WAN Encryption

Soumen Maity

A Capstone 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

07/24/2017

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. Also earlier they had one 10 Mbps MPLS (Multiprotocol Label Switching) host link for branch office WAN (Wide Area Network) connection. All the branches were connected with the data center using 1.5 Mbps service provider's MPLS T1 link. In addition, all the branches were accessing the Internet services through the headquarter data center Internet link. The data transmission over the MPLS link was unencrypted plain text communication. The old MPLS technology for the organization was not delivered the data encryption over the WAN link (Haran V., 2012). Due to this, there was a huge risk involved in data security and unauthorized capturing of data over the MPLS link. They were losing their business due to severe 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 was planning to cut off the IT budget for the corporation.

Therefore, the IT department had decided to implement the cost-effective, data encryption for branch offices WAN connectivity with enhanced performances. The best cost effective solution for addressing this issue was 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 was deployed by implementing the virtual private network (VPN) technology using the existing IT setups. As the WAN infrastructures were are based on Cisco routers, so the IT department had decided to deploy Dynamic Multipoint VPN (DMVPN)

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

The WAN encryption project was 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 was 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 had specific steps and associated activities. While the stages, steps, and actions suggest a linear sequence of events, in the real execution there was often an additional dynamic flow to the work. Some stages or steps may be co-occurring, and the work often circles back to revisit the earlier phases. The outcome of this project was WAN data encryption over the low-cost Internet link 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. Earlier the data center had another 10 Mbps MPLS host link for branch office connectivity. All the branches were connected with the data center through the 1.5 Mbps MPLS link. The MPLS data communication was unencrypted data communication (Haran V., 2012). Due to the clear text unencrypted data transmission over the WAN link, there was a huge security risk involved for WAN communication. They were losing their business due to severe 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 was planning to cut off the IT budget for the corporation.

Therefore, after discussion with the directorate, the IT department had decided to implement the cost-effective, data encryption technology for branch offices WAN connection with improved performances. The best cost effective solution for addressing those issues was 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 WAN infrastructures of the organization were based on Cisco routers, so the IT department had decided to deploy Cisco DMVPN without additional hardware costs. The

DMVPN is Cisco IOS software-based solution for building scalable IPsec VPNs. The IT department was analyzed that they may implement the same Cisco DMVPN over the MPLS link, but the MPLS is more expensive compared to the Internet link (Gottlieb A., 2012). Therefore, the IT department had decided to implement DMVPN over the public Internet connection for WAN traffic encryption. Also, the IT department had decided to deploy this solution by using the in-house IT staffs. By implemented the WAN encryption project, the IT department had delivered secured 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 had two central goals. The first goal was WAN encryption with secure authentication for protecting all traffic from external threats and the second goal was the cost effective solution. This project has tackled the implementation of WAN encryption for the organization from start to finish. First, a systematic cost-benefit analysis (CBA) between the MPLS link and the Internet link was performed to estimate the strengths and flaws of the alternatives. Second, the new Internet links were procured for all four-branch offices, which replaced the expensive MPLS links. The existing Internet connection of headquarter was reused for this project. Third, a company policy on WAN traffic encryption and authentication along with the statement of understanding and configuration was confirmed the WAN encryption security. The internal resources were deployed this project. Fourth, built prototype model in GNS3 network simulator for testing and development. Fifth, Installation and testing of new Internet connection were performed in all four-branch office locations. Sixth, notified all related stakeholders for significant downtime to the deployment of this solution. Seventh, network devices were configured according to the design documents, and penetration test was performed for certifying that WAN encryption.

Defense of the Solution

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 does not put IT security on the top of the priority list until it is too late.

The primary purpose of this project was to execute the cost-effective WAN encryption for securing the WAN traffic from external threats without spending extra money. The data center at headquarter had 10 Mbps MPLS host link, and all four branch offices were connected through 1.5 Mbps MPLS link. The WAN network infrastructure comprises with one Cisco 3945-SEC/K9 Integrated Services Router in the data center, and all four branches had Cisco 2911-SEC/K9 Integrated Services Router. The IT department had decided to deploy Cisco DMVPN using the existing hardware setup. The DMVPN is a Cisco IOS software-based solution for building scalable IPsec VPNs. The IT department was analyzed that they may implement the same Cisco DMVPN over the MPLS link, but the MPLS is more expensive compared to the Internet link (Gottlieb A., 2012). The best cost effective solution for addressing those issues was 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). Also, the IT department had decided to deploy this solution by using the in-house IT staffs. By implemented the WAN encryption project, the IT department had delivered secured value-added encryption for branch offices communications using the existing IT infrastructures and low-cost Internet link.

Methodology Justification

The research method used to investigate the problem included with the vulnerability assessment, security audit of the network and interview with the management. The project was 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 had concrete steps and associated activities. ACME Corporation had Cisco 3945-SEC/K9 router in the data center and Cisco 2911-SEC/K9 routers in all four branch offices. All routers were running with Cisco securityk9 IOS technology package, which was suitable for DMVPN implementation. Enhanced Interior Gateway Routing Protocol is using as the primary routing protocol for network traffic routing. As the communication over MPLS link was unsecured plain text communication, there was a security risk of data safety and unauthorized data capture over WAN link. There was no current solution exist which can secure this data communication over the WAN.

Before DMVPN deployment in a production environment, the solution was properly evaluated and analyzed. The test and development environment for implementing DMVPN was in a GNS3 network simulator. The GNS3 was a free graphical network simulator. It was capable of emulating some network devices like Cisco routers, switches, firewall, and servers (Gns3,

ND). This simulator prototype was installed in Windows 7 laptop for test and development. The 'Cisco securityk9 IOS technology package' evaluation license was used for the test environment. This evaluation license was valid for 30days. After performing the performance and security testing in GNS3 simulator, the test result was documented for analysis and outcome. Finally, the tested configuration was applied in a production environment.

Organization of the Capstone Report

Until now, the capstone report presents an outline of the WAN project, the scope, why we select this project with the reason why the proposed approach is chosen for this project, the methodology of the project. The rest of the project will continue as follows:

1. Systems and Process Audit
2. Detailed and Function Requirements
3. Project Design
4. Methodology
5. Project Development
6. Quality Assurance
7. Implementation Plan
8. Risk Assessment
9. Post-Implementation Support and Issues
10. Conclusions, Outcomes, and Reflection
11. Three appendices are attached as well:

- Appendix A: Network diagram
- Appendix B: Implementation Configuration Document
- Appendix C: Test and Verification

Systems and Process Audit

A system audit is an assessment or review of a system or process in contradiction of system requirements. It can disclose conformity or nonconformity to the network. A process audit is an audit of individual processes against predetermined process steps or activities. It can reveal incompetence and areas for improvement. In the WAN encryption project was 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 was 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 had specific steps and associated activities. While the stages, steps, and actions suggest a linear sequence of events, in the real execution there was often an additional dynamic flow to the work. Some stages or steps may be co-occurring, and the work often circles back to revisit the earlier phases. The outcome of this project was WAN data encryption over the low-cost Internet link for cost efficient and enhanced secure solution.

Audit Details

The systems and processes review, which was directed to support this, WAN encryption project comprised of two areas: an assessment of the current WAN data security practice, and an assessment of the cost effective WAN solution by replacing expensive MPLS link with the low-cost Internet link. The possibility of the systems and processes audit comprised the WAN data security by confidentiality, integrity, and availability. The MPLS technology for the organization was not delivered the data encryption facilities over the WAN link (Haran V., 2012). Due to clear text communication over the WAN link, there was a huge security risk involved in data

communication and unauthorized access of data. They were 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 was planning to cut off the IT budget for the corporation.

While MPLS technology provided a WAN connection between the remote locations and data center, 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. However, the WAN using MPLS link was very costly for the small organization. In the United States, the average pricing ranges for a DS-1/T-1 (1.5 Mbps) 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 like the Internet link (Akin Cahit, 2015). The best cost effective solution for addressing this issue was 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 was deployed by implementing the virtual private network (VPN) technology using the existing IT setups. As the WAN infrastructures were are based on Cisco routers, so the IT department had decided to deploy Dynamic Multipoint VPN (DMVPN) without further investments. The DMVPN is a Cisco IOS (Internetwork Operating System) software-based solution for building scalable IPsec VPNs. 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 was 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 had specific steps and associated activities.

Problem Statement

By performing the vulnerability assessment, security audit of the network and interview with the management it found that the MPLS technology for the organization was not delivered the data encryption facilities over the WAN link (Haran V., 2012). Due to clear text communication over the WAN link, there was a huge security risk involved in data communication and unauthorized access of data. They were 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 was planning to cut off the IT budget for the corporation.

While MPLS technology provided a WAN connection between the remote locations and data center, 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. However, the WAN using MPLS link was very costly for the small organization. In the United States, the average pricing ranges for a DS-1/T-1 (1.5 Mbps) 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 like the Internet link (Akin Cahit, 2015). The best cost effective solution for addressing this issue was 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 was deployed by implementing the virtual private network (VPN) technology using

the existing IT setups. As the WAN infrastructures were are based on Cisco routers, so the IT department had decided to deploy Dynamic Multipoint VPN (DMVPN) without further investments.

Problem Causes

The reason for this issue is a form of kind negligence, which has accepted the completely latest technology to pass by. For last six years, the majority of investment in branch office connectivity has been restricted to as needed break-fix events and services provider WAN (MPLS) services renewal contract only. The outcome of this attitude is a failure to install the latest technology which would decrease costs and advance services like advanced security technique VPN.

Typically, data transfer between branch offices and corporate headquarters occurs over a service provider (SP) network or the Internet. Therefore, the WAN security is a highly important factor for any organization. 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 Cisco gears and low-cost Internet link, some boundaries need to be aware of. The organization which is wanting to deploy the VPN had to confirm that adopting or considering the VPN was the best option for them. The VPN design and security deployment for the VPN are complicated. That means for implementing VPN; it is required experienced IT professional. The IT staffs should have 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 was used the 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

The MPLS technology for the organization was not delivered the data encryption facilities over the WAN link (Haran V., 2012). Due to clear text communication over the WAN link, there was a huge security risk involved in data communication and unauthorized access of data. They were losing their business because of several cyber-attacks like Man-in-the-middle attack, IP spoofing attacks from their competitors and disgruntled employees.

While MPLS technology provided a WAN connection between the remote locations and data center, 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. However, the WAN using MPLS link was very costly for the small

organization. In the United States, the regular pricing ranges for a DS-1/T-1 (1.5 Mbps) 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 like the Internet link (Akin Cahit, 2015). The best cost effective solution for addressing this issue was the replacement of expensive MPLS link with a low-cost Internet connection and WAN traffic encryption over the Internet link (Gottlieb A., 2012).

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 implemented the DMVPN using the existing WAN infrastructures as Cisco routers and associated IOS software i.e. without additional hardware investment. Also, the DMVPN had implemented over the low-cost Internet link. They removed the expensive MPLS link from their WAN infrastructures. Also, the in-house IT staff members had deployed this project. Any additional support was provided by the Cisco Technical Assistance Center (TAC) team as the organization already have Cisco TAC support contract for all Cisco gears. Keeping all of these factors in mind below was the cost breakdown for the WAN encryption project:

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
2	Removing MPLS 10 Mbps Host Link from HQ	Removing MPLS 10 Mbps Host Link from HQ	1	Monthly $5000.00	$60000.00
Total Benefits from removing the MPLS link for One Year					**$ 108000.00**

The MPLS link speed was T1 or 1.5 Mbps link. The IT department had replaced the MPLS link with 50 Mbps Internet link. They used the existing Internet link at the data center for DMVPN deployment and removed the 10 Mbps MPLS link which saves monthly $5000.00 for IT budget. By replacing this, the IT department can save an enormous amount of $ 103200.00 (Forty-Nine Thousand Two Hundred Dollars) for IT budget with better Internet bandwidth or better performances. Additionally, the secure WAN encryption has improved 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 Cisco gears and low-cost Internet link, some boundaries need to be aware of. The organization which is wanting to deploy the VPN had to confirm that adopting or considering the VPN was the best option for them. The VPN design and security deployment for the VPN are complicated. That means for implementing VPN; it is required experienced IT professional. The IT staffs should have 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 was used the 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.

The performance and reliability of the VPN can become a factor depending on the service provider that the organization is selecting for WAN communication. As 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.

Detailed and Functional Requirements

The 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). There are three VPN goals, which are data confidentiality, data integrity, and authentication. This WAN encryption capstone project had two central goals. The first goal was WAN encryption with secure authentication for protecting all users' traffic from external threats and the second goal was the cost effective solution. This project has tackled the implementation of WAN encryption for the organization from start to finish. The research methodology used to investigate the problem included with the vulnerability assessment, security audit of the network and interview with the management.

Functional (end-user) Requirements

It is clear that because of user's security need and especially because of the need of sending encrypted data over the WAN network, the VPN technology has been developed. The first functional requirement for end-users was that the enhanced security. When end-user connects to the data center network from a remote location through the Internet link using VPN, the data will be kept secure and encrypted. In this way, the users' information will be away from hackers' eyes. The second functional requirement for end-users was that the share files access. The WAN encryption using the VPN service will be useful for the group users who need to share data for an extended period. The third functional requirement for end-users was the better network performance and improved productivity. The increased Internet bandwidth and efficiency of the system will be increased network performance and improved the end-users productivity.

Detailed Requirements

WAN encryption by deploying the VPN into the organization can contribute to the achievement of business objectives in several ways. The first requirement was that it should significantly 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. The second requirement was that it should eliminate the need for expensive recurring MPLS link cost and support costs which should help the management for reducing the IT budget. The third requirement was that the functionality and resources should be shared with a corporate head office to all remote locations' employees. The fourth requirement was that it encourages the productivity of employees that work via virtual workplaces because of better WAN performances and enhanced security. The fifth requirement was that the data encryption techniques should make the customers feel secure as their data was protected from unauthorized data access, and it should soothe their worries.

Existing Gaps

After implementing the WAN encryption, it will contribute to the achievement of business objectives in several ways. The first gap it will fill that it considerably reduces the risk of security breaches and cyber attacks and improves the security for data communication, 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 WAN data communication because of advanced technologies that are used to secure the network from unauthorized user access. The second gap it will fill that all the end-users will be able to connect to the data center network from a remote location through the Internet link using VPN tunnel, the data will be kept secure and encrypted. In this way, the users' information will be away from hackers' eyes. The third gap it will fill that all the end-users will be able to access the share files securely. The fourth gap it will fill that all the end-users will get enhanced network performance for improving the productivity. The increased Internet bandwidth and efficiency of the system will be increased network performance

and improved the end-users productivity. The fourth gap it will fill the requisite of prohibitive recurring MPLS link cost and support costs. By this way, the management can reduce the IT budget. The fifth gap it will fill that the data encryption techniques will make the customers feel secure as their data is secure from unauthorized data access, and it will soothe their worries.

Project Design

Project design was an initial phase of the project where a project's key structure, features, measures for success, and key deliverables were all planned out. The point was to develop one or more designs which were used to accomplish the desired project objectives or goals. The stakeholders of the organization then selected the best design strategy for the actual implementation of the project. The project was established using the four major phases as initiation, planning, execution and control, and project closer, which referred to as the project "life cycle." Each stage had specific steps and associated activities. While the stages, steps, and actions suggest a linear sequence of events, in the real execution there was often an additional dynamic flow to the work. Some stages or steps may be co-occurring, and the work often circles back to revisit the earlier phases.

