of expensive MPLS link with a low-cost Internet connection and WAN traffic encryption over the Internet link (Gottlieb A., 2012). The WAN encryption will be deployed by implementing the virtual private network (VPN) technology using the existing IT setups. As the current WAN infrastructures are based on Cisco routers, so the IT department has decided to deploy Dynamic Multipoint VPN (DMVPN)

without any expenses. The DMVPN is a Cisco IOS (Internetwork Operating System) software-based solution for building scalable IPsec VPNs.

The WAN encryption project will be delivered the value-added data encryption security for branch offices communications using the existing IT setups and low-cost Internet link. The research methodology used to investigate the problem included with the vulnerability assessment, security audit of the network and interview with the management. The project will be implemented using the four major phases as initiation, planning, execution and control, and project closer, which referred to as the project "life cycle." Each stage has specific steps and associated activities. While the stages, steps, and actions suggest a linear sequence of events, in the real execution there is often an additional dynamic flow to the work. Some stages or steps may be co-occurring, and the work often circles back to revisit earlier phases. The outcome of this project will be WAN data encryption over the low-cost Internet connection for cost efficient and enhanced secure solution.

Table of Contents

Introduction

Security is a critical factor in any network. Typically, data transfer between branch offices and corporate headquarters occurs over the service provider (SP) network or the Internet. In this capstone project, a small-sized financial services company ACME has four branch offices in South Carolina. The headquarter situated in Columbia, and other branch offices located in Charleston, Greenville, Florence, and Orangeburg. The data center is located in headquarter, and it has one 100 Mbps Internet link and one 10 Mbps MPLS host link for branch office connection. All the branches have 1.5 Mbps MPLS connection for data center connectivity. Also, all the branches are accessing the Internet services through the data center Internet link. The existing MPLS technology for the organization does not provide the data encryption facilities over the WAN link (Haran V., 2012). Due to clear text communication over the WAN link, there is a huge security risk involved in data communication and unauthorized access of data. Nowadays they are losing their business because of several cyber-attacks like Man-in-the-middle attack, IP spoofing attacks from their competitors and disgruntled employees. Because of the unexpectedly poor business performances, the management team is planning to cut off the IT budget for the corporation.

Therefore, after discussion with the directorate, the IT department has decided to implement the cost-effective, data encryption technology for branch offices WAN connection with improved performances. The best cost effective solution for addressing this issue is the replacement of expensive MPLS link with a low-cost Internet connection and WAN traffic encryption over the Internet link (Gottlieb A., 2012). A VPN is a corporate's private network that uses a public network like Internet to connect remote locations together. It uses "virtual" network connections routed over the Internet from the corporate's private network to the remote locations

(Cisco, 2008). The current WAN infrastructures of the organization are based on Cisco routers, so the IT department has decided to deploy Cisco DMVPN without additional costs. The proposed DMVPN is a Cisco IOS software-based solution for building scalable IPsec VPNs. The IT department can implement the same Cisco DMVPN over the MPLS link. But the MPLS is more expensive compared to the Internet (Gottlieb A., 2012). So the IT department has decided to implement DMVPN over the public Internet link for WAN traffic encryption. Also, the IT department has decided to deploy this solution by using the in-house IT staffs. By implementing the WAN encryption project, the IT department will provide secure value-added encryption for branch offices communications using the existing IT infrastructures and low-cost Internet link.

Project Scope

WAN security will protect all the traffic from possible external threats. VPN is a security technique that creates a safe and encrypted network connection over a less secured or public network, such as the Internet (Rouse M., 2016). This WAN encryption capstone project has two central goals. The first goal is WAN encryption with secure authentication for protecting all traffic from external threats and the second goal is the cost effective solution. This project will tackle the implementation of WAN encryption for the organization from start to finish. First of all, a systematic cost-benefit analysis (CBA) between the MPLS link and the Internet link will be performed to estimate the strengths and flaws of the alternatives. Second, the new Internet links need to be procured for all four branch offices which will replace the existing expensive MPLS links. The current Internet connection of headquarter will be reused for this project. Third, a company policy on WAN traffic encryption and authentication along with the statement of understanding and configuration to confirm the WAN encryption security. The internal resources will deploy this project. Fourth, building prototype model in GNS3 network simulator for testing and development. Fifth, Installation and testing new Internet connection in all four branch office locations. Sixth, notify all related stakeholders for significant downtime to deploy this solution. Seventh,

network devices will be configured according to the design documents, and penetration test will be conducted for certifying that WAN encryption.

