Journal of Applied Science and Advanced Technology
Journal Homepage : https://jurnal.umj.ac.id/index.php/JASAT

Analysis and Implementation of Backup Line Network Using Branch Office VPN and Speedy Internet Broadband

Kotim Subandi[1*],Adriana Sari Aryani[2]
[1]*Ilmu Komputer FMIPA Universitas Pakuan , Jl. Pakuan PO Box 452 Bogor 16143,Indonesia*
[2]*Ilmu Komputer FMIPA Universitas Pakuan , Jl. Pakuan PO Box 452 Bogor 16143,Indonesia*

ARTICLE INFO

JASAT use only:
Received date : 1 September 2018
Revised date : 7 October 2018
Accepted date : 13 November 2018

Keywords:
TCP/IP
VPN
Network
Speedy

ABSTRACT

The purpose of this research is to build computer network infrastructure that connects between head office and branch office (Site), so that all network connection performance can be upgraded to help and support the company's business objectives. In order for these needs can be met well and can overcome the problems of technology failure when communication and information exchange is underway, the technology will be used is a connection that can always be online with the aim that quality in service approaching 100% (service excellent). Network Infrastructure to be implemented is to use two lines of connection, the first is to use Telkom Metro Ethernet, and the second connection Branch Office VPN by using internet line broadband speedy from Telkom, if one of the connection down then the other connection as a backup, and if both connections are in stable and good condition, it can be ascertained both connections can serve conveying data simultaneously. Which is used to set the two connections in the topology holder built head office with Head Office(Site)is Cisco Router

INTRODUCTION

Computer networks are expected to connect two geographically different locations in order to communicate well and smoothly and safely. The company has an internal network, the existing connection is used to connect from the head office (Head Office) to the branch office (Site), the number of branches owned by more than one. The company is very utilizing the network with data connections from the head office to the branch office, all activities at the branch office that are integrated with all information systems, can be done using the metro Ethernet telecom connection, if there is no connection then all information system related activities will not goes well. All existing information systems in both the head office and branch offices consist of applications such as e-mail, intranet online applications, SAP, POS applications related to customers, and applications related to vendors / suppliers.

Not only is the metro Ethernet telecom connection used by the company to connect from headquarters to branch offices, but the company also utilizes BOVPN (Branch Office Virtual Private Network) technology. Today there is a growing number of public internet networks and many companies are using BOVP to connect from the branch office (Head Office). By utilizing BOVPN, for the needs of the cost is relatively cheaper compared to using a lease line connection, because the lease line connection is a point to point connection, while BOVPN uses the public network (internet) because of this internet network every company utilizes connections it is even used to make connections that are private with a level of security that already has a separate protection from the public internet connection. Generally data communication from one place to another has many methods in implementing SOP networks, one of which is using telecom metro Ethernet. For connections used, broadband

* Corresponding author.
E-mail address: kotim.subandi@unpak.ac.id

DOI: https://dx.doi.org/10.24853/JASAT.1.2.39-48

internet speedy, the constraints that occur are frequent disconnections caused by interference on the external side. So that the internet speedy network connection can return to normal conditions requires a relatively longer time due to the many problems during the cable installation process. One example for the cable installation process carried out on public roads or highways requires the tracking of cables that are more precise and accurate, for constraints in a particular area, requiring a licensing process to enter the area, for example industrial areas, government and so on. To overcome this problem an alternative connection is needed, if the main connection is broken, then the backup connection can work automatically, this is very important for national and international companies, because if the connection from the head office goes to the branch office (Site) the problematic or offline, then all activities related to the information system and applications that are connected to the network will stop, this greatly hampers the business objectives of the company can not be fulfilled and no connection can be reached in the current company from the head office to the branch office (Site), the main connection using the metro Ethernet network.

The purpose of this study is to overcome the constraints of exchanging information and data communication, if when the main connection is interrupted, an alternative backup connection will run according to its function automatically, and if both connections can run properly, the two connections can automatically be skipped for communication interests simultaneously, so that it can accelerate the process of information and data. If both connections are installed properly, the main connection and back up connection. Load balance in Cisco routers is a technique that is used to distribute traffic load on both of these connection lines or even more in a balanced manner, so that network traffic can run optimally, maximize throughput, shorten waiting times and avoid overload on one of the connection lines that have been implemented in network infrastructure.