Scope

WAN security will protect all the traffic from possible external cyber 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 had two central goals. The first goal was WAN encryption with secure authentication for protecting all traffic from external threats and the second goal was the cost effective solution. This project has tackled the implementation of WAN encryption for the organization from start to finish. First, a systematic cost-benefit analysis (CBA) between the MPLS link and the Internet link was performed to estimate the strengths and flaws of the alternatives. Second, the new Internet links were procured for all four-branch offices, which replaced the

expensive MPLS links. The existing Internet connection of headquarter was reused for this project. Third, a company policy on WAN traffic encryption and authentication along with the statement of understanding and configuration was confirmed the WAN encryption security. The internal resources were deployed this project. Fourth, built prototype model in GNS3 network simulator for testing and development. Fifth, Installation and testing of new Internet connection were performed in all four-branch office locations. Sixth, notified all related stakeholders for significant downtime to the deployment of this solution. Seventh, network devices were configured according to the design documents, and penetration test was performed for certifying that WAN encryption.

Assumptions

The primary assumptions or hypothesis of this project was that the IT department wanted to implement WAN encryption using the Internet for securing the WAN traffic. Whereas the corporation already had MPLS link for WAN connectivity. The group was trying to configure the VPN for data encryption using the existing WAN infrastructures. The entire branch network had G2series Cisco 2911-SEC/K9 Integrated Services Routers, and data center had G2series Cisco 3945-SEC/K9 Integrated Services Router. Also, all the routers were installed with Cisco securityk9 IOS technology package software, which supported the DMVPN. As the WAN infrastructures were based on Cisco routers, so the IT department had 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 was that the Enhanced Interior Gateway Routing Protocol or EIGRP was using for automating routing decisions and route selection procedures. The last assumption was that the internal IT staffs were enough skillful and knowledgeable so that they were able to deploy the data encryption project for WAN communication with the support of Cisco TAC.

Project Phases

The project was implemented using the four major steps or phases as initiation, planning, execution and control, and project closer, which referred to as the project "life cycle." Each stage had concrete steps and associated activities. While the stages, steps, and actions suggest a linear sequence of events, in the real execution there was often an additional dynamic flow to the work. Some stages or steps may be co-occurring, and the work often circles back to revisit the earlier phases. The steps of the project were as follows:

Project Phase
Phase 1: Project Initiation
1.1 Defines Project and its Scope
1.2 Build a Business Case and Feasibility Study
1.3 Meeting with Stakeholders
1.4 Analysis Existing Network
1.5 Creation of Project Charter
1.6 Perform a Phase Review
Phase 2: Project Planning
2.1 Gather Functional and Technical Requirements
2.1.1 Collect existing Network Diagram
2.1.2 Gather existing Network Configuration
2.1.3 Gather existing IP Scheme
2.1.4 Gather existing Routing Information
2.2 Finalize the Project Scope and Budget Requirement
2.3 Identify Potential Risks and begin Managing Risks
2.4 Develop a Project Schedule
2.5 Create a Procurement Plan for new Internet link
2.6 Create Design document of Proposed Solution
2.7 Planning for Prototype Development and Testing
2.8 Perform a Phase Review
Phase 3: Project Execution and Control
3.1 Build Prototype for Development and Testing
3.1.1 Build Prototype in GNS3 Network Simulator
3.1.2 Configure GNS3 Network Simulator
3.1.3 Performance Testing in GNS3 Simulator
3.1.4 Security Testing in GNS3 Simulator

3.1.5 Create Prototype Test Result Documents
3.1.6 Prototype Test Result Analysis
3.2 Securityk9 IOS Technology License Activation
3.2.1 License Activation at Columbia HQ Router
3.2.2 License Activation at Charleston Router
3.2.3 License Activation at Greenville Router
3.2.4 License Activation at Florence Router
3.2.5 License Activation at Orangeburg Router
3.3 Routers Configuration
3.3.1 Columbia HQ Router Configuration
3.3.2 Columbia HQ User Acceptance Testing
3.3.3 Charleston Spoke Router Configuration
3.3.4 Charleston User Acceptance Testing
3.3.5 Greenville Spoke Router Configuration
3.3.6 Greenville User Acceptance Testing
3.3.7 Florence Spoke Router Configuration
3.3.8 Florence User Acceptance Testing
3.3.9 Orangeburg Spoke Router Configuration
3.3.10 Orangeburg User Acceptance Testing
3.4 DMVPN Performance Monitoring
3.5 Final Documents Creation
3.6 Perform a Phase Review
Phase 4: Project Closure
4.1 Review Project Completion
4.2 Perform Lessons Learned Analysis
4.3 Finalize the Project Close-out Report
4.4 Archive the Project Documentation

Timelines

Schedule: 04/10/2017 to 7/14/2016

Tasks Name	Duration	Start	End
Phase 1: Project Initiation	**15 Days**	**4/10/2017**	**7/14/2017**
1.1 Defines Project and its Scope	4 Days	4/10/2017	4/13/2017
1.2 Build a Business Case and Feasibility Study	3 Days	4/14/2017	4/16/2017
1.3 Meeting with Stakeholders	2 Day	4/17/2017	4/18/2017
1.4 Analysis Existing Network	2 Days	4/19/2017	4/20/2017

1.5 Creation of Project Charter	2 Days	4/21/2017	4/22/2017
1.6 Perform a Phase Review	1 Day	4/23/2017	4/23/2017
Phase 2: Project Planning	**15 Days**	**4/24/2017**	**5/8/2017**
2.1 Gather Functional and Technical Requirements	5 Days	4/24/2017	4/28/2017
2.1.1 Collect existing Network Diagram	1 Day	4/24/2017	4/24/2017
2.1.2 Gather existing Network Configuration	2 Day	4/25/2017	4/26/2017
2.1.3 Gather existing IP Scheme	1 Day	4/27/2017	4/27/2017
2.1.4 Gather existing Routing Information	1 Day	4/28/2017	4/28/2017
2.2 Finalize the Project Scope and Budget Requirement	2 Days	4/29/2017	4/30/2017
2.3 Identify Potential Risks and begin Managing Risks	1 Day	5/1/2017	5/1/2017
2.4 Develop a Project Schedule	1 Day	5/2/2017	5/2/2017
2.5 Create a Procurement Plan for new Internet link	1 Day	5/3/2017	5/3/2017
2.6 Create Design document of Proposed Solution	3 Days	5/4/2017	5/6/2017
2.7 Planning for Prototype Development and Testing	1 Day	5/7/2017	5/7/2017
2.8 Perform a Phase Review	1 Day	5/8/2017	5/8/2017
Phase 3: Project Execution and Control	**60 Days**	**5/9/2017**	**7/8/2017**
3.1 Build Prototype for Development and Testing	15 Days	5/9/2017	5/23/2017
3.1.1 Build Prototype in GNS3 Network Simulator	3 Days	5/9/2017	5/11/2017
3.1.2 Configure GNS3 Network Simulator	3 Days	5/12/2017	5/14/2017
3.1.3 Performance Testing in GNS3 Simulator	3 Days	5/15/2017	5/17/2017
3.1.4 Security Testing in GNS3 Simulator	3 Days	5/18/2017	5/20/2017
3.1.5 Create Prototype Test Result Documents	2 Days	5/21/2017	5/22/2017
3.1.6 Prototype Test Result Analysis	1 Day	5/23/2017	5/23/2017
3.2 Securityk9 IOS Technology License Activation	5 Days	5/24/2017	5/28/2017
3.2.1 License Activation at Columbia HQ Router	1 Day	5/24/2017	5/24/2017
3.2.2 License Activation at Charleston Router	1 Day	5/25/2017	5/25/2017
3.2.3 License Activation at Greenville Router	1 Day	5/26/2017	5/26/2017
3.2.4 License Activation at Florence Router	1 Day	5/27/2017	5/27/2017
3.2.5 License Activation at Orangeburg Router	1 Day	5/28/2017	5/28/2017
3.3 Routers Configuration	25 Days	5/29/2017	7/8/2017
3.3.1 Columbia HQ Router Configuration	1 Day	5/29/2017	5/29/2017
3.3.2 Columbia HQ User Acceptance Testing	4 Days	5/30/2017	6/2/2017
3.3.3 Charleston Spoke Router Configuration	1 Day	6/3/2017	6/3/2017
3.3.4 Charleston User Acceptance Testing	4 Days	6/7/2017	6/7/2017
3.3.5 Greenville Spoke Router Configuration	1 Day	6/8/2017	6/8/2017
3.3.6 Greenville User Acceptance Testing	4 Days	6/9/2017	6/12/2017
3.3.7 Florence Spoke Router Configuration	1 Day	6/13/2017	6/13/2017
3.3.8 Florence User Acceptance Testing	4 Days	6/14/2017	6/17/2017
3.3.9 Orangeburg Spoke Router Configuration	1 Day	6/18/2017	6/18/2017

3.3.10 Orangeburg User Acceptance Testing	4 Days	6/19/2017	6/22/2017
3.4 DMVPN Performance Monitoring	12 Days	6/23/2017	7/4/2017
3.5 Final Documents Creation	3 Days	7/5/2017	7/7/2017
3.6 Perform a Phase Review	1 Day	7/8/2017	7/8/2017
Phase 4: Project Closure	**6 Days**	**7/9/2017**	**7/14/2017**
4.1 Review Project Completion	2 Day	7/9/2017	7/10/2017
4.2 Perform Lessons Learned Analysis	2 Day	7/11/2017	7/12/2017
4.3 Finalize the Project Close-out Report	1 Day	7/13/2017	7/13/2017
4.4 Archive the Project Documentation	1 Day	7/14/2017	7/14/2017

The projected timeline was dependent upon the procurement of the Internet link from the service provider. The ISP had installed all four new Internet link in a timely fashion. The existing WAN infrastructures were reused for this project. The current cabling infrastructures were reused, so there was no dependency on wiring work. The actual DMVPN implementation was relatively graceful because most of the network issues were addressed during the prototype testing in GNS3 simulator. The total time was required for completing this project from initiation to closing phase was 96 days.

Dependencies

The project dependencies are the interactions or inter relation of the preceding tasks to the following works. Tasks may have multiple preceding tasks and various succeeding tasks. The most common dependency relationship is a finish-to-start relationship. The WAN encryption project dependencies are described in the table below. For example, the outcomes of the current network analysis (Task-5) and the functional and technical requirement (Task-9) audit reports were required for design document of proposed solution (Task-18). Similarly, the task creates a procurement plan for new Internet link (Task-17) must be complete for finishing the router configuration (Task-35 to 42).

Task No.	Tasks Name	Duration
1	**Phase 1: Project Initiation**	**15 Days**

2	1.1 Defines Project and its Scope	4 Days
3	1.2 Build a Business Case and Feasibility Study	3 Days
4	1.3 Meeting with Stakeholders	2 Day
5	1.4 Analysis Existing Network	2 Days
6	1.5 Creation of Project Charter	2 Days
7	1.6 Perform a Phase Review	1 Day
8	**Phase 2: Project Planning**	**15 Days**
9	2.1 Gather Functional and Technical Requirements	5 Days
10	2.1.1 Collect existing Network Diagram	1 Day
11	2.1.2 Gather existing Network Configuration	2 Day
12	2.1.3 Gather existing IP Scheme	1 Day
13	2.1.4 Gather existing Routing Information	1 Day
14	2.2 Finalize the Project Scope and Budget Requirement	2 Days
15	2.3 Identify Potential Risks and begin Managing Risks	1 Day
16	2.4 Develop a Project Schedule	1 Day
17	2.5 Create a Procurement Plan for new Internet link	1 Day
18	2.6 Create Design document of Proposed Solution	3 Days
19	2.7 Planning for Prototype Development and Testing	1 Day
20	2.8 Perform a Phase Review	1 Day
21	**Phase 3: Project Execution and Control**	**60 Days**
22	3.1 Build Prototype for Development and Testing	15 Days
23	3.1.1 Build Prototype in GNS3 Network Simulator	3 Days
24	3.1.2 Configure GNS3 Network Simulator	3 Days
25	3.1.3 Performance Testing in GNS3 Simulator	3 Days
26	3.1.4 Security Testing in GNS3 Simulator	3 Days
27	3.1.5 Create Prototype Test Result Documents	2 Days
28	3.1.6 Prototype Test Result Analysis	1 Day
29	3.2 Securityk9 IOS Technology License Activation	5 Days
30	3.2.1 License Activation at Columbia HQ Router	1 Day
31	3.2.2 License Activation at Charleston Router	1 Day
32	3.2.3 License Activation at Greenville Router	1 Day
33	3.2.4 License Activation at Florence Router	1 Day
34	3.2.5 License Activation at Orangeburg Router	1 Day
35	3.3 Routers Configuration	25 Days
36	3.3.1 Columbia HQ Router Configuration	1 Day
37	3.3.2 Columbia HQ User Acceptance Testing	4 Days
38	3.3.3 Charleston Spoke Router Configuration	1 Day
39	3.3.4 Charleston User Acceptance Testing	4 Days
40	3.3.5 Greenville Spoke Router Configuration	1 Day

41	3.3.6 Greenville User Acceptance Testing	4 Days
42	3.3.7 Florence Spoke Router Configuration	1 Day
43	3.3.8 Florence User Acceptance Testing	4 Days
44	3.3.9 Orangeburg Spoke Router Configuration	1 Day
45	3.3.10 Orangeburg User Acceptance Testing	4 Days
46	3.4 DMVPN Performance Monitoring	12 Days
47	3.5 Final Documents Creation	3 Days
48	3.6 Perform a Phase Review	1 Day
49	**Phase 4: Project Closure**	**6 Days**
50	4.1 Review Project Completion	2 Day
51	4.2 Perform Lessons Learned Analysis	2 Day
52	4.3 Finalize the Project Close-out Report	1 Day
53	4.4 Archive the Project Documentation	1 Day

Resource Requirements

The primary resources for this project are the Service Provider's Internet link, internal IT workforce, network & security administrator, and Cisco TAC support team. These resources are critical throughout the WAN encryption project. The network & security administrator will lead the project execution and control phase activities of this project.

The WAN infrastructures of the organization were based on Cisco routers so it was determined during the discussion with management that the IT team will deploy WAN encryption project using the existing Cisco WAN infrastructures. The WAN network infrastructure comprises with one Cisco 3945-SEC/K9 Integrated Services Router in the data center, and all four branches had Cisco 2911-SEC/K9 Integrated Services Router. All routers were running with Cisco securityk9 IOS technology package software, which was suitable for DMVPN implementation. Enhanced Interior Gateway Routing Protocol is using as the primary routing protocol for network traffic routing.

Risk Factors

There are several risks present during the different phases of project deployment. Although the WAN encryption delivers the value-added data encryption security for data communications using the Cisco gears and low-cost Internet link, some boundaries need to be aware of. The organization which is wanting to deploy the VPN had to confirm that adopting or considering the VPN was the best option for them. The VPN design and security deployment for the VPN are complicated. That means for implementing VPN; it is required experienced IT professional. The IT staffs should have 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 was used the 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.

The performance and reliability of the VPN can become a factor depending on the service provider that the organization is selecting for WAN communication. As 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.