Project Rationale

No business is entirely safe from the security vulnerabilities. According to Small Business Trends, 43% of cyber security attacks target small businesses (Sophy J., 2016). While larger enterprises are spending more money on cybersecurity, the smaller companies seem to be investing less. As per the “Global State of Information Security Survey 2015," small businesses (those with annual revenues of less than $100 million), cut security expenditure by 20 percent in 2014, while medium and large enterprises increased security investments by 5 percent (PwC, 2014). Most of the small firms have a shortage of budget to procure new network devices or spend additional money for other security measures which found in larger organizations. Because of less funding available for IT security, the hackers will heighten the rate of hacking attempt to interrupt the small business systems for data theft. Typically the small organization doesn't put IT security on the top of the priority list until it is too late.

The primary purpose of this project is executing the cost-effective WAN encryption for securing the WAN traffic from external threats without spending extra money. Currently, the data center at headquarter have 10 Mbps MPLS host link, and all four branch offices have 1.5 Mbps MPLS connection for data communication. The existing WAN network infrastructure comprises with one Cisco 3945-SEC/K9 Integrated Services Router in the data center, and all four branches have Cisco 2911-SEC/K9 Integrated Services Router. Hence, existing WAN infrastructures of the corporation are based on Cisco Integrated Services router, so the IT department has decided to deploy Cisco DMVPN using the current hardware setup. The DMVPN is a Cisco IOS software-based solution for building scalable IPsec VPNs. The IT department can implement the same Cisco DMVPN over the MPLS link. But the MPLS is very

costly compared to the Internet (Gottlieb A., 2012). Therefore, the IT department has decided to implement DMVPN over the public Internet link for WAN traffic encryption. After applying this scalable WAN encryption project, the IT department will deliver the value-added data encryption for branch offices communications using the current WAN infrastructures and low-cost Internet link.

Problem Summary

Nowadays the security is becoming a critical issue in any organization. Usually, the data transfer between branch offices and business headquarter happens through a service provider network or the Internet. In this capstone project, a small-sized financial services company has four branch offices in South Carolina. Headquarter is located in Columbia, and other branch offices are situated in Charleston, Greenville, Florence, and Orangeburg. The data center is providing the Internet services to all departments and branch offices. The data center at headquarter has one 100 Mbps Internet link and one 10 Mbps MPLS host link for branch office communication. All the branches have 1.5 Mbps MPLS connection for data center connectivity. The current MPLS technology for the organization does not support data encryption over the WAN link. Due to the clear text communication over the WAN link, there is a huge risk involved in data security and unauthorized data access. Currently, they are losing their business because of several cyber-attacks like Man-in-the-middle attack, IP spoofing attacks from their competitors and disgruntled employees. Because of the sinking of the company performances, the management team is planning to reduce the IT budget. Therefore, the IT department has decided to implement the cost-effective, data encryption technology for branch offices WAN connectivity with enhanced performances.

The best cost effective solution is the replacing of expensive MPLS link with a low-cost Internet connection with WAN traffic encryption by implementing the DMVPN technology over the Internet link. The VPN is a corporate's private network that uses a public network like Internet to connect remote locations together. It uses "virtual" network connections routed over the Internet from the corporate's private network to the remote locations. The current WAN infrastructures are based on Cisco routers, so the IT department has decided to deploy Cisco DMVPN without additional cost involved for materials purchases. The DMVPN is a Cisco IOS software-based solution for building scalable IPsec VPNs. The IT department can implement the same Cisco DMVPN over the MPLS link. But the MPLS is very expensive compared to the Internet, so the IT department has decided to implement DMVPN over the public Internet connection for WAN traffic encryption.

Problem Background

Data security is essential for all kind of organizations. The employees’ data, client information, bank account details, payment information, all of these data can be hard to change and most dangerous if it falls into the wrong hands like cyber criminals. These vital details should be protected at all times to confirm the integrity and confidentiality of the critical business records. This information is the core for the corporation, and without it, the business can't run. If a criminal can access this data, there is no limit to the damage they can inflict. The confidentiality, availability, and integrity of the critical data are crucial for data security. The data security or protection is all about the processes and practices that are in place to confirm data isn't being accessed or used by unauthorized parties or individuals. The data protection assures that the data is correct and reliable and is available when those with authorized access need it.