EXPERIMENTAL METHOD

Identification of problems

Based on the conditions in the field of problems, the existing problems can be identified as long as the writer goes directly to the field, namely:

1. Requires a network system that has a backup line to anticipate interference on the line
2. Need a secure network to be accessed through public / internet networks
3. Requires a connection that is able to work automatically when a network breaks from the head office.

Analysis of field conditions

Almost all employees in the company's corporate users in every department, even when working hours for network users connected to the internet there are approximately 300 to 500 employees / users who need their activities via the internet to do things ranging from the SAP application email. Intranetonline application, FTP, VPN, social media, and there are several banking applications.

Analysis of System Weaknesses

In this study, for the analysis of existing system weaknesses, the authors use the SWOT method

1. **Strength Analysis**
   The results of the analysis obtained by the researchers when conducting an analysis of PT. Panen Lestari Internusa (SOGO) there are some strengths or strengths obtained by the researcher, among others, the ability to observe and understand all information and internet system activities that are good by the company so as to facilitate the user uses a new system. Configuration experience, system installation both software and hardware by the company provides convenience in designing and implementing a new network topology that will be implemented
2. **Weakness Analysis**
   The following is a weakness analysis of PT. Panen Lestari Internusa (SOGO) has limitations in running both configuration access, installation due to the infrastructure that is based on MAN, WAN making it difficult when controlling and monitoring the network. The security system that is on the PT. Panen Lestari Internusa (SOGO) network is still vulnerable to attacks from outside the network.

3. **Opportunities Analysis**
   For this one analysis aims to understand and see opportunities from PT.Panen Lestari Internusa (SOGO) in the future is good reliability in understanding all system installation activities, configuration from PT. Panen Lestari Internusa (SOGO) which is expected to be able to develop a wider network and better by adding cover distance to the scope of the network.
4. **Threats Analysis**
   From some of the results of the analysis obtained by the author against attacks and threats that can penetrate network security defenses at PT. Panen Lestari Internusa (SOGO) is competition with several existing companies (competitors) that continue to grow so as to give an impact in the form of threats to families PT. Panen Lestari Internusa (SOGO) network.

Solution Problem Solving

The solution that will be applied to wrestle security issues on the internet network is by creating a SOP (Standard Operation Procedure) for the user so that users can access without causing light barriers that originate from unwanted users.

System Requirements Preparation

In this stage is the preparation of the installation and configuration of all devices that will be used, which include the needs of hardware, software and users.

RESULTS AND DISCUSSION

Hardware needed.

In this installation and configuration the required hardware is.

1. Personal Computer
   The device used to install and configure all devices used. Includes User Authentication configuration
2. Modem Linksys AG241
   This Links24 AG241 is a modem that uses ADSL technology (via the PSTN telephone line) for an internet connection that is faster than using a modem dial up model.
3. Watchguard X10e-W
   One very reliable tool to provide large-scale security and data centers that require a high level firewall, application control and instruction prevention system
4. Switch
   Ethernet switch to carry out the switching task of data packets and monitor their physical address. This type of switch works on the data link layer or the second layer in the OSI reference model
5. ADSL Modem
   Is a device used to connect a computer or router to a telephone line, to use ADSL services Like other modem types, the ADSL modem is a transceiver
6. Cisco Router
   The main equipment that is widely used in Broad Area Networks or Wide Area Networks (WAN). With Cisco routers, information can be forwarded to addresses that are far apart and located on different computer networks. Which aims to be able to forward data packets from a LAN to another LAN, Cisco routers use tables and routing protocols that function to regulate data traffic in the network.

Software that will be used

Software needed for configurations such as Linksys, which can be obtained free of charge through the official website (www.dyndns.com), and several applications at (www.watcgurguard.com)

Human Resources needed

Human resource requirements include man power that is involved in network system design and computer network topology design, among others.

1. Administrator, here the administrator is assigned as a computer network system controller, configure and maintaining network systems
2. User is a client or person who engages in using the computer network

System planning

The design of this system is needed to know and make sure the line speedy is installed, so that you can test network connections how the dedicated line connection system from the branch office goes to the head office in the Jakarta area using metro Ethernet Telkom can work properly.