Important Milestones

The milestones are the tools used in project management to mark particular points alongside a project schedule. These points may signal presenters such as a project start and end date, a requirement for external analysis or input and budget checks, among others. The following were significant milestones or signs are identified to gauge project progress:

- Accomplishment of IT assessment, analysis, and documentation
- Achievement of requirement gathering
- Completion of design phase
- Procurement of new Internet links
- Building prototype for development and testing
- Securityk9 IOS Technology License Activation
- Hub and spoke Routers Configuration
- User acceptance testing for all four locations
- VPN/DMVPN performance monitoring
- Implementation documents creation

- Perform lessons learned analysis
- Training and education program implemented

Deliverables

The main deliverables of this project existed Cisco setups like Cisco routers, IOS software, and design documentation. The existing Cisco routers were using for this project. Cisco 3945-SEC/K9 Integrated Services Router at a data center and all others four branches had Cisco 2911-SEC/K9 Integrated Services Router.

The other deliverable of this project was the design document. The design document consists of all related documents for deploying this project. It includes:

- Existing network architecture diagram
- Current routers configuration documents
- Existing IP scheme and routing information
- Proposed network architecture diagram
- Proposed IP scheme and route information
- Proof of concept result from prototype testing
- Recommend all configuration documents
- Software license up-gradation plan
- Implementation plan guideline and
- Support document manual creation.

Methodology

The research technique used to investigate the problem included with the vulnerability assessment, security audit of the network and interview with the management. The project was 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 had concrete steps and associated activities. While the stages, steps, and actions suggest a linear sequence of events, in the real execution there was often an additional dynamic flow to the work. Some stages or steps may be co-occurring, and the work often circles back to revisit the earlier phases. Numerous different methodologies were considered in the research phase of this WAN encryption project. None of the methods were entirely wrong, but in the end, the method that seemed the most correct for the particular small organization in question was carefully chosen.

ACME Corporation had Cisco 3945-SEC/K9 router in the data center and Cisco 2911-SEC/K9 routers in all four branch offices. All routers were running with Cisco securityk9 IOS technology package, which was suitable for DMVPN implementation. Enhanced Interior Gateway Routing Protocol is using as the primary routing protocol for network traffic routing. As the communication over MPLS link was unsecured plain text communication, there was a security risk of data safety and unauthorized data capture over WAN link. There was no current solution exist which can secure this data communication over the WAN.

Before DMVPN deployment in a production environment, the solution was properly evaluated and analyzed. The test and development environment for implementing DMVPN was in a GNS3 network simulator. The GNS3 was a free graphical network simulator. It was capable of emulating some network devices like Cisco routers, switches, firewall, and servers (Gns3, ND). This simulator prototype was installed in Windows 7 laptop for test and development. The ‘Cisco securityk9 IOS technology package’ evaluation license was used for the test environment. This evaluation license was valid for 30days. After performing the performance and security testing in GNS3 simulator, the test result was documented for analysis and outcome. Finally, the tested configuration was applied in a production environment.

The explanation for some the phases going on simultaneously to save time and cost during the execution. The ability to save time supports if there happen to be road blocks in other phases of the project that may take diligence to resolve. The best way to efficiently and complete this WAN encryption project was on time and very less budget.

Approach Explanation

The methodology taken in this WAN encryption project is to design a protected or secure WAN communication which should be scalable, easily configurable, can implement using the existing WAN infrastructures and which will be secure enough so that it can deploy over the low-cost Internet link. The functionality, security, and ease of use are often considered in a triad correlation because more of one element usually means losing one or both of the other aspects. All the small organization needed same quantities of all three factors - something that delivers world class features at a little cost (functionality), is comparatively easy for the IT department to deploy and maintain (ease-of-use), and is strong against the cyber attack (security).

It was clear that the data transmission over the MPLS link for the organization was unencrypted plain text communication. Due to this, there was a huge risk involved in data security and unauthorized capturing of data. They were losing their business because of severe cyber-attacks like Man-in-the-middle attack, IP spoofing attacks from their competitors and disgruntled employees and due to poor business performance the management was looking for reducing the IT budget. Therefore, the IT department had decided to implement the cost-effective, data encryption for branch offices WAN connectivity for protecting all kind of traffic. The project was executed for securing the WAN traffic from external threats without spending extra money.

The data center at headquarter had 10 Mbps MPLS host link, and all four branch offices were connected through 1.5 Mbps MPLS link. The WAN network infrastructure comprises with one Cisco 3945-SEC/K9 Integrated Services Router in the data center, and all four branches had Cisco 2911-SEC/K9 Integrated Services Router. The IT department had decided to deploy Cisco DMVPN using the existing hardware setup for protecting additional hardware cost. The DMVPN is a Cisco IOS software-based solution for building scalable IPsec VPNs. The IT department was analyzed that they may implement the same Cisco DMVPN over the MPLS link, but the MPLS is more expensive compared to the Internet link (Gottlieb A., 2012). The best cost effective solution for addressing those issues was the replacement of expensive MPLS link with a low-cost Internet connection and WAN traffic encryption over the Internet link (Gottlieb A., 2012). Also, the IT department had decided to deploy this solution by using the in-house IT staffs.

Before DMVPN deployment in a production environment, the solution was properly evaluated and analyzed. The test and development environment for implementing DMVPN was in a GNS3 network simulator. The GNS3 was a free graphical network simulator. It was capable of emulating some network devices like Cisco routers, switches, firewall, and servers (Gns3, ND). This simulator prototype was installed in Windows 7 laptop for test and development. The 'Cisco securityk9 IOS technology package' evaluation license was used for the test environment. This evaluation license was valid for 30days. After performing the performance and security testing in GNS3 simulator, the test result was documented for analysis and outcome. Finally, the tested configuration was applied in a production environment. To make both phases of the project as easy to implement and maintain as possible, step-by-step guides were created during installation.

Approach Defense

The WAN network infrastructure of ACME Corporation include with Cisco 3945-SEC/K9 Integrated Services Router in the data center, and all four branch offices have Cisco 2911-SEC/K9 Integrated Services Router. All routers were running with Cisco securityk9 IOS technology package software. The EIGRP (Enhanced Interior Gateway Routing Protocol) was used for network traffic routing. The data transmission between the branches and headquarter were through the service provider's MPLS WAN cloud. This communication was unencrypted non-secure plain text communication. Therefore, there was a chance of compromise data security and unauthorized capturing of plain text data over the MPLS cloud. Hence, IT department had decided to implement secure, encrypted communication over the Internet cloud with lower implementation and operational cost. The ideal solution was DMVPN deployment using the old WAN infrastructures. The primary concern for DMVPN deployments was:

1. The Cisco router model at data center acts as hub router
2. The Cisco router model at branch for working as spoke router and
3. The Cisco Securityk9 IOS technology package is running on all routers.

WAN routers are the most critical devices, and those are responsible for reliable IP forwarding and Quality of Service. The bandwidth required at each remote location determines which model of the router is suitable for hub and spoke. G2series Cisco 3945-SEC/K9 is next-generation, modular Integrated Services Router. They are designed for WAN aggregation, with the flexibility to support 150 Mbps system bandwidth performance and scaling (Cisco Systems, 2014). This router is suitable for the data center to act as hub or backbone router, which can handle 50Mbps, Internet link traffic. According to Cisco Systems, 2016 says, "The Cisco 3900 Series offers embedded hardware encryption acceleration, voice- and video-capable DSP slots,

optional firewall, intrusion prevention, call processing, voicemail, and application services. Also, the platforms support the industry's widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, copper, and fiber Gigabit Ethernet. The Cisco 3900 Series offers superior performance and flexibility for flexible network deployments from small business offices to large enterprise offices - all while providing industry-leading investment protection."

The bandwidth required at each remote location determines which model of the router will suitable for acting as spoke. The most important factor is the ability to process the expected amount and type of traffic. The existing G2series Cisco 2911-SEC/K9 Integrated Services Routers is suitable for a branch office to act as spoke router, which can handle up to 50Mbps bandwidth traffic (Cisco Systems, 2014). According to Cisco Systems, 2016: "All Cisco 2900 Series Integrated Services Routers offer embedded hardware encryption acceleration, voice- and video-capable digital signal processor (DSP) slots, optional firewall, intrusion prevention, call processing, voicemail, and application services. Also, the platforms support the industries widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, copper, and fiber GE."

Also, Miercom's "Lab Testing Summary Report," 2009 mentioned that: "Cisco ISR G2 platforms delivered five times improved performance compared to the previous-generation ISRs. Cisco ISR 3945 given throughput of up to 150 Mbps with integrated services enabled. ISR G2 platforms support bandwidth–optimized and scalable video including TelePresence and streaming. Cisco ISR G2 platforms offer "Service Ready Engine" providing the flexibility to turn on services on demand. All of the Cisco ISR G2 branch routers delivered throughput which exceeded by 102% to 214% the stated bandwidth requirements of the branch, while integrated features were activated. All test results were observed without any frame loss and maintaining

CPU utilization of 75%". From the above discussion, we can conclude that the existing network infrastructures, Cisco 3945-SEC/K9 and Cisco 2911-SEC/K9 routers models are suitable for DMVPN deployment with better network performance.

The Cisco securityk9 IOS technology package software was appropriate for DMVPN implementation. According to Cisco Systems, 2009: "The Cisco IOS Security technology package license can support standard IP Security, Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), Cisco IOS Zone-Based Firewall, advanced application inspection and control, firewall for secure unified communications, VRF-aware firewall, firewall high availability, transparent firewall, Cisco IOS IPS, transparent IPS, VRF-aware IPS, secure provisioning and digital certificates, and Cisco IOS Certificate Server and Client."

Another major requirement for this project is better encryption for DMVPN traffic. The Cisco securityk9 IOS technology package is suitable for better encryption. According to Cisco Systems, 2009: "IPSec standards supported include Digital Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES; 128, 192, and 256) for encryption; Rivest, Shamir, Aldeman (RSA) algorithm signatures and Diffie-Hellman for authentication; and Secure Hash Algorithm 1 (SHA-1) or Message Digest Algorithm 5 (MD5) hashing algorithms for data integrity." From this discussion, we can conclude that proposed Cisco securityk9 IOS technology package is suitable for DMVPN implementation with better encryption.

The existing EIGRP routing protocol can continue for route selection in DMVPN. It is easy to configure, easy for planning, has route summarization and it is scalable to large networks. The routes or IP prefixes in the routing tables grow as networks grow. The IP route summarization will help up for reducing the bandwidth utilization, processor utilization, and memory need to handle large route tables and reduce convergence time for link failure. These

will justify the WAN encryption by deploying the DMVPN project is a long term scalable solution for the organization, and the chosen approach was perfectly matching with the business requirement.

Project Development

Before and during project development, needs for hardware, software, tech stack, architecture, and resources were all evaluated. Alterations will be made as required to confirm the final product and services are associated with business requirements.

Hardware

The existing hardware devices were used for WAN encryption project. All the branch network had G2series Cisco 2911-SEC/K9 Integrated Services Routers, and data center had G2series Cisco 3945-SEC/K9 Integrated Services Router. WAN routers are the most critical devices, and those are responsible for reliable IP forwarding and Quality of Service. The bandwidth required at each remote location determines which model of the router is suitable for hub and spoke. G2series Cisco 3945-SEC/K9 is next-generation, modular Integrated Services Router. They are designed for WAN aggregation, with the flexibility to support 150 Mbps system bandwidth performance and scaling (Cisco Systems, 2014). This router is suitable for the data center to act as hub or backbone router, which can handle 100Mbps, Internet link traffic.

The bandwidth required at each remote location determines which model of the router is suitable for acting as spoke. The most significant factor is the ability to process the expected amount and type of traffic. The existing G2series Cisco 2911-SEC/K9 Integrated Services Routers is suitable for a branch office to act as spoke router, which can handle up to 50Mbps bandwidth traffic (Cisco Systems, 2014). Also, the existing cabling infrastructures were reused for this project. Also, one Windows 7 laptop was used for GNS3 simulator prototype lab setup

for testing and development. Internet link for all four location was procured for replacement of MPLS.

Software

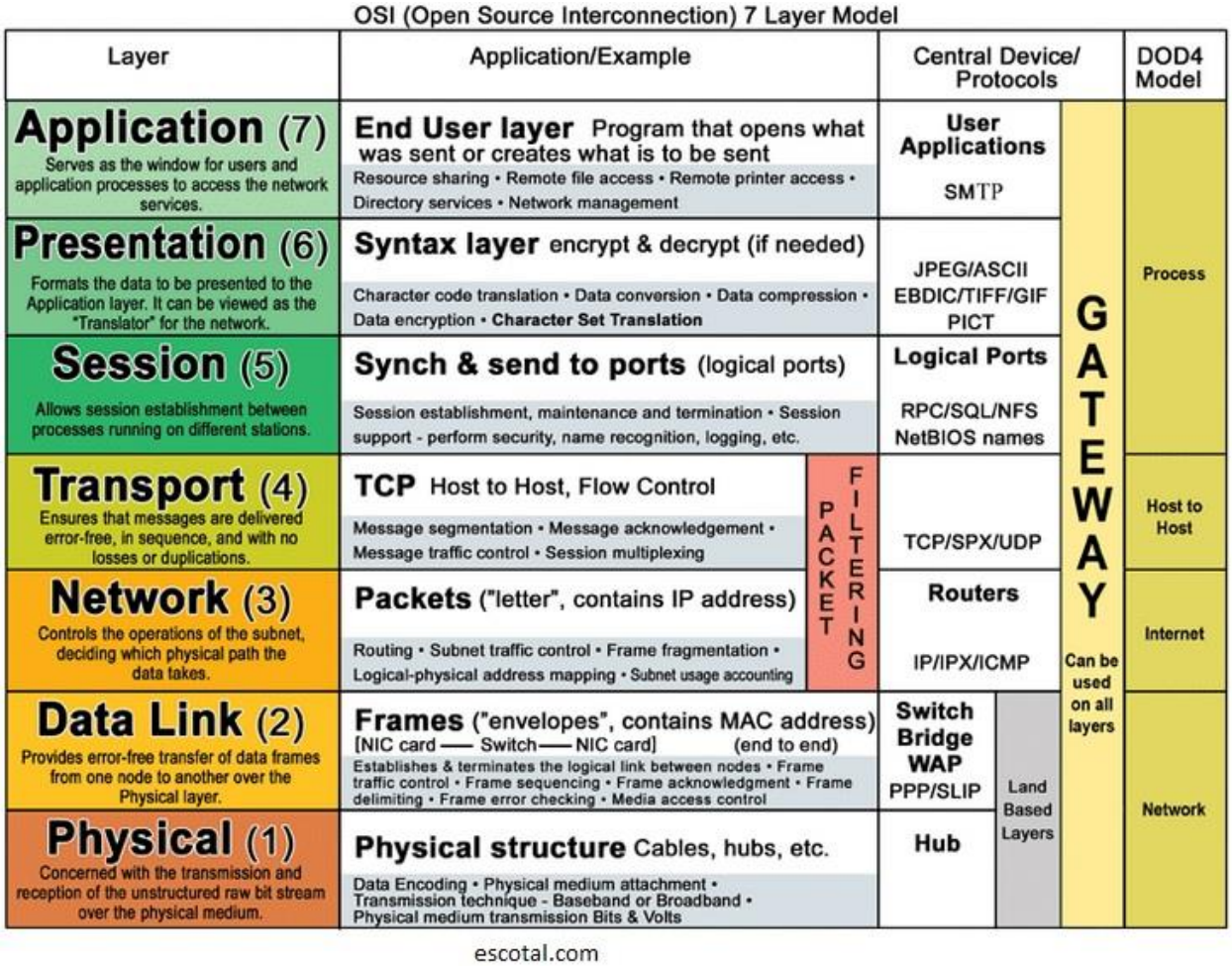
All routers were running with Cisco securityk9 IOS technology package software. The Cisco proprietary routing protocol EIGRP was used for network traffic routing. The Cisco IOS Security technology package software can support standard IP Security, Dynamic Multipoint VPN (DMVPN), VRF-aware firewall, firewall high availability, Cisco IOS IPS, transparent IPS, secure provisioning and digital certificates, and Cisco IOS Certificate Server and Client.