For any commercial establishments, data security is not only an enterprise option; it's the law. Losing sensitive business data by way of physical theft can have severe penalties on a company, possibly crippling the entire business. While there are several different security techniques, data encryption is perhaps the most useful regarding protecting confidential data. Therefore it is essential to encrypt business communication and business-critical data to keep the data secure and decrease the risks of all kinds of Internet eavesdropping. The WAN Encryption service enables secure site-to-site connections through the Internet, where all traffic between the sites will automatically encrypt and authenticated. The VPN is encrypted and can be used to connect two networks together over the Internet, and the users can access remote resources securely and efficiently.

Need for the Solution

Cyber-crime in the form of hacking, business espionage, and even cyberterrorism, is on the increase. Information security threats remain usual, and there is a growing emphasis on businesses of all types to confirm the integrity and security of their data, both at in data center location and in motion through LAN or WAN environment. The VPN connection achieves two scientific results. First, VPN encrypts all WAN traffic and making all activity completely illegible to any eavesdroppers, and second, VPN manipulates the original private IP address with the public WAN IP address which makes WAN communication hide from the public network. Implementing WAN encryption by deploying the VPN into the organization can contribute to the achievement of business objectives in several ways.

First of all, it significantly reduces the risk of security breaches and cyber attacks and improves the security for data exchanges, and if hackers capture the encrypted data, it will not be readable or understandable to the hackers. The VPN offers a much higher level of protected wide area network communication because of advanced technologies that are used to secure the network from unauthorized user access. Second, it’s eliminating the need for expensive recurring MPLS link cost and support costs which will help to the management for reducing the IT budget. Third, the functionality and resources will

be shared with a corporate head office to all remote locations' employees. Fourth, it encourages productivity of employees that work via virtual workplaces because of better WAN performances and enhanced security. Fifth, data encryption make the customers feel secure as their data are protected from unauthorized access, and it will soothe their worries. Sixth, the Cisco DMVPN are very flexible regarding growing the business and adding new remote locations. The configuration scalability of Cisco DMVPN allows the organization to new remote location without having much configuration changes to accommodate the growth.

Reason for Approach

The WAN encryption capstone project has two crucial goals as WAN encryption with secure authentication for protecting all traffic from external threats, and it should be cost-effective without additional expenditures. If the organization has not deployed the WAN encryption by using the VPN for data transmission over a service provider (SP) network or the Internet, the business goals will be impacted in several ways. First of all, the WAN encryption will protect all the WAN traffic from potential external threats in less secure or public network, such as the Internet. If it is not implementing the risk of security breaches and cyber attacks will be increased, and if the hackers capture the unencrypted clear text data, it will be readable to the hackers very easily. Second, the WAN encryption by deploying VPN can implement over the low-cost Internet link which will remove the expensive MPLS link cost using the existing Cisco WAN infrastructure. So if the WAN encryption is not deploying the present security risk and cyber attacks over the expensive MPLS connection will not eliminate, and the business will be impacted more. Third, if the WAN encryption is not implementing the functionality and resources of the private corporate network will not be shared with the remote locations' employees easily. Fourth, if WAN encryption is not applying the customers will be worried about the sharing of their details, bank information, and social security number because it is most

dangerous if it falls into the wrong hands. Fifth, if WAN encryption is not implemented the growth of business and adding new remote locations, i.e., the business expansion will be very tough because of business data security and cyber attacks.

The secure encrypted VPN can easily be built on top of both MPLS link and the Internet link for all companies to protected their traffic across any connection. But the WAN using MPLS link is very costly for any small organization. In the United States, the typical pricing ranges for a DS-1/T-1 MPLS connection will come with a list price of anywhere from $750 to $1000 per month – which is $585 per Mbps, compared to $2-$10 of the broadband Internet links. By way of explanation, the MPLS is 100 times more costly per Megabit delivered compared to other business class connectivity options (Akin Cahit, 2015).