Planned System

The system planned in the PT. Panen Lestari Internusa network (SOGO) is from the WAN1 Port in WatchGuard connected to the Ethernet port on the Modem, the LAN0 port on the WatchGuard is connected to the core switch, in addition to the WAN1 and LAN0 ports in the WatchGuard are not used. The system

algorithm that will be designed on the Backup Line Network using the PT. PLI-Indonesia network (SOGO) is as follows:

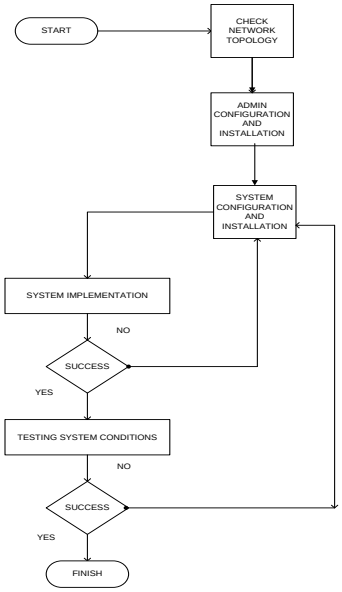

Fig.1. Algorithm of the Installation software system

Increased performance and quality of the Backup Line Network and network security can run well according to the design and topology that has been built so it requires the support of some software on the hardware installed in the network topology

1. Dyndns

Dyndns.com is a very simple cloud based application for serving the host

Fig. 2. Host Service

2.VPN

VPN is a utility tool that is used to remotely host a central office to a branch office using SSH (secure shell).

3. Server 2012

Is the operating system needed specifically for server needs. With a variety of features that are very competent and have very simple settings Windows server 2012 is an alternative choice, both for beginners who do not understand the operating system at all, even those who are professionals who need the best capabilities of the Windows Server OS 2012.

Configure the system and implement the system to configure WatchGuard as a BOVPN (Branch Office Virtual Network Private) in accordance with the SOP (Standard Operation Procedure) that has been created so that when testing the network system, along with the features that are already installed in Network topology can run according to the intended destination

System Work Analysis

Monitor and analyze whether the implemented system is running in accordance with the desired goals or not, if the system is successful, the process is continued at the system testing stage and if the system has not been successful it must be re-checked the system configuration then analyzed so that it can be concluded that an error during configuration.

Final System Testing

It must be ensured that the configuration that has been carried out has been able to run based on the SOP that has been made and how the function of the system is built whether the capability has been tested as it was done during the analysis.

Network Topology Implementation

Designing and building a computer network infrastructure should first make a sketch of the type of topology that will be built because with the network topology a network administrator will more easily implement the configuration on a dedicated line connection from the branch office to the head office, the topology applied is the existing topology in PT. PLI-Indonesia (SOGO) in Figure 3 below is the network topology when implementing the system:

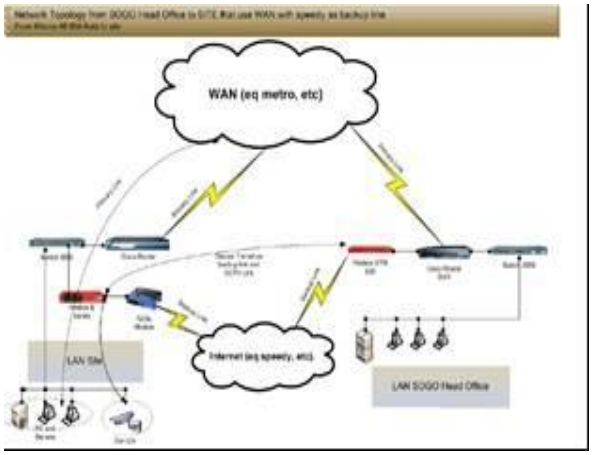

Fig.3. Network Topology Head Office to Branch Offices

There are several solutions that can be applied to realize the formulation of the problems that have been written in the previous chapters. It is necessary to do the system configuration process in order to enter into these stages, there are several steps that must be passed first, including

Configure the Linksys Modem

To do a configuration on a Linksys Modem, the process turns on by installing and continuing it by pressing the adapter button then connecting the Linksys modem Ethernet port to your PC. Set IP PC to 192.168.1.2 because IP default on modem 192.168.1.1 then open Mozilla browser. then open 192.168.1.1 after that you are asked to enter your username and password with the default admin mode (admin), then you can change the username to adminps (Example for PS) the Linksys admin password becomes (for example ch0t1m). in Figure 4. display for administration setup