The test and development environment for implementing DMVPN was in a GNS3 network simulator. The GNS3 was a free graphical network simulator. It was capable of emulating some network devices like Cisco routers, switches, firewall, and servers (Gns3, ND). This simulator prototype was installed in Windows 7 laptop for test and development. The 'Cisco securityk9 IOS technology package' evaluation license was used for the test environment. This evaluation license was valid for 30days.

Tech Stack

The OSI (open system interconnection) model is a means by which network protocols can be executed. It includes seven different layers of communication as the application layer, presentation layer, session layer, transport layer, network layer, data link and physical layer. Where VPN networks are concerned, they are defined by which layer is used to deliver security. The encryption can happen at different layers. Depending upon which layer the encryption occurs at, varying levels of traffic will be encrypted. A Network layer VPN functions on layer 3 or network layer. The network layer VPN security will encrypt any traffic, irrespective of the different applications being used. This type of VPN is used by some of the most well-known

names in Internet security. For example, Cisco uses this layer for VPNs. These VPN servers are sometimes provided under the names GRE.



Architecture Details

The WAN encryption project was implemented by deploying the DMVPN technology using the existing Cisco WAN infrastructure over the Internet link. DMVPN is a secure private network and an enhanced technique of the traditional VPN. Traditional VPNs connect each remote location to the HQ. The DMVPN essentially creates a mesh VPN topology, which means that each location can connect straight with all other locations, no matter where they are situated. The Dynamic Multipoint VPN (DMVPN) is a combination of Generic Routing Encapsulation

(GRE), Next-Hop Resolution Protocol (NHRP), and IPSec. It works in the hub and spoke topology.

GRE: A GRE tunnel is simple non-negotiated tunnel; GRE only needs tunnel endpoints. GRE encapsulates frames or packets into another IP packet and IP header. It is completely stateless, and Tunnel interface is by default always up even if the remote point is unavailable. GRE has only 4 to 8 bytes of overhead. There are the following two types of GRE tunnels:

- **Point-to-point or PtP (GRE):** It has the IP address, the tunnel source, and destination address. The address of origin (source address) is the local physical IP address and the destination IP address is remote physical IP address.
- **Point-to-multipoint (mGRE):** It has the same parameters as the PtP GRE except for the target IP address. mGRE interfaces do not have a tunnel destination interface.

NHRP: The functions of NHRP are as follows:

- NHRP is a layer 2 or data link layer protocol and cache like ARP which is used in DMVPN to map a tunnel IP address to an NBMA address.
- The tunnel address is the IP address defined on the tunnel interface. It is also known as the logical IP address.
- The Non-Broadcast Multiple Access (NBMA) address is the IP address used as tunnel source (or destination). It is also known as the routable IP address or the public IP address.
- NHRP has its cache wherein it stores the mapping of logical and the NBMA IP address. NHRP can have static and dynamic entries. With NHRP, devices attached to an NBMA network dynamically learn the NBMA address of the other systems that are part of that

network, permitting these systems to directly connect without needing traffic to use an Intermediate hop.

- NHRP works in the hub and spoke topology. The hub is known as Next-Hop Server (NHS), and the spoke or client is known as the Next-Hop Client or NHC.

IPSec: GRE/NHRP can build a fully functional overlay network. GRE is insecure so it must be protected. IPSec is used to protect the traffic. IPSec is integrated with DMVPN, but this is not the essential part of DMVPN. Packets are encapsulated in GRE, and then IPSec is used to encrypt the packet. NHRP controls the tunnels, IPSec does the encryption IPSec profile is created and is applied on the tunnel interface. The IPSec profile is like a crypto map without "set peer" and "match address." IPsec uses a lot of gears to achieve high-level security. The primary protocols that IPsec uses are:

- **ESP (Encapsulation Security Payload):** ESP can provide data confidentiality and integrity, but cannot protect the IP header. The IP protocol number of ESP is 50.
- **AH (Authentication Header):** AH can provide the integrity service to the data packet, but cannot offer confidentiality to data packets like ESP. The IP protocol number of AH is 51.
- **IKE (Internet Key Exchange):** IKE provides support for the negotiation of parameters between end points or VPN peers and thus establishes, maintains and terminates security associations (SA). The SA termination can be based on time (seconds) or transfer (kilobytes) rate. The IKE is a type of ISAKMP (Internet Security Association Key Management Protocol) implementation, which is a framework for authentication and key exchange. IKE establishes the security association (SA) between two endpoints through a three-phase process.

Resources Used

The WAN encryption project is designed so that two IT staff can able to implement all the setup, though ideally more workforces should be dedicated to the deployment procedure if a speedy implementation is required. Once execution is complete, one employee will be needed to configure and troubleshoot the Cisco devices, but they will still have time to complete other technical support associated jobs.

At least one committed workforce is required for this WAN encryption project to deliver general coordination and continuity of the project. Splitting the responsibility for oversight of different phases between the various IT staff is not a good idea without a coordinator who can confirm communication is occurring through every step of project implementation. A dedicated project manager will confirm all milestones are accomplished, and the timeline is adhered to.

Funding will be required for the initial the Internet links procurements for all four branch offices before the DMVPN implementation. Also, additional workforce hours may be needed for a speed up the job. Also, the IT department had decided to deploy this project by using the in-house IT staffs and existing WAN infrastructures.

Final Output

Typically, data transfer between branch offices and corporate headquarters occurs over a service provider (SP) network or the Internet. Therefore, the WAN security is a highly important factor for any organization. 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. The final output of this project is

the deployment of the plan of action as a way of securing the WAN data encryption for protecting the WAN traffic using the existing Cisco WAN infrastructures and in-house IT workforces. By deploying this project, the business will be protected from severe cyber-attacks like Man-in-the-middle attack, IP spoofing attacks from their competitors and disgruntled employees.

Quality Assurance

The quality assurance is a suite for the systematic monitoring and evaluation of the different features of a project, service, or facility to confirm that standards of quality are being met. Auditing is a portion of the quality assurance function. It is essential to assure the quality because it is used to associate actual conditions with necessities and to report those outcomes to the management of the organization.

Quality Assurance Approach

The quality control principles are as below:

- The WAN traffic should be as protected and secured as the LAN (Local Area Network).
- The important client's data, employees personal information, and business data will not transfer over the WAN as unencrypted traffic.
- The most efficient and secure form of encryption will be utilized for all WAN traffic.
- The service provider’s WAN downtime will be kept to a lowest.

Criterion	The IT Department
All traffic on the WAN network should encrypt.	Monitors all WAN traffic to confirm that no unencrypted plaintext data is seen on the WAN connection.
WAN traffic should be secured from the cyber attack attempts.	Perform routine penetration and vulnerability testing to confirm all recommended security measures have been implemented.
Internet bandwidth monitoring and testing.	Perform routine Internet bandwidth monitoring and testing for verifying the guaranteed WAN link speed.

Solution Testing

VPN penetration testing will help the organization to baseline (detect the gaps that exist in the current execution and modify the configuration consequently to safeguard itself from known complications) its present VPN security stance, identify threats and flaws, and implement a new security procedure which will mitigate risks. The penetration testing of an IPsec VPN was comprised some stages like:

- Scanning or detecting the VPN gateway.
- PSK mode assessment and PSK sniffing.
- Offline PSK cracking.
- Testing the VPN gateway for vendor specific vulnerabilities like, Cisco.

The solution was initially rolled out for testing and development on a Windows 7 laptop. The Internet bandwidth performance testing was performed on Windows 7 laptop. The following acceptance standards are planned for final execution:

Milestone	Deliverable	Acceptance Criteria
Internet bandwidth testing	Internet speed 50 Mbps	All four locations have 50 Mbps upload and download Internet speed
Router IOS software version	Cisco securityk9 IOS technology package	All WAN routers have Cisco securityk9 IOS technology package installed
All traffic on the WAN network should encrypt.	Strong pre-shared key (PSK) authentication for IPSec VPN	Strong pre-shared key (PSK) had configured in all WAN routers
WAN traffic should be secured from the cyber attack attempts.	Complex pre-shared key (PSK) authentication for IPSec VPN	Complex pre-shared key (PSK) had configured in all WAN routers. Therefore authentication was secured.

Implementation Plan

This section should contain the details of an implementation plan. Provide details on how you would roll out the project, what kind of resources would be necessary, and the different

phases (if applicable). This should also contain details on end user training and documentation. Discuss the plan for implementing the project. Include the following in your discussion:

Strategy for the Implementation

The project was 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 had concrete steps and associated activities. While the stages, steps, and actions suggest a linear sequence of events, in the real execution there was often an additional dynamic flow to the work. Some stages or steps may be co-occurring, and the work often circles back to revisit the earlier phases. The reason subsequent succeeding stages were selected was to complete the whole project as quickly as possible so that the organization could begin gaining the benefits. The outcome of this project was WAN data encryption over the low-cost Internet link for cost efficient and enhanced secure solution.

Phases of the Rollout

Phases of the implementation will occur as follows:

Tasks Name	Testing	Criteria
Phase 1: Project Initiation		
1.1 Defines Project and its Scope	Build test case and feasibility study of project scope.	Define project scope. Refer the test case and review the scope with the related stakeholders.
1.2 Build a Business Case and Feasibility Study		
1.3 Meeting with Stakeholders		
1.4 Analysis Existing Network		
1.5 Creation of Project Charter		
1.6 Perform a Phase Review		
Phase 2: Project Planning		
2.1 Gather Functional and Technical Requirements	Verify the final project scope with the stakeholders and verify the proposed solution meets the requirements	Develop final project scope. Create proposed solution
2.1.1 Collect existing Network Diagram		
2.1.2 Gather existing Network Configuration		
2.1.3 Gather existing IP Scheme		
2.1.4 Gather existing Routing Information		
2.2 Finalize the Project Scope and Budget Requirement		

2.3 Identify Potential Risks and begin Managing Risks		
2.4 Develop a Project Schedule		
2.5 Create a Procurement Plan for new Internet link		
2.6 Create Design document of Proposed Solution		
2.7 Planning for Prototype Development and Testing		
2.8 Perform a Phase Review		
Phase 3: Project Execution and Control		
3.1 Build Prototype for Development and Testing	GNS3 simulator based configuration on a test router into the Windows 7 laptop.	Build GNS3 lab setup and analyzed the test results.
3.1.1 Build Prototype in GNS3 Network Simulator		
3.1.2 Configure GNS3 Network Simulator		
3.1.3 Performance Testing in GNS3 Simulator		
3.1.4 Security Testing in GNS3 Simulator		
3.1.5 Create Prototype Test Result Documents		
3.1.6 Prototype Test Result Analysis		
3.2 Securityk9 IOS Technology License Activation		
3.2.1 License Activation at Columbia HQ Router	Securityk9 IOS Technology License Activated successfully in all location.	Securityk9 IOS Technology License Activation successful.
3.2.2 License Activation at Charleston Router		
3.2.3 License Activation at Greenville Router		
3.2.4 License Activation at Florence Router		
3.2.5 License Activation at Orangeburg Router		
3.3 Routers Configuration	All routers configuration successfully. VPN tunnel has built. All required route information is there in EIGRP routing table.	All routers configuration successfully. EIGRP route configuration correctly.
3.3.1 Columbia HQ Router Configuration		
3.3.2 Columbia HQ User Acceptance Testing		
3.3.3 Charleston Spoke Router Configuration		
3.3.4 Charleston User Acceptance Testing		
3.3.5 Greenville Spoke Router Configuration		
3.3.6 Greenville User Acceptance Testing		
3.3.7 Florence Spoke Router Configuration		
3.3.8 Florence User Acceptance Testing		
3.3.9 Orangeburg Spoke Router Configuration		
3.3.10 Orangeburg User Acceptance Testing		
3.4 DMVPN Performance Monitoring		
3.5 Final Documents Creation		
3.6 Perform a Phase Review		
Phase 4: Project Closure		
4.1 Review Project Completion	Lessons learned and knowledge sharing session completed with	Experience and knowledge sharing session completed.
4.2 Perform Lessons Learned Analysis		
4.3 Finalize the Project Close-out Report		
4.4 Archive the Project Documentation		

	the IT services department.	

Details of the Go-Live

The WAN encryption project will be considered fully completed when all the remote locations will be able to communicate with the data center using the VPN tunnels. The entire remote locations user will be able to access the share resources in the data center. The WAN traffic will be kept protected and encrypted. In this way, the WAN traffic will be away from hackers' eyes. The IT department executive will validate the go-live. After the go-live, the entire DMVPN configuration will be fine-tuned with the help of Cisco TAC, and the end user support will be delivered to all locations.

Dependencies

The project dependencies are the interactions or inter relation of the preceding tasks to the following works. Tasks may have multiple preceding tasks and various succeeding tasks. The most common dependency relationship is a finish-to-start relationship. Some tasks are there which is not dependent on other tasks. For examples, GNS3 test lab setup is not dependent on another phase. The WAN router Securityk9 IOS Technology License Activation is not dependent with other phases. License activation can be done anytime. The WAN encryption project dependencies are described in the table below. For example, the outcomes of the current network analysis (Task-5) and the functional and technical requirement (Task-9) audit reports were required for design document of proposed solution (Task-18). Similarly, the task creates a procurement plan for new Internet link (Task-17) must be complete for finishing the router configuration (Task-35 to 42).