Prospectus Organization

Till now the prospectus document presents an outline of the WAN project, the scope, why we select this project, the problem summary, problem background, need for the solution, and the reason why the proposed approach is selected for this project. The rest of the prospectus will contain the problem statement that summarizes the problem declaration of the business, which details the background information, causes, business impacts analysis for selecting the WAN encryption by deploying the cost effective Cisco VMVPN project. A cost-benefit analysis, risk analysis, assumptions, and limitations of the proposed solution will be presented to support that reusing the existing WAN infrastructure is sufficient for deploying the enhanced WAN encryption solution over the Internet link instead of using the expensive MPLS link. The technical terms related to WAN encryption by implementing the Cisco DMVPN will be described. And finally, in the technology solution section, it will be explained the reasons for selecting this technology solution.

Problem Statement

Security is a critical factor in any network. Typically, data transfer between branch offices and corporate headquarters occurs over a service provider (SP) network or the Internet. In this capstone project, a small-sized financial services company ACME have four branch offices in South Carolina. The headquarter situated in Columbia, and other branch offices located in Charleston, Greenville, Florence, and Orangeburg. Also, all the branches are accessing the Internet services through the headquarter data center Internet link. The current MPLS technology for the organization does not provide the data encryption over the WAN link. Due to the clear text communication over the WAN link, there is a huge risk involved in data security and unauthorized access of data. Nowadays they are losing their business because of several cyber-attacks like Man-in-the-middle attack, IP spoofing attacks from their competitors and disgruntled employees. Due to the dropping of the company performances, the management team is planning to cut the IT budget for the organization and ask IT department for cost effective substitute enhanced solution without spending additional expenses.

Background Information

According to the survey in late 2015 revealed that eight out of ten small businesses don't have the first level of cyber attack response plan, even though cyber crimes hit a majority (MacDonald E., 2016). Also, as per Department of Justice's Internet Crime Complaint Center recorded 269,422 cyber security related complaints in 2014 report which is an exponential upturn of over 1500% from 2000 (MacDonald E., 2016). The cyber criminals are targeting small businesses more than ever before. The hackers steal small business information to do things like rob bank accounts via wire transfers; file for fraudulent tax refunds; take customers' identity information; commit health insurance or Medicare fraud. The attackers can also hijack a small

company's website to hack other information in small enterprises. That is the way it is critical to protecting the employee and client information, bank account details, payment information, all of these data from wrong hands. By implementing the WAN encryption it will reduce the risk of security breaches and cyber attacks and improves the security for data exchanges, and if hackers capture the encrypted data, it will not be readable or understandable to the hackers. The VPN offers a much higher level of protected wide area network communication because of advanced technologies that are used to secure the network from unauthorized user access. That is why it is important to deploy a cost-effective WAN encryption for securing the WAN traffic from external threats without spending additional money.

The secure encrypted VPN can easily be built on top of both MPLS link and the Internet link for all companies to protect their traffic across any connection. But the WAN using MPLS link is very costly for any small organization. In the United States, the typical pricing ranges for a DS-1/T-1 MPLS connection will come with a list price of anywhere from $750 to $1000 per month – which is $585 per Mbps, compared to $2-$10 of the broadband Internet links. By way of explanation, the MPLS is 100 times more costly per Megabit delivered compared to other business class connectivity options (Akin Cahit, 2015).

Causes

Typically, data transfer between branch offices and corporate headquarters occurs over a service provider (SP) network or the Internet. So the WAN security is a highly important factor in any business. Encryption is the process of changing information in such a way as to make it unreadable to anybody except those possessing special knowledge (typically denoted to as a "key") which allows them to change all the information back to its original and readable format.

The encryption is essential because it allows the organization to protect their data securely. This method, even if the data is stolen, it will be safe.

Although the WAN encryption delivers the value-added data encryption security for WAN communications using the existing IT infrastructures and low-cost Internet link, some restrictions need to be aware of. The business that wants to deploy the VPN has to confirm that adopting or considering the VPN is the best option for them. The design and security employment for a VPN can be complicated. That means it needs a professional with a high level of knowledge and understanding for VPN configuration and can address any issue during the VPN implementation. For a small organization getting great skills expert with adequate experience in networking and security is a difficult task. Also for managing and troubleshooting of the VPN requires excellent skills. It's firm's responsibilities that they should have enough resources before implementing the VPN technology into business. The performance and reliability of the VPN can become a factor depending on the service provider that the organization is selecting for WAN communication. If the VPN is implemented using the Internet link, it is essential to work with the service provider for minimal guaranteed downtime.