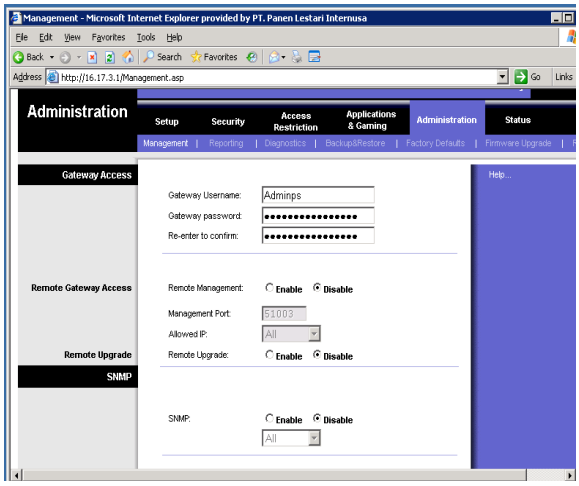

Fig. 4. Setup User& Password admin.

Then Change the Linksys IP to 16.17.3.1 (3 represents branch_id 003 for example PS as a branch office) this is to facilitate an administrator when configuring a connection from branch to head office and set the connection to be as shown below

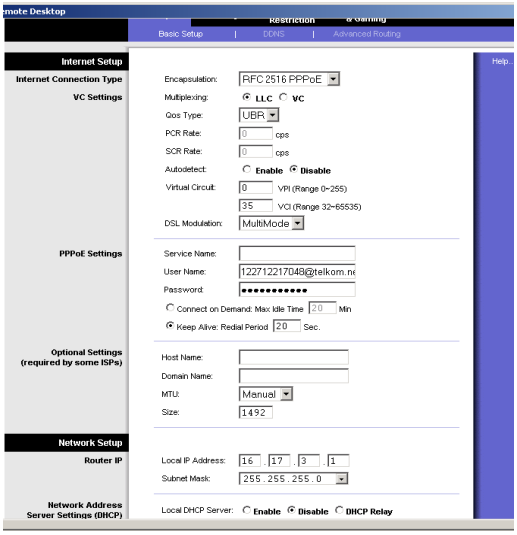

Fig. 5. IP Settings at the Branch Office

Set DMZ IP to 16.17.3.2 (IP external WatchGuard). A very simple Demilitarized Zone is a feature that allows devices behind the modem to be accessed from the internet. This brought image shows if the DMZ has been active and directed to IP 16.17.3.2

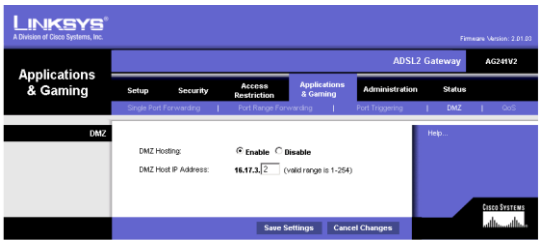

Fig. 6. Setup IP DMZ

DynDNS.org also provides services that are free, so researchers strongly recommend choosing DynDNS.org, at this stage the author creates an account at DynDNS.org, then select "Add Host Service", and fill in the image below:

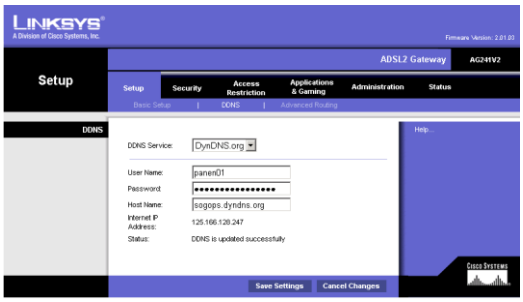

Fig. 7. Setting DDNS di Linksys

Determining Hostname: choose the subdomain and domain that will be used (sogops.Dyndns.org) to point to the IP that has been configured at the beginning, then create a username and password to provide the Ip Address network security system: what is used is IP 125.168.128.247

Base Hardware

All-in-one Internet-sharing router, 4-port switch, and Wireless-G (802.11g) AP 54Mbps Share one internet connection and another source with wired and Wireless-G Ethernet devices, Push button settings feature makes wireless configuration safe and simple, High security: because there are TKIP and AES encryption, there is wireless MAC addressing, a strong SPI firewall.