Task No.	Tasks Name	Duration
1	**Phase 1: Project Initiation**	**15 Days**

2	1.1 Defines Project and its Scope	4 Days
3	1.2 Build a Business Case and Feasibility Study	3 Days
4	1.3 Meeting with Stakeholders	2 Day
5	1.4 Analysis Existing Network	2 Days
6	1.5 Creation of Project Charter	2 Days
7	1.6 Perform a Phase Review	1 Day
8	**Phase 2: Project Planning**	**15 Days**
9	2.1 Gather Functional and Technical Requirements	5 Days
10	2.1.1 Collect existing Network Diagram	1 Day
11	2.1.2 Gather existing Network Configuration	2 Day
12	2.1.3 Gather existing IP Scheme	1 Day
13	2.1.4 Gather existing Routing Information	1 Day
14	2.2 Finalize the Project Scope and Budget Requirement	2 Days
15	2.3 Identify Potential Risks and begin Managing Risks	1 Day
16	2.4 Develop a Project Schedule	1 Day
17	2.5 Create a Procurement Plan for new Internet link	1 Day
18	2.6 Create Design document of Proposed Solution	3 Days
19	2.7 Planning for Prototype Development and Testing	1 Day
20	2.8 Perform a Phase Review	1 Day
21	**Phase 3: Project Execution and Control**	**60 Days**
22	3.1 Build Prototype for Development and Testing	15 Days
23	3.1.1 Build Prototype in GNS3 Network Simulator	3 Days
24	3.1.2 Configure GNS3 Network Simulator	3 Days
25	3.1.3 Performance Testing in GNS3 Simulator	3 Days
26	3.1.4 Security Testing in GNS3 Simulator	3 Days
27	3.1.5 Create Prototype Test Result Documents	2 Days
28	3.1.6 Prototype Test Result Analysis	1 Day
29	3.2 Securityk9 IOS Technology License Activation	5 Days
30	3.2.1 License Activation at Columbia HQ Router	1 Day
31	3.2.2 License Activation at Charleston Router	1 Day
32	3.2.3 License Activation at Greenville Router	1 Day
33	3.2.4 License Activation at Florence Router	1 Day
34	3.2.5 License Activation at Orangeburg Router	1 Day
35	3.3 Routers Configuration	25 Days
36	3.3.1 Columbia HQ Router Configuration	1 Day
37	3.3.2 Columbia HQ User Acceptance Testing	4 Days
38	3.3.3 Charleston Spoke Router Configuration	1 Day
39	3.3.4 Charleston User Acceptance Testing	4 Days
40	3.3.5 Greenville Spoke Router Configuration	1 Day

41	3.3.6 Greenville User Acceptance Testing	4 Days
42	3.3.7 Florence Spoke Router Configuration	1 Day
43	3.3.8 Florence User Acceptance Testing	4 Days
44	3.3.9 Orangeburg Spoke Router Configuration	1 Day
45	3.3.10 Orangeburg User Acceptance Testing	4 Days
46	3.4 DMVPN Performance Monitoring	12 Days
47	3.5 Final Documents Creation	3 Days
48	3.6 Perform a Phase Review	1 Day
49	**Phase 4: Project Closure**	**6 Days**
50	4.1 Review Project Completion	2 Day
51	4.2 Perform Lessons Learned Analysis	2 Day
52	4.3 Finalize the Project Close-out Report	1 Day
53	4.4 Archive the Project Documentation	1 Day

Deliverables

The main deliverables of this project existed Cisco setups like Cisco routers, IOS software, and design documentation. The existing Cisco routers were using for this project. Cisco 3945-SEC/K9 Integrated Services Router at a data center and all others four branches had Cisco 2911-SEC/K9 Integrated Services Router.

The other deliverable of this project was the design document. The design document consists of all related documents for deploying this project. It includes:

- Existing network architecture diagram
- Current routers configuration documents
- Existing IP scheme and routing information
- Proposed system architecture diagram
- Proposed IP system and route information
- Proof of concept result from prototype testing
- Recommend all configuration documents
- Software license up-gradation plan

- Implementation plan guideline and
- Support document manual creation.

Training Plan for Users

The WAN encryption project training will involve of two stages. In the first stage, all IT staffs at data center will be taught how to configure and troubleshoot the DMVPN technology using Cisco IOS Software including tunnel creation, IPSec, and routing, etc. In the second stage, all IT staffs of remote location will receive training on the DMVPN technology using Cisco IOS Software including tunnel creation, IPSec, routing, and troubleshooting, etc. This training will be a systematic learning through the use of group exercises, active discussion, and individual tasks to deliver an engaging and interactive module that will ensure all IT support staffs can transfer their new skills into the workplace.

Risk Assessment

The risk assessment is a procedure to identify possible threats and explore what could happen if a hazard happens. Although the WAN encryption has many benefits, it also adds business risk into daily operations. It is essential for the organization to consider all business risk comprising consequences and potential improvements earlier going ahead with the project.

There are several risks present during the different phases of project deployment. Although the WAN encryption delivers the value-added data encryption security for data communications using the Cisco gears and low-cost Internet link, some boundaries need to be aware of. The organization which is wanting to deploy the VPN had to confirm that adopting or considering the VPN was the best option for them. The VPN design and security deployment for the VPN are complicated. That means for implementing VPN; it is required experienced IT professional. The IT staffs should have 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 was used the 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.

The performance and reliability of the VPN can become a factor depending on the service provider that the organization is selecting for WAN communication. As 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.

Quantitative and Qualitative Risks

There are three primary risks were identified in the risk assessment conducted earlier to the WAN project execution:

Risk	Likelihood	Severity	Controllability	Overall Qualitative	Overall Quantitative
Hacker succeeds in penetrating the WAN network.	Low - IPsec and ISAKMP are not very vulnerable to attacks and would discourage most hackers.	High – In this case, severe damage could be inflicted on the LAN, and confidential company data could be stolen.	High – Measures can be taken to further secure the network including proper VPN configuration, and the use of strong passwords.	Low	This can't be quantified – potential of extremely high losses plus possible loss of customer base.
Router crashes during the business hours.	Medium – the router will have the heaviest load during hours of operation so would be most likely to hit them.	High – In this case, severe damage could be inflicted business will be down.	High – Measures can be taken to high availability/ redundant solution.	Low	This can't be quantified – potential of extremely high business losses plus possible loss of customer base.
Internet Link down during the office hours of operation.	Medium – the router will have the heaviest load during business hours of operation so would be most likely to crash then.	High – In this case, severe damage could be inflicted business will be down.	High – Measures can be taken to high availability / redundant solution.	Low	This can't be quantified – potential of extremely high business losses plus possible loss of customer base.

Cost/Benefit Analysis

Below are the possible benefit short falls and overrun consequences that correspond to the three identified risk areas:

Risk Area	Benefit Shortfall	Shortfall Cost	Cost Overrun	Overrun Consequences
Hacker succeeds in penetrating the WAN network.	IPsec and ISAKMP do not provide adequate protection like SSL from hacking. The Very low risk in the next 3 to 5 years.	Depends on what the hacker decides to do while on the network – a shortfall is not quantifiable.	The small business decides to implement AES encryption instead to provide higher security. Medium risk.	The existing Cisco securityk9 IOS technology package can support AES encryption. No additional cost involved.
Router crashes during the business hours.	Medium – All routers are protected with Cisco SMART net support (24x7x5) contract. So if Router crash Cisco will help to fix it. However, no redundant solution available.	All Cisco routers are protected with Cisco SMART net support (24x7x5) contract. For a redundant solution, each router approximately cost is $1500 to $2000.	The low risk that the business decides to upgrade redundant solution.	For a redundant solution, each router cost is $1500 to $2000 approximately.
Internet Link down during business hours.	Medium – the service provider should deliver 99.5% availability of the Internet link. However, no redundant solution available.	The service provider should deliver 99.5% availability of the Internet link. However, no redundant solution available. Another redundant Internet link cost is $100 to $120 for 50 Mbps link	The low risk that the business decides to upgrade redundant solution.	For redundant Internet link solution each 50 Mbps Internet link cost is $100 to $ 120.

Risk Mitigation

The risk, related to the WAN encryption plan comprises the WAN routers damage influenced by the sudden power failure, lightning, code failure, hardware failure, etc. These risk factors are unavoidable. The first risk mitigation technique is, if the router has hardware faults it can be replaced with new router received from Cisco, as all the routers are cover with Cisco SMART net 24x7x8 support. The pros of the new router will come with latest firmware and software code which will be much more stable compared to the old hardware. The cons of using a new router are it required new configuration from scratches. The second risk mitigation technique is high availability/ redundant Cisco router solution. The pros of the redundant Cisco router solution is if one router is down the backup router will be functioning. The cons of redundant Cisco router solution is it requires additional investment.

Another risk, related to the WAN encryption plan comprises the Internet link failure due to the ISP fault. The risk mitigation technique of the Internet link unavailability is procured another Internet connection or backup Internet link from different ISP for the organization. The pros of the secondary Internet link is if first Internet connection fails the services will be available from the backup Internet link. The cons of the secondary Internet link is it requires additional investment.

The last risk, related to the WAN encryption plan comprises hacker succeeding in the WAN traffic capture. The risk mitigation technique is implemented AES encryption for providing higher security. The pros of this are it uses a stronger algorithm for encrypting the traffic which is very difficult to decrypt by the hackers.The cons of this method are it will increase the payload of the data packet, which needs more CPU and memory processing power.

Post Implementation Support and Issues

To have an effective plan, there must be regular support and maintenance program to keep the product and services working properly. Excellent support guides help decrease the requirement for hiring costly external experts. On-going maintenance extends the working life of resources and reduces unintended down time. When executing a plan all initial guidelines and necessities need to be met, that what makes post implementation and support resources are crucial.

Post Implementation Support

Once the WAN encryption has implemented, all associates of the IT services department who did not directly take part in project execution will be given training on the DMVPN/ VPN operation and how to manage the setup. The administrator training is the primary line of support - it is essential that all admins know how the system works so they can identify any discrepancies. All associates of the IT services department will be able to offer tier one support and troubleshooting service after the training cycle is done.

Since the WAN encryption by deploying the DMVPN was specifically implemented for WAN traffic encryption, it is unlikely that tier two or three support will be required maximum for DMVPN troubleshooting. If members of the IT department encounter complications they cannot solve they can always refer to the Cisco TAC support by opening a new ticket.

Post Implementation Support Resources

The WAN encryption by deploying the DMVPN does not need a lot of support resources. The network & Security administrator will need to be on call during business hours to troubleshoot any WAN communication issues. No other workforces will be needed for daily support. Certain tasks in the maintenance plan may require the assistance of other IT workforces

to confirm timely task accomplishment. The project manager will be available for any escalation for post implementation support phase. For configuration and administration issues the network & security administrator can contact the Cisco TAC support.

Maintenance Plan

To better serve the customers needs the IT workforces will develop a short-term maintenance plan that covers many of the most common support cases that IT department handle. IT maintenance plan are those tasks which IT support staffs perform on a day-to-day basis, allowing for the upkeep of the network and services. Some of the more common network maintenance tasks include, but are not limited to, the subsequent common events:

- Installing, replacing or upgrading both hardware and software
- Monitoring, tuning and optimizing the network
- Documenting the system and maintaining network documentation
- Securing the network from both internal and external threats
- Planning for network upgrades, expansions, or enhancements
- Scheduling backups and restoring services or the network from backups
- Ensuring compliance with legal regulations and corporate policies
- Troubleshooting problem reports
- Maintaining and updating device configurations

To better serve our customers needs the IT department will develop a quarterly and annually long-term maintenance plan that covers many of the most common support cases that the IT department handle. The IT department will analyze the operation of the network and provide a breakdown of issues and potential problems that they find. System Maintenance checks include:

- Document network devices (switches/routers)
- Review device configuration
- Review DMVPN configuration
- Monitor the system logs.

The metrics collected via the network monitoring system will be reviewed quarterly and annually for trending results. The primary goal of this routine analysis will be to define any further need will be required.

Conclusion, Outcomes, and Reflection

As security is a critical factor in any network and the data transfer between branch offices and corporate headquarters occurs over the service provider (SP) network or the Internet. Therefore, the WAN security is a highly important factor in any business. Encryption is the process of altering 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.

Project Summary

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. Earlier the data center had another 10 Mbps MPLS host link

for branch office connectivity. All the branches were connected with the data center through the 1.5 Mbps MPLS link. The MPLS data communication was unencrypted data communication (Haran V., 2012). Due to the clear text unencrypted data transmission over the WAN link, there was a huge security risk involved for WAN communication. They were losing their business due to severe 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 was planning to cut off the IT budget for the corporation.

Therefore, after discussion with the directorate, the IT department had decided to implement the cost-effective, data encryption technology for branch offices WAN connection with improved performances. The best cost effective solution for addressing those issues was 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 WAN infrastructures of the organization were based on Cisco routers, so the IT department had decided to deploy Cisco DMVPN without additional hardware costs. The DMVPN is Cisco IOS software-based solution for building scalable IPsec VPNs. The IT department was analyzed that they may implement the same Cisco DMVPN over the MPLS link, but the MPLS is more expensive compared to the Internet link (Gottlieb A., 2012). Therefore, the IT department had decided to implement DMVPN over the public Internet connection for WAN traffic encryption. Also, the IT department had decided to deploy this solution by using the in-house IT staffs. By implemented the WAN encryption project, the IT department had

delivered secured value-added encryption for branch offices communications using the existing IT infrastructures and low-cost Internet link.

Deliverables

By implemented the WAN encryption project, the IT department had delivered secured value-added encryption for branch offices communications using the existing IT infrastructures and low-cost Internet link. Other deliverables of this project existed Cisco setups like Cisco routers, IOS software, and design documentation. The current Cisco routers were using for this project. Cisco 3945-SEC/K9 Integrated Services Router at a data center and all others four branches had Cisco 2911-SEC/K9 Integrated Services Router.

The other deliverable of this project was the design document. The design document consists of all related documents for deploying this project. It includes:

- Existing network architecture diagram
- Current routers configuration documents
- Existing IP scheme and routing information
- Proposed system architecture diagram
- Proposed IP scheme and route information
- Proof of concept result from prototype testing
- Recommend all configuration documents
- Software license up-gradation plan
- Implementation plan guideline and
- Support document manual creation.

Outcomes

There was an outstanding positive response from the stakeholders for this WAN encryption project. The implementation was very smooth and demonstrated the value of planning, coordination, and careful testing in GNS3. Issues and obstacles that were detected and resolved during the testing phase. In fact, the complicated nature of the deployment plan resulted in a 100% successful first-time roll-out for the massive deployment. When consideration is given to the political sensitivity and high visibility of this project it was an unqualified success.

Reflection

As a security consultant and technical expert for my organization, it was imperative that we are not only attempting to migrate the old systems or processes. Instead, we have implemented a new regime and a new “evolved” way of WAN communication and data encryption. The first step is awareness of alteration, followed by a readiness to grow, and finally careful planning and execution. Furthermore, the extensive testing regiment provided the stakeholders with strong confidence in the solution that resulted in fewer false-positive error reports. This expedited the overall rollout and significantly contributed to the project’s overwhelming success.

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

Cisco Systems. (2014). *VPN WAN Technology Design Guide*. Retrieved from http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf

Cisco Systems. (2016). *Cisco 3900 Series Integrated Services Routers Data Sheet*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/routers/3900-series-integrated-services-routers-isr/data_sheet_c78_553924.html

Cisco Systems. (2016). *Cisco 2900 Series Integrated Services Routers Data Sheet*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html

Cisco Systems. (2015). *Cisco's Integrated Services Routers Generation Two Licensing and Packaging*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/software-activation-on-integrated-services-routers-isr/white_paper_c11_556985.html

Miercom. (2016). *Lab Testing Summary Report*. Retrieved from http://miercom.com/pdf/reports/20091028.pdf

Cisco Systems. (2009). *Network Security Features for Cisco Integrated Services Routers Generation 2 Platform*. Retrieved from

http://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78-556151.pdf

Cisco Systems. (2014). *Network Security Features for Cisco Integrated Services Routers Generation 2 Platform*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78-556151.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

Gns3, ND, *Frequently Asked Questions*, online https://gns3.com/software/faq

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

Appendix A: Network Diagram

The old network diagram of ACME corporation is shown in Figure 1: Network Diagram illustrates how all the location was connected with the data center over the MPLS link. There were five routers attached to the MPLS as shown in the figure. They were as Columbia Router, Charleston Router, Greenville Router, Florence Router, and Orangeburg Router respectively.