If it occurs to be needed to create an additional setup, the existing solutions can become mismatched and cause technical issues if the organization use a different product vendor than the business used for the original current installation. In this project, the IT team will be using the existing Cisco infrastructure for WAN encryption. Hence if the organization wants to extend their corporate network in any new location, they need to use the same Cisco setup for WAN connectivity

Business Impacts

While MPLS technology provided a WAN connection between the physical locations, it was still costly and required constant maintenance. The secure encrypted VPN can easily be built on top of both MPLS link and the Internet link for all companies to protect their traffic across any connection. But the WAN using MPLS link is very costly for any small organization. In the United States, the typical pricing ranges for a DS-1/T-1 MPLS connection will come with a list price of anywhere from $750 to $1000 per month – which is $585 per Mbps, compared to $2-$10 of the broadband Internet links. By way of explanation, the MPLS is 100 times more costly per Megabit delivered compared to other business class connectivity options (Akin Cahit, 2015).

The existing MPLS technology for the organization does not provide the data encryption facilities over the WAN link (Haran V., 2012). Due to clear text communication over the WAN link, there is a huge security risk involved in data communication and unauthorized access of data. Nowadays they are losing their business because of several cyber-attacks like Man-in-the-middle attack, IP spoofing attacks from their competitors and disgruntled employees. Because of the unexpectedly poor business performances, the management team is planning to cut off the IT budget for the corporation.

Therefore, after discussion with the directorate, the IT department has decided to implement the cost-effective, data encryption technology for branch offices WAN connection with improved performances. The best cost effective solution for addressing this issue is the replacement of expensive MPLS link with a low-cost Internet connection and WAN traffic encryption over the Internet link (Gottlieb A., 2012). A VPN is a corporate's private network that uses a public network like Internet to connect remote locations together. It uses "virtual" network connections routed over the Internet from the corporate's private network to the remote locations

(Cisco, 2008). The current WAN infrastructures of the organization are based on Cisco routers, so the IT department has decided to deploy Cisco DMVPN without additional costs. The proposed DMVPN is a Cisco IOS software-based solution for building scalable IPsec VPNs. The IT department can implement the same Cisco DMVPN over the MPLS link. But the MPLS is more expensive compared to the Internet (Gottlieb A., 2012). So the IT department has decided to implement DMVPN over the public Internet link for WAN traffic encryption. Also, the IT department has decided to deploy this solution by using the in-house IT staffs. By implementing the WAN encryption project, the IT department will provide secure value-added encryption for branch offices communications using the existing IT infrastructures and low-cost Internet link.

Cost Analysis

The cost benefit analysis is a systematic procedure for estimating all costs involved and possible profits to be derived from the alternatives. It is a quick and straightforward technique that the organization used for non-critical financial decisions. It has four steps by which the IT department perform the cost benefit analysis for this project as:

1. Brainstorm Costs and Benefits: First of all, the IT department should analyze all expenses related to this WAN encryption project, and make a list of all items. Then, continue the same process for all of the benefits of the project.
2. Assign a Monetary Value to the Costs: The costs include the costs of hardware resources needed, the Internet link cost, as well as the expense of the installation and deployment human workforce cost involved in all phases of a project.
3. Assign a Monetary Value to the Benefits: This phase is less straightforward than step two or assigns a monetary value to the costs! First of all, it's often complicated to forecast revenues correctly, especially for newly added services. Second, along with the financial

benefits, there are often intangible, or soft, benefits which are essential outcomes of this project.

4. Compare Costs and Benefits: At last finally, IT department should compare the value of the project costs to the value of profits, and use this analysis to decide the course of action. For this, the IT department has calculated total costs and with comprehensive benefits, and compare the two values to determine whether the advantages of this project outweigh the expenses.