Configure WatchGuard

Before the configuration is done, surely the product activation is www.watchguard.com with username (for example: FoodhallInd and password u4rd14n), write the WatchGuard serial make sure the Active Product "has been inputted with the serial number. In product information" name this product "is filled in by the branch office code (example: FHGB), for End User License. there is select agree on Activation Center all detailed information will appear, serial_ number lincese_id etc. save all information in notepad

Activate the WatchGuard box

Connect the LAN0 port to the monitor to the PC using a straight cable, Set the LAN LAN on the Computer / PC to automatic then go to https://192.168.111.1 Make sure you have done the "next" process until the "Accept" step and then select the internet connection method at the branch office concerned. Eq: PPOE

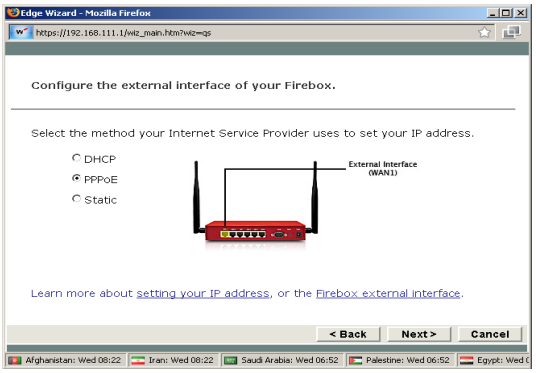

Fig. 8. Interface IP Settings

Make sure that you have filled in the username, domain (if any) and password then fill in the IP that will be used as a gateway (Local Site Network) for the relevant branch office.

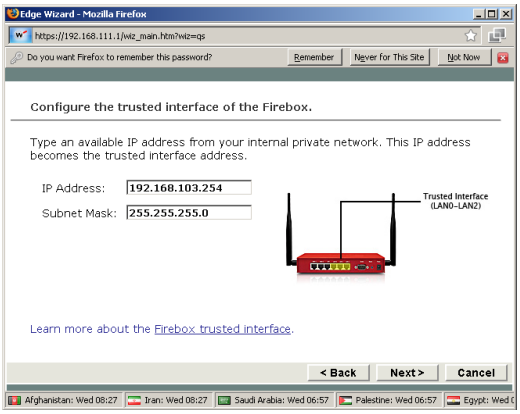

Fig. 9. Branch Office IP Settings

Make sure you have filled the passphrase with the standard (admin), then do all the activation steps until the finish and we are ready to upgrade the firmware and configuration

Upgrade firmware WatchGuard box.

In order to upgrade with the latest version, make sure to download the latest firmware, https://www.watchguard.com,archive/softwarecenter.asp, then change the IP LAN on the computer to become a segment with IP Firebox. After the IP change process is complete, make sure to execute the executable file until all processes are declared finish as shown in Figure. 10

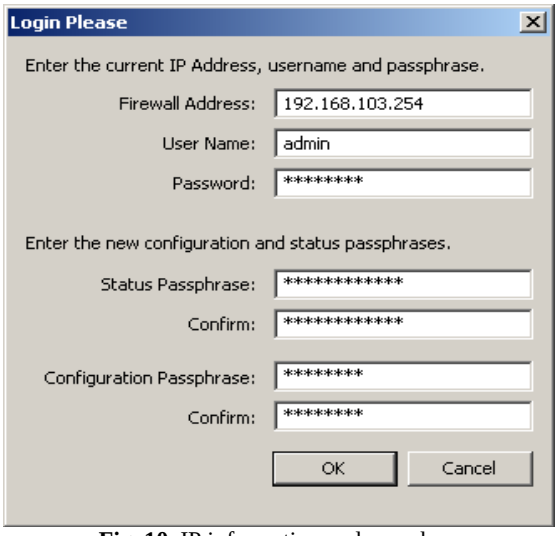

Fig. 10. IP information and passphrase

Fig. 11. Firmware finish upgrade

Configure the WatchGuard box

After the WatchGuard has been upgraded, the next step is to configure the WatchGuard box. first make sure to https: // ipfirebox: 8080 via the browser do login to the WatchGuard box using the passphrase that was created at the beginning in figure 11