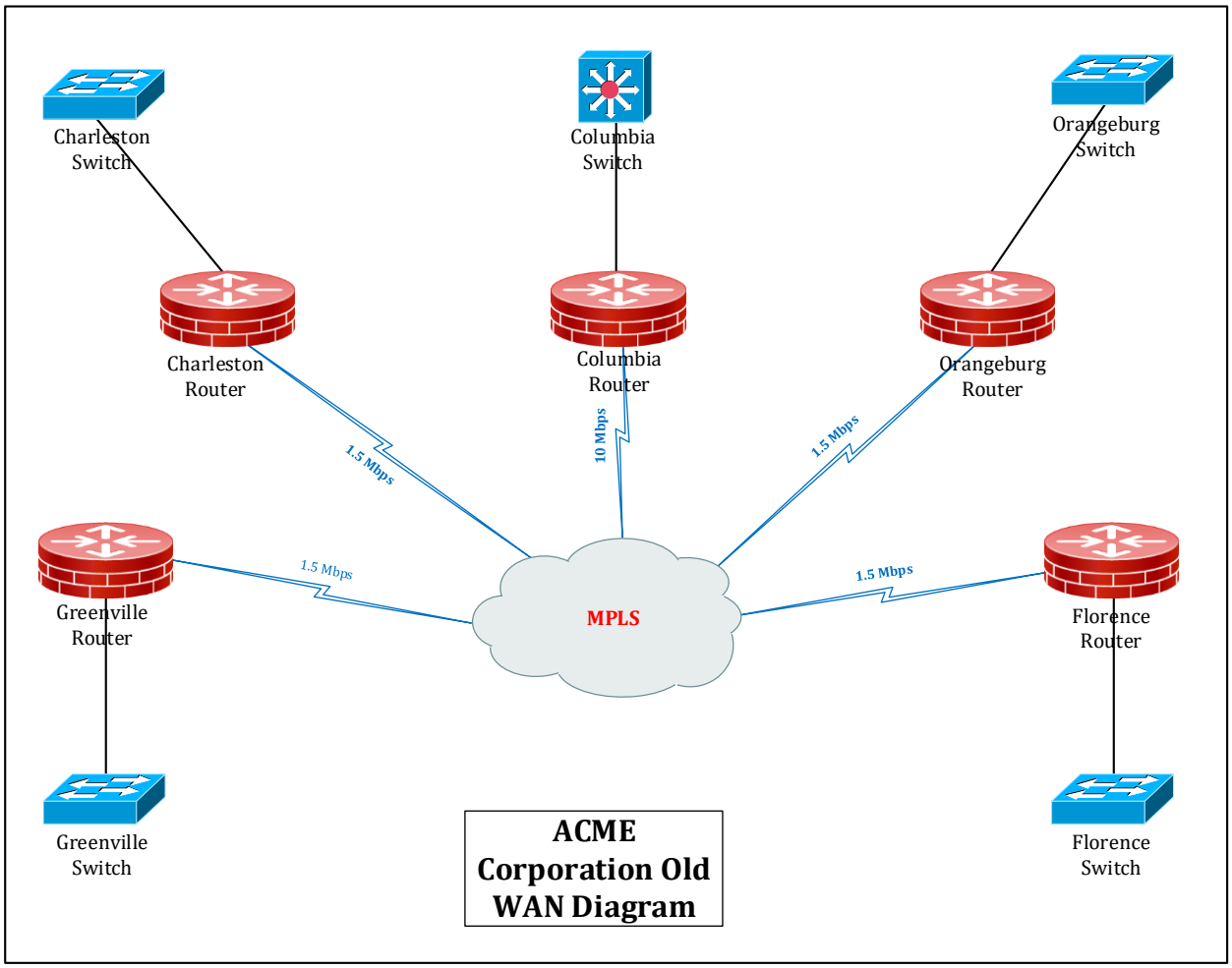


Figure-1

The current network diagram of ACME corporation is shown in Figure 2: Network Diagram illustrates how to configure the DMVPN. There are five routers connected to the Internet as shown in the illustration. They are as Columbia Router, Charleston Router, Greenville Router, Florence Router, and Orangeburg Router respectively. The Columbia router configured

as the hub router, and Charleston, Greenville, Florence, and Orangeburg routers are set up as the spoke routers.

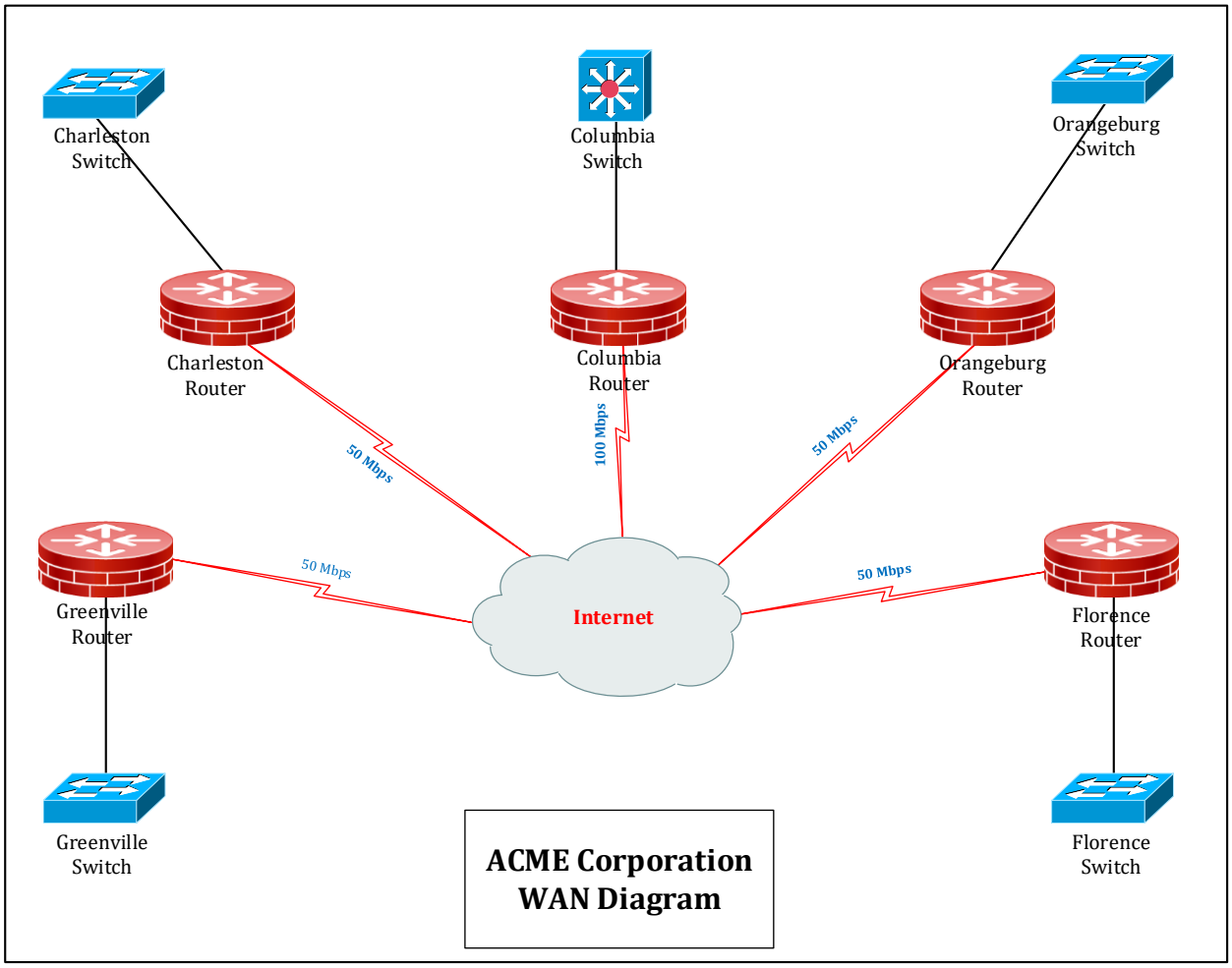


Figure-2

Appendix B: Implementation Configuration Document

Columbia HUB Router Basic Connectivity Details: The Columbia Router NBMA (non-broadcast multiple access) addresses or the public address is 192.160.10.1, and it is connected to the Internet. Subnet 172.16.1.0/24 is the protected corporate internal network.

```
Columbia-HUB-Rtr#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0     unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.324 192.160.10.1    YES NVRAM  up                    up
GigabitEthernet1/0     172.16.1.1      YES NVRAM  up                    up
GigabitEthernet2/0     unassigned      YES NVRAM  administratively down down
Tunnel0                10.1.1.1        YES NVRAM  up                    up
Columbia-HUB-Rtr#
```

Figure-3

Charleston Spoke Router Basic Connectivity Details: The Charleston Router NBMA (non-broadcast multiple access) address or the public address is 192.160.10.21, and it is connected to the Internet. Subnet 172.16.21.0/24 is the protected corporate internal network.

```
Charleston-Rtr#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0     unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.324 192.160.10.21   YES NVRAM  up                    up
GigabitEthernet1/0     172.16.21.1     YES NVRAM  up                    up
GigabitEthernet2/0     unassigned      YES NVRAM  administratively down down
Tunnel0                10.1.1.21       YES NVRAM  up                    up
Charleston-Rtr#
```

Figure-4

Greenville Spoke Router Basic Connectivity Details: The Greenville Router NBMA (non-broadcast multiple access) addresses or the public address is 192.160.10.31, and it is connected to the Internet. Subnet 172.16.31.0/24 is the protected corporate internal network.

```
Greenville-Rtr#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0     unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.324 192.160.10.31   YES NVRAM  up                    up
GigabitEthernet1/0     172.16.31.1     YES NVRAM  up                    up
GigabitEthernet2/0     unassigned      YES NVRAM  administratively down down
Tunnel0                10.1.1.31       YES NVRAM  up                    up
Greenville-Rtr#
```

Figure-5

Florence Spoke Router Basic Connectivity Details: The Florence Router NBMA (non-broadcast multiple access) addresses or the public address is 192.160.10.41, and it is connected to the Internet. Subnet 172.16.41.0/24 is the protected corporate internal network.

```
Florence-Rtr#
Florence-Rtr#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0     unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.324 192.160.10.41   YES NVRAM  up                    up
GigabitEthernet1/0     172.16.41.1     YES NVRAM  up                    up
GigabitEthernet2/0     unassigned      YES NVRAM  administratively down down
Tunnel0                10.1.1.41       YES NVRAM  up                    up
Florence-Rtr#
```

Figure-6

Orangeburg Spoke Router Basic Connectivity Details: The Orangeburg Router NBMA (non-broadcast multiple access) address or the public address is 192.160.10.51, and it is connected to the Internet. Subnet 172.16.51.0/24 is the protected corporate internal network.

```
Orangeburg-Rtr#
Orangeburg-Rtr#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0     unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.324 192.160.10.51   YES NVRAM  up                    up
GigabitEthernet1/0     172.16.51.1     YES NVRAM  up                    up
GigabitEthernet2/0     unassigned      YES NVRAM  administratively down down
Tunnel0                10.1.1.51       YES NVRAM  up                    up
Orangeburg-Rtr#
```

Figure-7

The configuration of DMVPN:

DMVPN requires the step-by-step configuration and verification of its various components. It involves the following four steps to complete the configuration of DMVPN:

1. Configuration of mGRE

2. Configuration and verification of NHRP

3. Configuration and verification of EIGRP

4. Configuration and verification of IPSec

The configuration of Columbia HUB Router:

```
Current configuration: 2234 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Columbia-HUB-Rtr
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone EDT -5 0
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
```

```
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set MINE esp-3des
 mode tunnel
!
crypto ipsec profile DMVPN
 set transform-set MINE
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 tunnel source 192.160.10.1
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 no ip address
 shutdown
```

```
 duplex auto
!
interface GigabitEthernet0/0
 description to Internet link
 no ip address
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet0/0.324
 description Columbia-DMVPN-HUB
 encapsulation dot1Q 324
 ip address 192.160.10.1 255.255.0.0
!
interface GigabitEthernet1/0
 description to LAN Interface
 ip address 172.16.1.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 1
 network 10.0.0.0
 network 172.16.0.0
 network 192.160.0.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
banner motd ^CC
**************************************************************************
*
*                                                                        *
```

```
*          UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED!          *
*                                                                     *
***********************************************************************
*
^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

Configuration of Charleston Spoke Router:

```
Current configuration : 2338 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Charleston-Rtr
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone EDT -5 0
no ip icmp rate-limit unreachable
!
!
!
!
!
```

```
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set MINE esp-3des
 mode tunnel
!
crypto ipsec profile DMVPN
 set transform-set MINE
!
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.1.1.21 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 1 35
```

```
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip nhrp map 10.1.1.1 192.160.10.1
 ip nhrp map multicast 192.168.10.1
 ip nhrp map multicast 192.160.10.1
 ip nhrp network-id 1
 ip nhrp nhs 10.1.1.1
 tunnel source 192.160.10.21
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description to Internet Link
 no ip address
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet0/0.324
 description Charleston-DMVPN-SPOKE
 encapsulation dot1Q 324
 ip address 192.160.10.21 255.255.0.0
!
interface GigabitEthernet1/0
 description to LAN Interface
 ip address 172.16.21.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 1
 network 10.0.0.0
 network 172.16.0.0
 network 192.160.0.0
!
ip forward-protocol nd
```

```
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
banner motd ^CC
**************************************************************************
*
*                                                *
*         UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED!          *
*                                                *
**************************************************************************
*
^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

Configuration of Greenville Spoke Router:

```
Current configuration : 2338 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Greenville-Rtr
```

```
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone EDT -5 0
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set MINE esp-3des
 mode tunnel
!
```

```
crypto ipsec profile DMVPN
 set transform-set MINE
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.1.1.31 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip nhrp map 10.1.1.1 192.160.10.1
 ip nhrp map multicast 192.168.10.1
 ip nhrp map multicast 192.160.10.1
 ip nhrp network-id 1
 ip nhrp nhs 10.1.1.1
 tunnel source 192.160.10.31
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description to Internet link
 no ip address
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet0/0.324
 description Greenville-DMVPN-SPOKE
 encapsulation dot1Q 324
 ip address 192.160.10.31 255.255.0.0
!
interface GigabitEthernet1/0
 description to LAN Interface
 ip address 172.16.31.1 255.255.255.0
```

```
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 1
 network 10.0.0.0
 network 172.16.0.0
 network 192.160.0.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
banner motd ^CC
**************************************************************************
*
*                                                                        *
*          UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED!             *
*                                                                        *
**************************************************************************
*
^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
```

```
!
!
end
```

Configuration of Florence Spoke Router:

```
Current configuration : 2334 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Florence-Rtr
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone EDT -5 0
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
```

```
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set MINE esp-3des
 mode tunnel
!
crypto ipsec profile DMVPN
 set transform-set MINE
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.1.1.41 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip nhrp map 10.1.1.1 192.160.10.1
 ip nhrp map multicast 192.168.10.1
 ip nhrp map multicast 192.160.10.1
 ip nhrp network-id 1
 ip nhrp nhs 10.1.1.1
 tunnel source 192.160.10.41
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description to Internet link
```

```
 no ip address
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet0/0.324
 description Florence-DMVPN-SPOKE
 encapsulation dot1Q 324
 ip address 192.160.10.41 255.255.0.0
!
interface GigabitEthernet1/0
 description to LAN Interface
 ip address 172.16.41.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 1
 network 10.0.0.0
 network 172.16.0.0
 network 192.160.0.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
banner motd ^CC
**************************************************************************
*
*                                                                        *
*         UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED!              *
*                                                                        *
**************************************************************************
*
```

```
^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

Configuration of Orangeburg Spoke Router:

```
Current configuration : 2338 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Orangeburg-Rtr
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone EDT -5 0
no ip icmp rate-limit unreachable
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
```

```
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set MINE esp-3des
 mode tunnel
!
crypto ipsec profile DMVPN
 set transform-set MINE
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.1.1.51 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip nhrp map 10.1.1.1 192.160.10.1
 ip nhrp map multicast 192.168.10.1
```

```
 ip nhrp map multicast 192.160.10.1
 ip nhrp network-id 1
 ip nhrp nhs 10.1.1.1
 tunnel source 192.160.10.51
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description to Internet link
 no ip address
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet0/0.324
 description Orangeburg-DMVPN-SPOKE
 encapsulation dot1Q 324
 ip address 192.160.10.51 255.255.0.0
!
interface GigabitEthernet1/0
 description to LAN Interface
 ip address 172.16.51.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 1
 network 10.0.0.0
 network 172.16.0.0
 network 192.160.0.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
```

```
!
!
!
!
control-plane
!
banner motd ^CC
**************************************************************************
*
*                                                                        *
*         UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED!              *
*                                                                        *
**************************************************************************
*
^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

Appendix C: Test and Verification

Verification on Columbia HUB Router:

Now the full secure tunnel has been created, and all the traffic are protected using the IPSec parameters.