In this WAN project, the IT department has decided they will be using the existing WAN infrastructures as Cisco routers and associated IOS software. Also, they are going to replace the expensive MPLS link with a low-cost broadband Internet connection. It was also decided that the in-house IT staffs will deploy this project and any additional support will be provided by Cisco Technical Assistance Center (TAC) team as they already have Cisco TAC support contract for all Cisco gears. Keeping all of these factors in mind below is the proposed cost breakdown for the WAN encryption project by deploying the Cisco DMVPN solution:

Costs					
Sr. No.	**Item Name**	**Description**	**Quantity**	**Each Cost**	**Total Cost @ Year**
1	Internet Link at Data Center	Existing Internet Link will be using	0	0	$0
2	Internet Link at Branches	4 Branch each with 50Mbps speed	4	Monthly $100.00	$4800.00
3	Hardware Cost	Existing Cisco Router will be using	0	0	$0
4	Manpower Cost	In-house IT resources will be using	0	0	$0
5	Configuration support Cost	Existing Cisco TAC support	0	0	$0
Total Cost for One Year					**$4800.00**

Benefits					
Sr. No.	**Item Name**	**Description**	**Quantity**	**Each Cost**	**Total Benefits @ Year**
1	Removing MPLS 1.5 Mbps Link from Branches	Removing 1.5 Mbps MPLS Link from 4 branches	4	Monthly $1000.00	$48000.00
Total Benefits from removing the MPLS link for One Year					**$48000.00**

The current MPLS link speed is T1 or 1.5 Mbps link. The IT department will be replacing the MPLS link with 50 Mbps Internet link. By replacing this, the IT department can save an enormous amount of $ 43200.00 (Forty-Three Thousand Two Hundred Dollars) for IT budget with better Internet bandwidth or better performances. Additionally, the secure WAN encryption will improve the productivity of the business and enhance the brand value of the company.

Risk Analysis

Although the WAN encryption delivers the value-added data encryption security for WAN communications using the existing IT infrastructures and low-cost Internet link, some restrictions need to be aware of. The business that wants to deploy the VPN has to confirm that adopting or considering the VPN is the best option for them.

The biggest risk to implementing the DMVPN for WAN encryption requires knowledgeable and skillful technical staffs. The design and security deployment for a VPN can be complicated. That means it needs a professional with a high level of knowledge and understanding for VPN configuration and can address any issue during the VPN implementation. For a small organization getting great skills expert with adequate experience in networking and security is a difficult task. Also for managing and troubleshooting of the VPN requires excellent

skills. It's firm's responsibilities that they should have enough resources before implementing the VPN technology into business. Also, VPN troubleshooting requires high skill and experiences.

The performance and reliability of the VPN can become a factor depending on the service provider that the organization is selecting for WAN communication. If the VPN is implemented using the Internet link, it is essential to work with the service provider for minimal guaranteed downtime.

If it occurs to be needed to create an additional setup, the existing solutions can become mismatched and cause technical issues if the organization use a different product vendor than the business used for the original current installation. In this project, the IT team will be using the existing Cisco infrastructure for WAN encryption. Hence if the organization wants to extend their corporate network in any new location, they need to use the same Cisco setup for WAN connectivity.

Assumptions

The primary hypothesis or assumption of this project is that the organization wants to implement WAN encryption using the Internet for securing the WAN traffic. Whereas the corporation already has MPLS link for WAN connectivity. The group is trying to configure the VPN for data encryption using the existing WAN infrastructures. Currently, all the branch network have G2series Cisco 2911-SEC/K9 Integrated Services Routers, and data center have G2series Cisco 3945-SEC/K9 Integrated Services Router. Also, all the routers have Cisco securityk9 IOS technology package software which supports DMVPN. As the current WAN infrastructures are based on Cisco routers, so the IT department has decided to deploy Cisco DMVPN without additional hardware and software investment. The DMVPN is a Cisco IOS software-based solution for building scalable IPsec VPNs. Another assumption is that the

Enhanced Interior Gateway Routing Protocol or EIGRP is using as a for automating routing decisions and configuration.network route selection procedures. The last assumption is that the internal IT staffs are enough skillful and knowledgeable so that they can able to deploy the data encryption project for WAN communication.