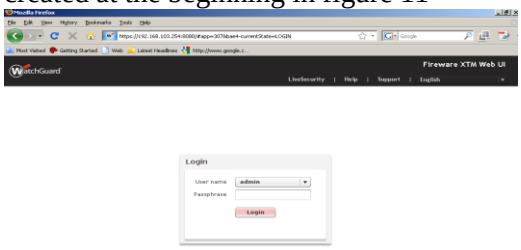

Fig. 12. Login Admin Menu

Checking the condition of the network system has been configured in a way after Login using the admin and then enter the system, in the system then fill in the information make sure the condition of the status link of the IP that has been set (example 192.168.103.254) is active "up" as shown in Fig. 13

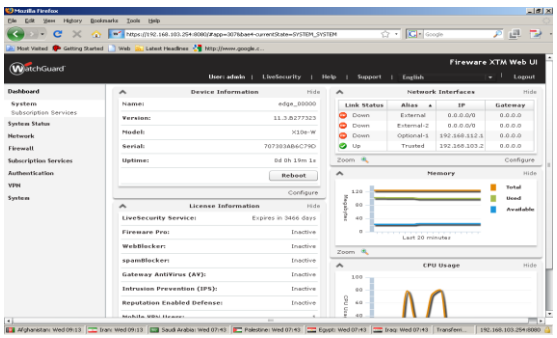

Fig. 13. Device Information

Set the Firewall Policies in order to control and monitor the data packets that will pass on the network by configuring the WatchGuard Firewall must be able to filter and control permitted data traffic to access private networks protected by firewalls. Perform authentication of access to record every transaction occurring in the firewall. it has been entered later Firewall (Firewall Policies), for outgoing systems then it must be edited and which is embedded to any external specifically the IP server and IP WatchGuard only, the next stage the WatchGuard must be edited from to any, "save" Make sure Firewall, Firewall Policies, section the form becomes any like Fig 14

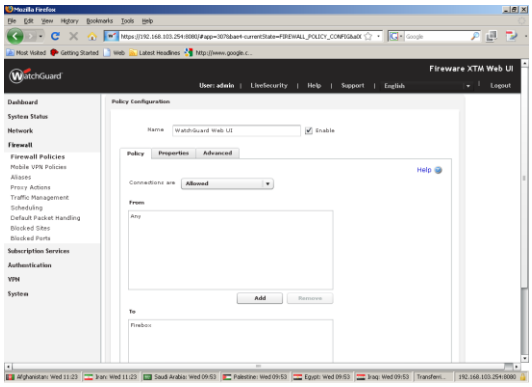

Fig. 14. Policy Configuration

Configure BOVPN WatchGuard at the Branch Office

The initial stage make sure you have chosen the VPN menu then Branch Office VPN. Then select the gateway then add. (Gateway name: for example SOGOHO Preshared key: 123456789) as shown in the picture below:

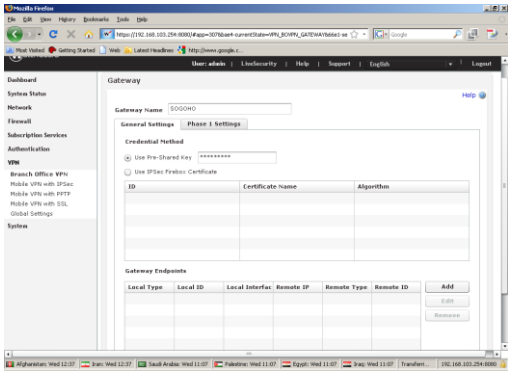

Fig. 15. Gateway

Followed by the Gateway endpoints configuration choose add this to determine the local gateway to the domain by name "sogodyndns" fill in the remote gateway by selecting static IP addresses, and specifications of the gateway id IP address to tunnel with IP

202,171.8,196, as in Figure 14, Stage next determines Phase1 Settings. By entering Nat Traversal: 60 seconds, IKE Keep-alive: 60 Seconds with 5 max failures., Dead Peer detection: 20 seconds with 5 max failures. Transform Settings: SHA1-DES for phase1 transform with Diffie-Helman group 1 key group and SA life 24 hours, as shown below

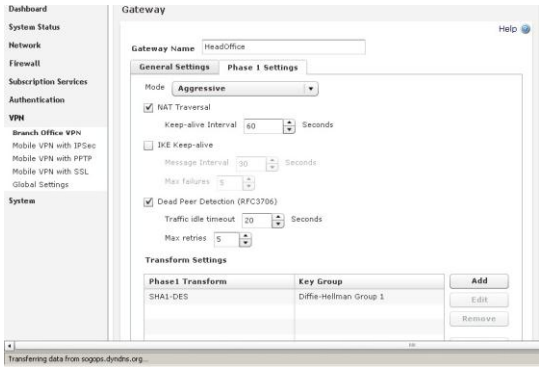

Fig. 16. Gateway VPN

System Testing

The testing phase of this system the author performs 2 testing processes against the configuration that has been made in the discussion in the previous chapter. The test will be carried out in the form of testing on