The following Figure 8: Verification of IPSecshows that the Ike tunnels status between the routers.

```
Columbia-HUB-Rtr#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.160.10.1    192.160.10.21   QM_IDLE           1002 ACTIVE
192.160.10.1    192.160.10.51   QM_IDLE           1004 ACTIVE
192.160.10.1    192.160.10.31   QM_IDLE           1001 ACTIVE
192.160.10.1    192.160.10.41   QM_IDLE           1003 ACTIVE

IPv6 Crypto ISAKMP SA

Columbia-HUB-Rtr#
```

Figure-8: Verification of IPSec

```
Columbia-HUB-Rtr#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.160.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.160.10.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.160.10.21/255.255.255.255/47/0)
   current_peer 192.160.10.21 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1058, #pkts encrypt: 1058, #pkts digest: 1058
    #pkts decaps: 1058, #pkts decrypt: 1058, #pkts verify: 1058
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.160.10.1, remote crypto endpt.: 192.160.10.21
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x3A860B7D(981863293)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xA16307F2(2707621874)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 13, flow_id: 13, sibling_flags 80004040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4148474/2229)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x3A860B7D(981863293)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 14, flow_id: 14, sibling_flags 80004040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4148474/2229)
```

Figure-9: Encrypted Traffic

```
Columbia-HUB-Rtr#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:4,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.160.10.21          10.1.1.21    UP 01:12:55     D
     1 192.160.10.31          10.1.1.31    UP 01:12:52     D
     1 192.160.10.41          10.1.1.41    UP 01:12:47     D
     1 192.160.10.51          10.1.1.51    UP 01:12:43     D

Columbia-HUB-Rtr#
```

Figure-10: Tunnel built using NHRP

```
Columbia-HUB-Rtr#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Tunnel0
L        10.1.1.1/32 is directly connected, Tunnel0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet1/0
L        172.16.1.1/32 is directly connected, GigabitEthernet1/0
D        172.16.21.0/24 [90/26880256] via 10.1.1.21, 01:20:31, Tunnel0
D        172.16.31.0/24 [90/26880256] via 10.1.1.31, 01:20:31, Tunnel0
D        172.16.41.0/24 [90/26880256] via 10.1.1.41, 01:20:31, Tunnel0
D        172.16.51.0/24 [90/26880256] via 10.1.1.51, 01:20:31, Tunnel0
C     192.160.0.0/16 is directly connected, GigabitEthernet0/0.324
      192.160.10.0/32 is subnetted, 1 subnets
L        192.160.10.1 is directly connected, GigabitEthernet0/0.324
Columbia-HUB-Rtr#
```

Figure-11: Route information

```
Columbia-HUB-Rtr#ping 172.16.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/27/40 ms
Columbia-HUB-Rtr#ping 172.16.31.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.31.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/18/32 ms
Columbia-HUB-Rtr#ping 172.16.41.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.41.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/44 ms
Columbia-HUB-Rtr#ping 172.16.51.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.51.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms
Columbia-HUB-Rtr#
```

Figure-12: Ping Response

```
Columbia-HUB-Rtr#traceroute 172.16.21.1
Type escape sequence to abort.
Tracing the route to 172.16.21.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.21 48 msec 20 msec 20 msec
Columbia-HUB-Rtr#traceroute 172.16.31.1
Type escape sequence to abort.
Tracing the route to 172.16.31.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.31 44 msec 16 msec 20 msec
Columbia-HUB-Rtr#traceroute 172.16.41.1
Type escape sequence to abort.
Tracing the route to 172.16.41.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.41 40 msec 20 msec 20 msec
Columbia-HUB-Rtr#traceroute 172.16.51.1
Type escape sequence to abort.
Tracing the route to 172.16.51.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.51 28 msec 40 msec 28 msec
Columbia-HUB-Rtr#
```

Figure-13: Traceroute log

```
Log Buffer (8192 bytes):

*Jul 19 04:17:04.203: %PLATFORM-3-PACONFIG: Exceeds 600 bandwidth points for slots 0, 1, 3 & 5
*Jul 19 04:17:10.439: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Jul 19 04:17:10.455: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jul 19 04:17:10.467: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Jul 19 04:17:10.479: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
*Jul 19 04:17:10.971: %SYS-6-CLOCKUPDATE: System clock has been updated from 04:17:10 UTC Wed Jul 19 2017 to 23:
nsole.
*Jul 19 04:17:12.475: %SYS-5-CONFIG_I: Configured from memory by console
*Jul 19 04:17:12.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Jul 19 04:17:12.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Jul 19 04:17:12.775: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
*Jul 19 04:17:12.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to down
*Jul 19 04:17:12.783: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
*Jul 19 04:17:13.363: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)S5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Feb-14 06:51 by prod_rel_team
*Jul 19 04:17:13.607: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Jul 19 04:17:13.755: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Jul 19 04:17:14.287: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
*Jul 19 04:17:21.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
*Jul 19 04:17:37.395: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.21 (Tunnel0) is up: new adjacency
*Jul 19 04:17:39.123: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.31 (Tunnel0) is up: new adjacency
*Jul 19 04:17:44.463: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.41 (Tunnel0) is up: new adjacency
*Jul 19 04:17:49.903: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.51 (Tunnel0) is up: new adjacency
Columbia-HUB-Rtr#
```

Figure-14: Generated logs

Verification on Charleston Spoke Router:

Now the full secure tunnel has been created, and all the traffic are protected using the IPSec parameters.

The following Figure 15: Verification of IPSecshows that the Ike tunnels status between the routers.

```
Charleston-Rtr#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.160.10.1    192.160.10.21   QM_IDLE           1001 ACTIVE
192.160.10.21   192.160.10.41   QM_IDLE           1006 ACTIVE
192.160.10.31   192.160.10.21   QM_IDLE           1005 ACTIVE
192.160.10.21   192.160.10.31   QM_IDLE           1004 ACTIVE
192.160.10.51   192.160.10.21   QM_IDLE           1003 ACTIVE
192.160.10.41   192.160.10.21   QM_IDLE           1002 ACTIVE
192.160.10.21   192.160.10.51   QM_IDLE           1007 ACTIVE

IPv6 Crypto ISAKMP SA

Charleston-Rtr#
```

Figure-15: Verification of IPSec

```
Charleston-Rtr#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.160.10.21

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.160.10.21/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.160.10.31/255.255.255.255/47/0)
   current_peer 192.160.10.31 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
    #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.160.10.21, remote crypto endpt.: 192.160.10.31
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x5D9E03C6(1570636742)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xEDA4BFA(249187322)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 9, flow_id: 9, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4250531/3508)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)
      spi: 0xFD6539B8(4251269560)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 11, flow_id: 11, sibling_flags 80004040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3508)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound ah sas:
```

Figure-16: Encrypted Traffic

```
Charleston-Rtr#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:4,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.160.10.1           10.1.1.1    UP 01:25:58     S
     1 192.160.10.31         10.1.1.31    UP 00:00:06     D
     1 192.160.10.41         10.1.1.41    UP 00:00:11     D
     1 192.160.10.51         10.1.1.51    UP 00:00:06     D

Charleston-Rtr#
```

Figure-17: Tunnel built using NHRP

```
Charleston-Rtr#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Tunnel0
L        10.1.1.21/32 is directly connected, Tunnel0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
D        172.16.1.0/24 [90/26880256] via 10.1.1.1, 01:29:53, Tunnel0
C        172.16.21.0/24 is directly connected, GigabitEthernet1/0
L        172.16.21.1/32 is directly connected, GigabitEthernet1/0
D        172.16.31.0/24 [90/28160256] via 10.1.1.31, 01:29:51, Tunnel0
D        172.16.41.0/24 [90/28160256] via 10.1.1.41, 01:29:45, Tunnel0
D        172.16.51.0/24 [90/28160256] via 10.1.1.51, 01:29:38, Tunnel0
C     192.160.0.0/16 is directly connected, GigabitEthernet0/0.324
      192.160.10.0/32 is subnetted, 1 subnets
L        192.160.10.21 is directly connected, GigabitEthernet0/0.324
Charleston-Rtr#
```

Figure-18: Route information

```
Charleston-Rtr#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/22/24 ms
Charleston-Rtr#ping 172.16.31.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.31.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/26/48 ms
Charleston-Rtr#ping 172.16.41.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.41.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/26/44 ms
Charleston-Rtr#ping 172.16.51.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.51.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/36 ms
Charleston-Rtr#
```

Figure-19: Ping Response

```
Charleston-Rtr#traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.1 80 msec 20 msec 20 msec
Charleston-Rtr#traceroute 172.16.31.1
Type escape sequence to abort.
Tracing the route to 172.16.31.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.31 40 msec 28 msec 20 msec
Charleston-Rtr#traceroute 172.16.41.1
Type escape sequence to abort.
Tracing the route to 172.16.41.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.41 40 msec 20 msec 16 msec
Charleston-Rtr#traceroute 172.16.51.1
Type escape sequence to abort.
Tracing the route to 172.16.51.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.51 16 msec 56 msec 20 msec
Charleston-Rtr#
```

Figure-20: Traceroute log

```
Log Buffer (8192 bytes):

*Jul 19 04:17:08.207: %PLATFORM-3-PACONFIG: Exceeds 600 bandwidth points for slots 0, 1, 3 & 5
*Jul 19 04:17:19.879: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Jul 19 04:17:19.891: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jul 19 04:17:19.903: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Jul 19 04:17:19.915: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
*Jul 19 04:17:20.779: %SYS-6-CLOCKUPDATE: System clock has been updated from 04:17:20 UTC Wed Jul 19 2017 to 23:17
nsole.
*Jul 19 04:17:23.755: %SYS-5-CONFIG_I: Configured from memory by console
*Jul 19 04:17:24.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Jul 19 04:17:24.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Jul 19 04:17:24.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
*Jul 19 04:17:24.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to down
*Jul 19 04:17:24.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
*Jul 19 04:17:24.915: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)S5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Feb-14 06:51 by prod_rel_team
*Jul 19 04:17:25.211: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Jul 19 04:17:25.247: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Jul 19 04:17:25.395: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
*Jul 19 04:17:31.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
*Jul 19 04:17:37.311: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.1 (Tunnel0) is up: new adjacency
Charleston-Rtr#
Charleston-Rtr#show clock
*01:03:01.499 EDT Wed Jul 19 2017
Charleston-Rtr#
Charleston-Rtr#
```

Figure-21: Generated logs

Verification on Greenville Spoke Router:

Now the full secure tunnel has been created, and all the traffic are protected using the IPSec parameters.

The following Figure 22: Verification of IPSecshows that the Ike tunnels status between the routers.

```
Greenville-Rtr#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.160.10.31   192.160.10.41   QM_IDLE           1006 ACTIVE
192.160.10.41   192.160.10.31   QM_IDLE           1004 ACTIVE
192.160.10.21   192.160.10.31   QM_IDLE           1002 ACTIVE
192.160.10.31   192.160.10.51   QM_IDLE           1007 ACTIVE
192.160.10.1    192.160.10.31   QM_IDLE           1001 ACTIVE
192.160.10.51   192.160.10.31   QM_IDLE           1005 ACTIVE
192.160.10.31   192.160.10.21   QM_IDLE           1003 ACTIVE

IPv6 Crypto ISAKMP SA

Greenville-Rtr#
```

Figure-22: Verification of IPSec

```
Greenville-Rtr#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.160.10.31

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.160.10.31/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.160.10.21/255.255.255.255/47/0)
   current_peer 192.160.10.21 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 17, #pkts encrypt: 17, #pkts digest: 17
    #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.160.10.31, remote crypto endpt.: 192.160.10.21
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0xFD6539B8(4251269560)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xCAC1C41E(3401696286)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: 5, sibling_flags 80004040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4261131/3153)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)
      spi: 0x5D9E03C6(1570636742)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 7, flow_id: 7, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4239970/3153)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:
```

Figure-23: Encrypted Traffic

```
Greenville-Rtr#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:4,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.160.10.1           10.1.1.1    UP 01:33:59     S
     1 192.160.10.21         10.1.1.21    UP 00:08:10     D
     1 192.160.10.41         10.1.1.41    UP 00:02:49     D
     1 192.160.10.51         10.1.1.51    UP 00:02:43     D

Greenville-Rtr#
```

Figure-24: Tunnel built using NHRP

```
Greenville-Rtr#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Tunnel0
L        10.1.1.31/32 is directly connected, Tunnel0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
D        172.16.1.0/24 [90/26880256] via 10.1.1.1, 01:32:23, Tunnel0
D        172.16.21.0/24 [90/28160256] via 10.1.1.21, 01:32:23, Tunnel0
C        172.16.31.0/24 is directly connected, GigabitEthernet1/0
L        172.16.31.1/32 is directly connected, GigabitEthernet1/0
D        172.16.41.0/24 [90/28160256] via 10.1.1.41, 01:32:17, Tunnel0
D        172.16.51.0/24 [90/28160256] via 10.1.1.51, 01:32:10, Tunnel0
C     192.160.0.0/16 is directly connected, GigabitEthernet0/0.324
      192.160.10.0/32 is subnetted, 1 subnets
L        192.160.10.31 is directly connected, GigabitEthernet0/0.324
Greenville-Rtr#
```

Figure-25: Route information

```
Greenville-Rtr#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/29/76 ms
Greenville-Rtr#ping 172.16.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/25/40 ms
Greenville-Rtr#ping 172.16.41.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.41.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/93/172 ms
Greenville-Rtr#
Greenville-Rtr#ping 172.16.51.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.51.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/72/136 ms
Greenville-Rtr#
```

Figure-26: Ping Response

```
Greenville-Rtr#traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.1 40 msec 24 msec 16 msec
Greenville-Rtr#
Greenville-Rtr#traceroute 172.16.21.1
Type escape sequence to abort.
Tracing the route to 172.16.21.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.21 68 msec 24 msec 24 msec
Greenville-Rtr#traceroute 172.16.41.1
Type escape sequence to abort.
Tracing the route to 172.16.41.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.41 16 msec 60 msec 20 msec
Greenville-Rtr#traceroute 172.16.51.1
Type escape sequence to abort.
Tracing the route to 172.16.51.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.51 20 msec 64 msec 20 msec
Greenville-Rtr#
```