Limitations

Although the WAN encryption delivers the value-added data encryption security for WAN communications using the existing IT infrastructures and low-cost Internet link, some restrictions need to be aware of. The business that wants to deploy the VPN has to confirm that adopting or considering the VPN is the best option for them. The design and security employment for a VPN can be complicated. That means it needs a professional with a high level of knowledge and understanding for VPN configuration and can address any issue during the VPN implementation. For a small organization getting great skills expert with adequate experience in networking and security is a difficult task. Also for managing and troubleshooting of the VPN requires excellent skills. It's firm's responsibilities that they should have enough resources before implementing the VPN technology into business. The performance and reliability of the VPN can become a factor depending on the service provider that the organization is selecting for WAN communication. If the VPN is implemented using the Internet link, it is essential to work with the service provider for minimal guaranteed downtime.

If it occurs to be needed to create an additional setup, the existing solutions can become mismatched and cause technical issues if the organization use a different product vendor than the business used for the original current installation. In this project, the IT team will be using the existing Cisco infrastructure for WAN encryption. Hence if the organization wants to extend

their corporate network in any new location, they need to use the same Cisco setup for WAN connectivity.

Technical Terms

The technical terms are an important part of all scientific and technical writing. Each field and specialty usually use a vocabulary that relays a variety of technical concepts using its language.

- LAN - A local area network or LAN is an interconnected computer and associated devices within a limited area such as a university campus, office building.
- WAN - A wide area network or WAN is a geographically distributed private network over a service provider (SP) network.
- Router - A router is an ISO layer-3 or network layer device that evaluates the data packets contents to transmit within a network or to another network.
- Encryption - Encryption is the process of encoding the electronic data in such a way that only authorized parties can access it.
- VPN - A VPN or virtual private network is a private network that is built over a service provider (SP) network or the Internet.
- Site-to-site VPN - Site-to-site VPN is a type of VPN connection that is created between two geographically separate locations over the public Internet connection or a WAN connection.
- DMVPN - The DMVPN or Dynamic Multipoint VPN is a Cisco IOS software-based solution for building scalable IPsec VPNs. A DMVPN is a secure network that exchanges data between sites without needing to pass traffic through a corporate's headquarter VPN server.

- IKE - The IKE or Internet Key Exchange is a key management protocol standard which is used in combination with the Internet Protocol Security (IPSec) standard protocol.
- IP Sec - IPsec or Internet protocol security is a set of rules that ensure the safety of Internet Protocol. It can use cryptography to provide the security. IPsec can be utilized for the setting up of VPN securely.
- AH - The authentication header or AH authenticates the sender, and it discovers any changes in data during transmission.
- ESP - The ESP or encapsulating security payload is not only performed authentication for the sender but also encrypts the data being sent.
- Tunnel Mode - The tunnel mode will take the whole IP packet to form secure communication between two places or gateways.
- Transport Mode - The transport mode only encapsulates the IP payload, not the entire IP packet as in tunnel mode to confirm a secure channel of communication.
- IOS - Cisco IOS or Internetwork Operating System is a family of software used on most of all Cisco Systems routers and network switches.
- EIGRP - Enhanced Interior Gateway Routing Protocol or EIGRP is using as a for automating routing decisions and configuration.network route selection procedures. It's an advanced distance-vector routing protocol.
- MPLS - The MPLS or Multiprotocol Label Switching is a type of data-carrying technique or method for WAN communications.

Technology Solution

The business sensitive data is at risk not only at rest but also in transit means when it is communicated over the WAN link. In the new APT (advanced persistent threat) environment,

the unauthorized hackers gain access to a network and stay there undetected long time for steal the critical data. It is essential to encrypt the business communication and business critical data to keep the data safe and reduce the risks of others internet eavesdropping. The WAN Encryption service enables secure site-to-site connections through the service providers network like the Internet, where all WAN traffic between the locations will be automatically encrypted and authenticated. For further clarification the necessities of WAN encryption project, there will be an explanation of the business drivers, justification of business drivers, what would occur if WAN encryption will not deploy, and how this solution matches with the firm urgencies.

Business Drivers

The five primary drivers of small businesses are cash, profit, assets, growth, and people. The first business drive is cash which is the fuel of the corporate. Lack of money or cash any business can't run. The business should know about the generating of funds for running the business. The primary driver for any small business is profit. Without profit, the company can't run. The assets comprise everything a corporation uses to produce the revenue. Business growth or constant change is a certainty in today's business environment, and growth is one of the ways to handle it. The peoples are the center of the five key business drivers (Information Strategies, (2017). All these business parameters are relevant for business operation and development, but the end primary corporate drivers will turn around the economic or monetary setting.