1. Testing the Switch Over

This test is very necessary to find out whether there is still a frequent disruption of the primary network from the side of the branch office and will use line backup, namely speedy, from the side of the branch office do not need to reconnect or no trigger, which needs to be done at the central office, namely removing routing at the branch office concerned in the backhaul only at the head office, as shown in the picture below

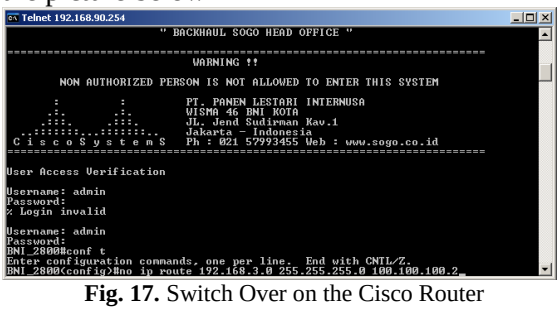

Fig. 17. Switch Over on the Cisco Router

2. Testing the Back Switch.

Testing of interference at the branch office when using the backup line has been solved, to switch back is able to return the primary line by way of even routing backhaul in the central office to the primary line, as in Figure 18.

Fig. 18. Switch Back on Cisco Route

CONCLUSION

After all the testing process has been successfully carried out, the implementation of the research with the title "Analysis and Implementation of Back Up Line Network Using Branch Office VPN and Speedy Internet Broadband" can be taken as follows:.

1. Telkom Metro Ethernet can be a connection between two connection lines located at the head office and the connections that are in the branch office
2. Line broadband internet speedy becomes back up line if one connection is down
3. The Cisco Router is used to manage both connections in the network between the head office and the branch office
4. If there is a disturbance in the primary network at the branch office and will use line backup, that is speedy, from the branch office, there is no need to do something or there is no trigger. switch over to branch offices
5. If the branch office interference using line backup has been solved, then to switch back to the primary line is to add routing in the backhaul of the head office to the primary line. Keep in mind that after switching back Success Sometimes there are still TCP connections that do not all use primary lines or still use backups, because when the switch back the TCP connection is still established

ACKNOWLEDGMENT

The Editor's Board would like to thank you for your willingness to review our manuscript that was published in this edition, and we thank you to all the colleagues who have helped resolve this journal.

REFERENCES

[1] Abdul Syukur., Liza Julianti., 2018 Simulasi Pemanfaatan *Dynamic Routing Protocol EIRP* Pada *Route*r di Jaringan Universitas Islam Riau Beserta Autentikasinya. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.201851535 Vol. 5, No. 1, Maret 2018, hlm. 23-34

[2] Andy Hidayat Jatmika., Royana Afwani., 2018, Analisis Dan Perancangan Arsitektur *Community Cloud Computing* Untuk Menunjang Pelayanan Kesehatan Ibu Dan Anak (Studi Kasus: Puskesmas Se-Kota Mataram), Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.201851538 Vol. 5, No. 1, Maret 2018, hlm. 51-56

[3] BALBONI, P., 2009. *Cloud computing for ehealth data protection issues. ENISA Working Group on Cloud Computing*. Daryanto, 2010, *Teknik Jaringan Komputer*. Alfabeta, Bandung. 168 halaman

[4] M. Asmuddin Ahmad. , Kusnawi., 2012 Analisa dan Implementasi web Proxy Clearos Sebagai otentikasi jaringan Aminers Spot , JURNAL DASI ISSN: 1411-3201Vol. 13 No. 2 JUNI 2012

[5] SAREEN, P., 2013. *Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud. International Journal of Advanced Research in Computer Science*

[6] Wagito. 2007. "Jaringan Komputer (Teori dan Implementasi Berbasis Linux)" Yogyakarta:Gava Media

[7] WIJAYA, CHANDRA, 2011, Simulasi Pemanfaatan Dynamic Routing Protokol OSPF Pada Router di Jaringan Komputer Unpar :Tesis M. T