Figure-27: Traceroute log

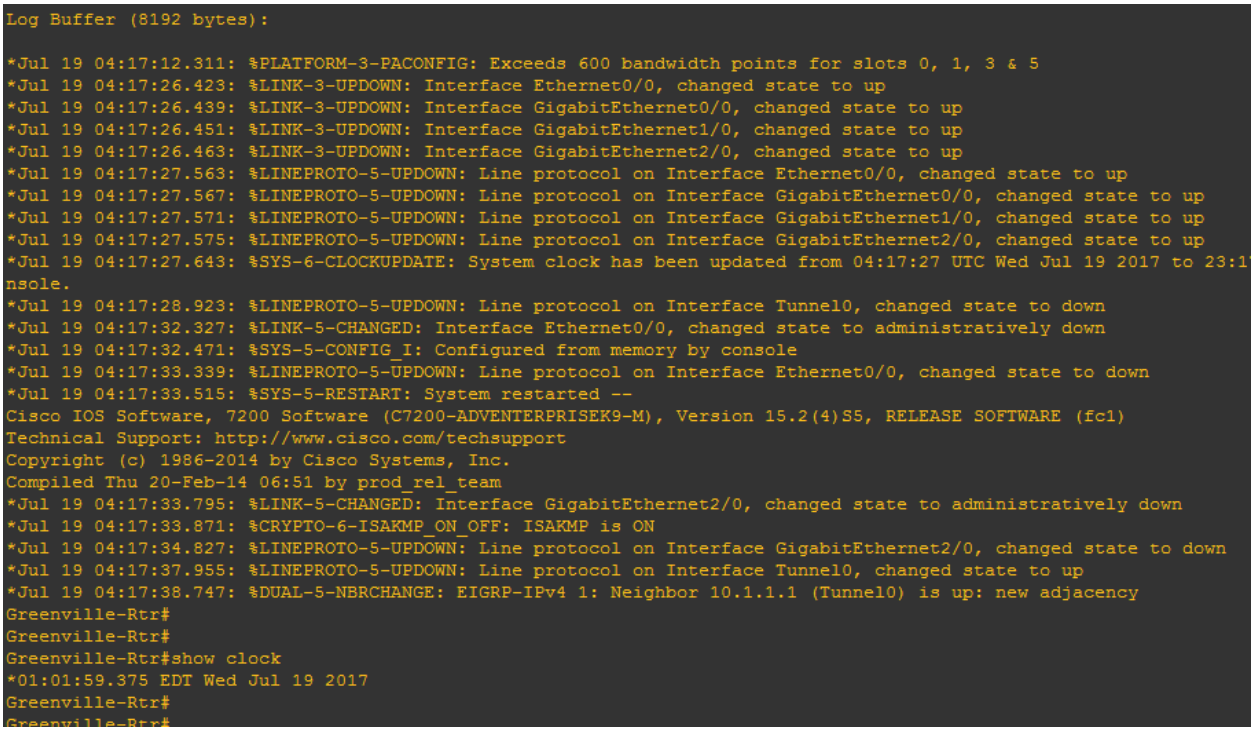


Figure-28: Generated logs

Verification on Florence Spoke Router:

Now the full secure tunnel has been created, and all the traffic are protected using the IPSec parameters.

The following Figure 29: Verification of IPSecshows that the Ike tunnels status between the routers.

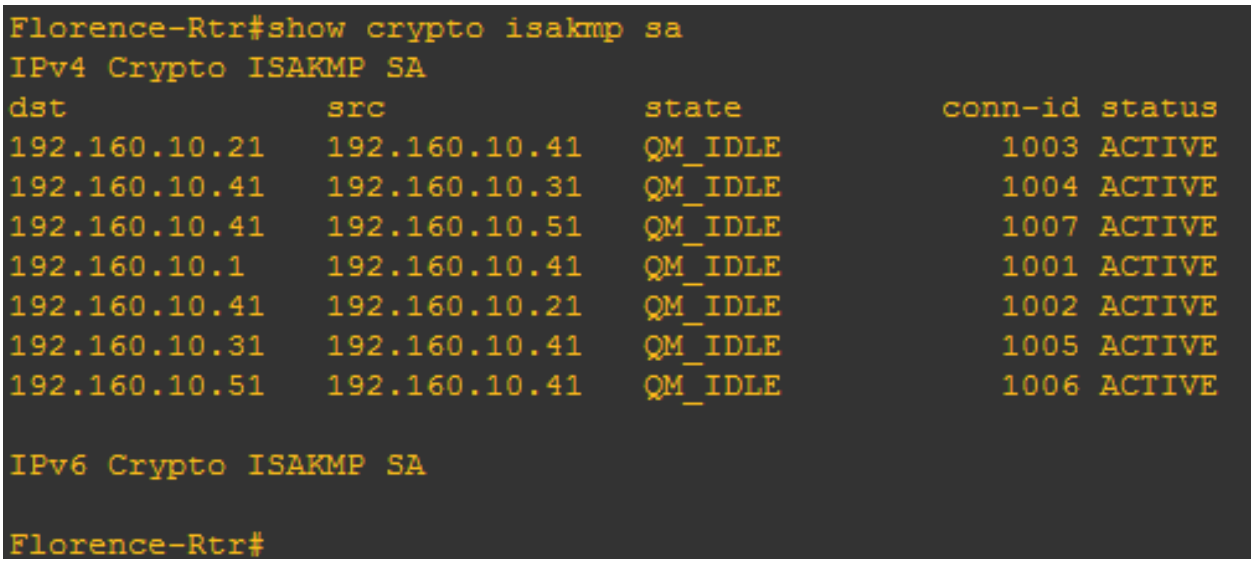


Figure-29: Verification of IPSec

```
Florence-Rtr#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.160.10.41

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.160.10.41/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.160.10.51/255.255.255.255/47/0)
   current_peer 192.160.10.51 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.160.10.41, remote crypto endpt.: 192.160.10.51
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x56544B54(1448364884)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x3229DE(3287518)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 13, flow_id: 13, sibling_flags 80004040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4361765/3408)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)
      spi: 0x4DB37893(1303607443)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 15, flow_id: 15, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4281896/3418)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:
```

Figure-30: Encrypted Traffic

```
Florence-Rtr#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:4,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.160.10.1           10.1.1.1    UP 01:37:23     S
     1 192.160.10.21         10.1.1.21    UP 00:11:45     D
     1 192.160.10.31         10.1.1.31    UP 00:06:19     D
     1 192.160.10.51         10.1.1.51    UP 00:02:41     D

Florence-Rtr#
```

Figure-31: Tunnel built using NHRP

```
Florence-Rtr#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Tunnel0
L        10.1.1.41/32 is directly connected, Tunnel0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
D        172.16.1.0/24 [90/26880256] via 10.1.1.1, 01:36:08, Tunnel0
D        172.16.21.0/24 [90/28160256] via 10.1.1.21, 01:36:08, Tunnel0
D        172.16.31.0/24 [90/28160256] via 10.1.1.31, 01:36:08, Tunnel0
C        172.16.41.0/24 is directly connected, GigabitEthernet1/0
L        172.16.41.1/32 is directly connected, GigabitEthernet1/0
D        172.16.51.0/24 [90/28160256] via 10.1.1.51, 01:36:01, Tunnel0
C     192.160.0.0/16 is directly connected, GigabitEthernet0/0.324
      192.160.10.0/32 is subnetted, 1 subnets
L        192.160.10.41 is directly connected, GigabitEthernet0/0.324
Florence-Rtr#
```

Figure-32: Route information

```
Florence-Rtr#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/33/84 ms
Florence-Rtr#ping 172.16.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/18/36 ms
Florence-Rtr#ping 172.16.31.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.31.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/36 ms
Florence-Rtr#ping 172.16.51.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.51.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/103/276 ms
Florence-Rtr#
```

Figure-33: Ping Response

```
Florence-Rtr#traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.1 88 msec 20 msec 20 msec
Florence-Rtr#traceroute 172.16.21.1
Type escape sequence to abort.
Tracing the route to 172.16.21.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.21 16 msec 20 msec 24 msec
Florence-Rtr#traceroute 172.16.31.1
Type escape sequence to abort.
Tracing the route to 172.16.31.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.31 20 msec 20 msec 20 msec
Florence-Rtr#traceroute 172.16.51.1
Type escape sequence to abort.
Tracing the route to 172.16.51.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.51 20 msec 20 msec 24 msec
Florence-Rtr#
```

Figure-34: Traceroute log

```
Log Buffer (8192 bytes):

*Jul 19 04:17:16.315: %PLATFORM-3-PACONFIG: Exceeds 600 bandwidth points for slots 0, 1, 3 & 5
*Jul 19 04:17:32.247: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Jul 19 04:17:32.263: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jul 19 04:17:32.275: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Jul 19 04:17:32.287: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
*Jul 19 04:17:33.147: %SYS-6-CLOCKUPDATE: System clock has been updated from 04:17:33 UTC Wed Jul 19 2017 to 23:17:
nsole.
*Jul 19 04:17:33.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
*Jul 19 04:17:33.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Jul 19 04:17:33.319: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
*Jul 19 04:17:33.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
*Jul 19 04:17:34.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
*Jul 19 04:17:37.223: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Jul 19 04:17:37.771: %SYS-5-CONFIG_I: Configured from memory by console
*Jul 19 04:17:38.459: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Jul 19 04:17:38.895: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
*Jul 19 04:17:38.995: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)S5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Feb-14 06:51 by prod_rel_team
*Jul 19 04:17:39.339: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Jul 19 04:17:39.895: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to down
*Jul 19 04:17:43.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
*Jul 19 04:17:43.759: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.1 (Tunnel0) is up: new adjacency
Florence-Rtr#
```

Figure-35: Generated logs

<u>Verification on Orangeburg Spoke Router</u>:

Now the full secure tunnel has been created, and all the traffic are protected using the IPSec parameters.

The following Figure 36: Verification of IPSecshows that the Ike tunnels status between the routers.

```
Orangeburg-Rtr#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.160.10.41   192.160.10.51   QM_IDLE           1007 ACTIVE
192.160.10.31   192.160.10.51   QM_IDLE           1005 ACTIVE
192.160.10.51   192.160.10.21   QM_IDLE           1002 ACTIVE
192.160.10.1    192.160.10.51   QM_IDLE           1001 ACTIVE
192.160.10.51   192.160.10.31   QM_IDLE           1004 ACTIVE
192.160.10.51   192.160.10.41   QM_IDLE           1006 ACTIVE
192.160.10.21   192.160.10.51   QM_IDLE           1003 ACTIVE

IPv6 Crypto ISAKMP SA

Orangeburg-Rtr#
```

Figure-36: Verification of IPSec

```
Orangeburg-Rtr#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:4,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.160.10.1           10.1.1.1    UP 01:40:33     S
     1 192.160.10.21         10.1.1.21    UP 00:14:54     D
     1 192.160.10.31         10.1.1.31    UP 00:09:28     D
     1 192.160.10.41         10.1.1.41    UP 00:05:55     D

Orangeburg-Rtr#
```

Figure-37: Tunnel built using NHRP

```
Orangeburg-Rtr#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Tunnel0
L        10.1.1.51/32 is directly connected, Tunnel0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
D        172.16.1.0/24 [90/26880256] via 10.1.1.1, 01:40:06, Tunnel0
D        172.16.21.0/24 [90/28160256] via 10.1.1.21, 01:40:06, Tunnel0
D        172.16.31.0/24 [90/28160256] via 10.1.1.31, 01:40:06, Tunnel0
D        172.16.41.0/24 [90/28160256] via 10.1.1.41, 01:40:06, Tunnel0
C        172.16.51.0/24 is directly connected, GigabitEthernet1/0
L        172.16.51.1/32 is directly connected, GigabitEthernet1/0
C     192.160.0.0/16 is directly connected, GigabitEthernet0/0.324
      192.160.10.0/32 is subnetted, 1 subnets
L        192.160.10.51 is directly connected, GigabitEthernet0/0.324
Orangeburg-Rtr#
```

Figure-38: Route information

```
Orangeburg-Rtr#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/18/48 ms
Orangeburg-Rtr#ping 172.16.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms
Orangeburg-Rtr#ping 172.16.31.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.31.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/24 ms
Orangeburg-Rtr#ping 172.16.41.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.41.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/38/100 ms
Orangeburg-Rtr#
```

Figure-39: Ping Response

```
Orangeburg-Rtr#traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.1 16 msec 20 msec 20 msec
Orangeburg-Rtr#traceroute 172.16.21.1
Type escape sequence to abort.
Tracing the route to 172.16.21.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.21 16 msec 8 msec 12 msec
Orangeburg-Rtr#traceroute 172.16.31.1
Type escape sequence to abort.
Tracing the route to 172.16.31.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.31 12 msec 20 msec 16 msec
Orangeburg-Rtr#traceroute 172.16.41.1
Type escape sequence to abort.
Tracing the route to 172.16.41.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.41 20 msec 20 msec 24 msec
Orangeburg-Rtr#
```

Figure-40: Traceroute log

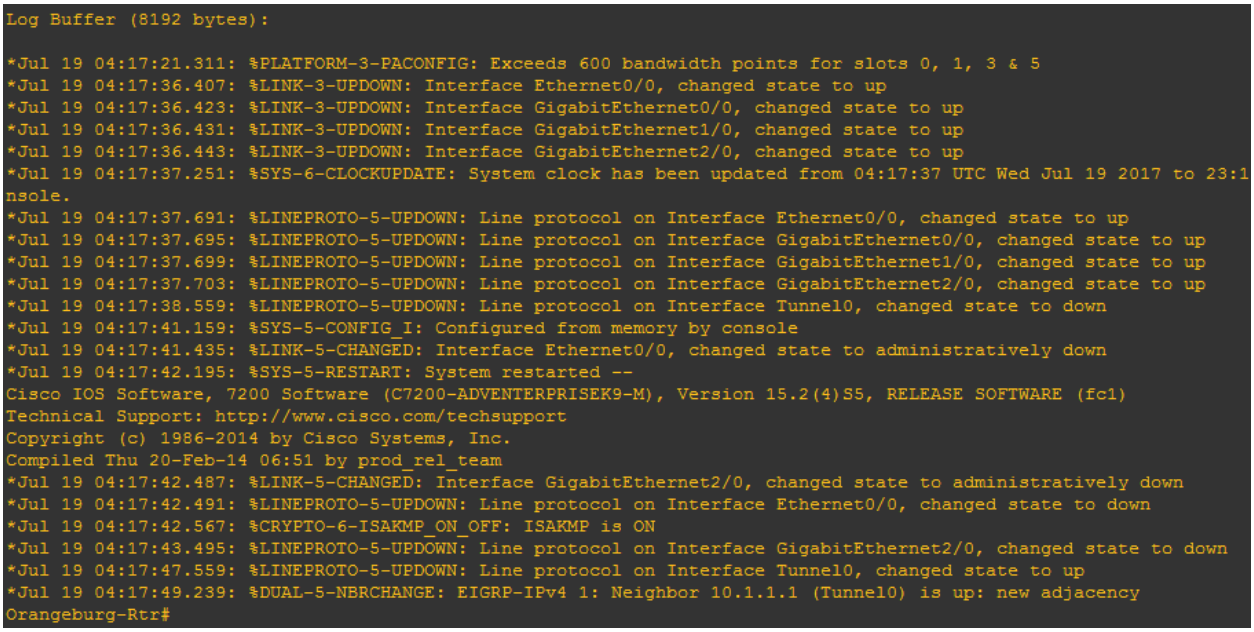


Figure-41: Generated logs