Justification

The organization must operate with profit so that the investor should support the business and invest more. Nobody will spend any money on the firm if it has no return on the investment. The key to exploiting profit potential in a small business is to always look for efficiency gains and increase the revenue at a higher ratio than the costs. So for making the small business

profitable, it needs a high productivity and workforce ratio. Unproductive workforce always burdens for the company and its growth. The flexibility of the business will help to accumulate with the changing environment. Without the flexibility of the firm, it becomes immobile and can far behind the challenges in the industry. The business growth attracts more investors for investments in the business and opens more income opportunities. At last, it is critical that all assets into the operational requirements to be protected for avoiding the theft and legal procedures which may result in a loss instead of profit.

No Solution

If the organization has not deployed the WAN encryption by using the VPN for data transmission over a service provider (SP) network or the Internet, the business goals will be impacted in several ways. First of all, the WAN encryption will protect all the WAN traffic from potential external threats in less secure or public network, such as the Internet. If it is not implementing the risk of security breaches and cyber attacks will be increased, and if the hackers capture the unencrypted clear text data, it will be readable to the hackers very easily. Second, the WAN encryption by deploying VPN can implement over the low-cost Internet link which will remove the expensive MPLS link cost using the existing Cisco WAN infrastructure. So if the WAN encryption is not deploying the present security risk and cyber attacks over the expensive MPLS connection will not eliminate, and the business will be impacted more. Third, if the WAN encryption is not implementing the functionality and resources of the private corporate network will not be shared with the remote locations' employees easily. Fourth, if WAN encryption is not applying the customers will be worried about the sharing of their details, bank information, and social security number because it is most dangerous if it falls into the wrong hands. Fifth, if WAN encryption is not implemented the growth of business and adding new remote locations,

i.e., the business expansion will be very tough because of business data security and cyber attacks.

Solution

Implementing WAN encryption by deploying the VPN into the organization can contribute to the achievement of business objectives in several ways. First of all, it significantly reduces the risk of security breaches and cyber attacks and improves the security for data exchanges, and if hackers capture the encrypted data, it will not be readable or understandable to the hackers. The VPN offers a much higher level of protected wide area network communication because of advanced technologies that are used to secure the network from unauthorized user access. Second, it's eliminating the need for expensive recurring MPLS link cost and support costs which will help to the management for reducing the IT budget. Third, the functionality and resources will be shared with a corporate head office to all remote locations' employees. Fourth, it encourages productivity of employees that work via virtual workplaces because of better WAN performances and enhanced security. Fifth, data encryption make the customers feel secure as their data are protected from unauthorized access, and it will soothe their worries. Sixth, the Cisco DMVPN are very flexible regarding growing the business and adding new remote locations. The configuration scalability of Cisco DMVPN allows the organization to new remote location without having much configuration changes to accommodate the growth.

References

Akin Cahit, (2015), *What is the cost of MPLS?,* online https://www.mushroomnetworks.com/blog/2015/08/20/what-is-the-cost-of-mpls/

Cisco Systems, (2008), *How Virtual Private Networks Work, Document ID:14106*, online http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

Gottlieb A. (2012), *Next-generation Enterprise WANs*, online http://www.networkworld.com/article/2222196/cisco-subnet/why-does-mpls-cost-so-much-more-than-internet-connectivity-.html

Haran V. (2012), *Essar's WAN encryption strategy to secure data in motion: In focus*, online http://www.computerweekly.com/feature/Essars-WAN-encryption-strategy-to-secure-data-in-motion-In-focus

Information Strategies, (2017), *SMALL BUSINESS DIGEST*, online http://www.2sbdigest.com/Key-Drivers

MacDonald E., (2016), *Cyber Attacks on Small Businesses on the Rise*, online http://www.foxbusiness.com/features/2016/04/27/cyber-attacks-on-small-businesses-on-rise.html

PwC, (2014), *Managing cyber risks in an interconnected world Key findings from The Global State of Information Security® Survey 2015*, online http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

Rouse M.(2016), *virtual private network (VPN),* online http://searchnetworking.techtarget.com/definition/virtual-private-network

Sophy J. (2016), *43 Percent of Cyber Attacks Target Small Business*, online

https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html