# Designing a Secure and Reliable Network using EIGRP, VPN, DMZ and IDS/IPS

**Benfano Soewito[1] and Berkah I. Santoso[2]**

[1,2]Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer – Universitas Bakrie
[1]benfano.soewito@bakrie.ac.id, [2]berkah.santoso@bakrie.ac.id

*Abstract*— **Nowadays networking is not something new for us, we have hear about networking applications and problems every day at the present time. We can now easily communicate with each other despite the distance apart, exchange data, audio, video, and information. Network consists of Local Area Network (LAN) and Wide Area Network (WAN). Local Area Network is a computer network that covers only a small area networks, such as campus computer networks, buildings, offices, homes, or schools. While the Wide Area Network is a data communications network that operates beyond the geographic scope of the LAN. Knowing the applications, devices, and protocols before designing the network is very important to build a reliable and safe network. We have designed, build, and simulated a network using EIGRP, VPN, DMZ and IDS/IPS. The result of our simulation shows the network has a good performance, secure, and reliable.**

*Keywords*—**WAN, LAN, NAT, ACL, VLAN, headquarter, branch offices.**

## I. Introduction

Companies are required to have a LAN and WAN in order to communicate between headquarters and branch offices. WAN differs from a LAN in several ways. LAN is a computer network that covers only a small area networks. WAN allows the transmission of data across a larger geographic distance. Both of these networks, LAN and WAN protocols have a unique configuration or have different functions according to their needs such as NAT, ACL, VLAN and Frame Relay technologies. In this paper, we assume a company is currently building a network from scratch. They do not have a LAN and a WAN in their building and office. The company expects to have a network that can improve performance in business or in a job without any interference in terms of security, network availability, and network management while ignoring cost considerations. Therefore, the network is designed to meet the needs of communication systems and applications in the company. The paper is organized as follows. In section 2, we discuss fundamental theory. We design the network according to the applications in section 3. Implementation are presented and discussed in section 4. Section 5 summarizes and concludes the paper.

## II. Fundamental Theory

The computer network is a combination of hardware, software, protocol, and cabling that enables a variety of computing devices communicate with each other. The important hardware in networking are: server, router, switch, ASA and IPS.

1. **The server** is a computer system that provides a specific type of service in a computer network. Server powered by a processor that is scalable and RAM, also comes with a specific operating system, referred to as the network operating system or network operating system. The server is also running administrative software that controls access to the network and the resources contained therein, as well as file or printer device (printer), and provides access to the workstation network members;

2. **Router** is a component of network that send data packets over a network or the Internet to the destination, through a process known as routing. The process of routing occurs at layer 3 (network layer such as internet protocol) protocol stack of the seven-layer OSI. Router serves as a liaison between two or more networks to carry data from one network to another.

3. **Switches** are connecting multiple devices to form a local area network (LAN). Switch Network is a networking tool that performs transparent bridging (connective tissue segmentation lot with forwarding based on MAC address).

4. **Adaptive Security Appliance (ASA)** are combining the functionality of Private Internet eXchange (PIX), Virtual Private Network (VPN) and Intrusion Prevention Systems (IPS). It's classified as a network layer firewall with stateful inspection.

5. **Intrusion Prevention Systems (IPS)** are network security appliances that monitor network and/or system activities for malicious activity. Its functions are to identify malicious activity, log information about said activity, attempt to block/stop activity and report activity.

Computer software is an important component in computer system. Software is a collection of computer programs and related data that provides the instructions for telling a computer what to do and how to do it. Software refers to one or more computer programs and data held in the storage of the computer. In other words, software is a set of programs, procedures, algorithms and its documentation concerned with the operation of a data processing system. Program software performs the function of the program it implements, either by directly providing instructions to the computer hardware or by serving as input to another piece of software.

A protocol is needed in order the computers can communicate between them. A communications protocol is a system of digital message formats and rules for exchanging those messages in or between computing systems and in telecommunications. A protocol may have a formal description. Protocols may include signaling, authentication and error detection and correction capabilities. A protocol definition defines the syntax, semantics, and synchronization of communication; the specified behavior is typically independent of how it is to be implemented. A protocol can therefore be implemented as hardware or software or both. Communications protocols have to be agreed upon by the parties involved. To reach agreement a protocol may be developed into a technical standard. Two protocols that widely used in internet or communication are OSI (Open Systems Interconnection) and TCP/IP.

- **OSI** or Open Systems Interconnection is a network architecture model which is used to make several suppliers (vendors) can communicate with each other. Prior to the OSI, the network computer system is very dependent on the supplier. OSI attempt to establish a common standard model of computer networks to support interoperability between different suppliers. In large networks are common to many different network protocols. The absence of a model of the same protocol, making it difficult for many devices to communicate with each other.

- **TCP / IP** is a standard data communication system used in computer networks to communicate with each other separately and exchange - exchange data. This protocol could not stand alone, because the protocol is a collection of protocols. This protocol uses a simple scheme called the IP address (IP Address), which allows up to several hundred million computers to be able to talk to each other on the Internet. This protocol is routeable where protocol is suitable fatherly linking system that is different (such as Microsoft Windows and UNIX) to form a heterogeneous network. ). Various kinds of protocols running on top of TCP / IP addressing scheme, and the concept of TCP / IP defined in documents called Request for Comments (RFC).

Computer networks can be differentiated based on several criteria. As wide area, transmission media, the operation pattern, and so on. Based on the spacious area is the computer networks can be distinguished:

1. **LAN** (Local Area Network) is a computer network that covers only a small area networks, such as campus computer networks, buildings, offices, in homes, schools or smaller.

2. **MAN** (Metropolitan Area Network) is a computer network that covers an area the size of a city or a combination of multiple LANs that are connected to a large network.

3. **WAN** (Wide Area Network) is a data communications network that operates beyond the geographic scope of the LAN. WAN differs from a LAN in several ways.

There are several topologies that are in both LAN and WAN networks.

- **Bus topology**, using a wired backbone and all hosts connected directly to the cable.
- **Star topology,** connect all devices on the central or concentrator. Typically concentrator is a hub, switch, or a WAN provider.
- **Ring topology**, connect the device to other devices to form a ring (closed circles).
- **Mesh topology**, connecting devices in point-to-point. This means that all computers connected to each other. Once they could not be found means there is a broken link. This topology is commonly used in critical locations, such as nuclear installations.
- **Extended Topology Star**, is a star topology has been developed. The idea is to combine multiple star topology into a single unit. The tools used to connect all remedy - each star topology is a hub or switch.
- **Hierarchical topology**, almost similar to the extended star. The difference lies in their interfaces. Each star topology do not use a hub or switch, but using the computer as a control traffic in this topology.

**IP (internet protocol)** is the core of the TCP / IP protocol. There are fields in the IP header contains the Internet address or IP address. IP address of the origin and destination of data packets can be found in this section. However, the IP address is not recognized by the network hardware. Hardware only understands the MAC address. So we need a way to bridge the two types of address. This is where the role of protocols ARP (Address Resolution Protocol).

**ARP** is the Internet layer and work with IP protocols. ARP is used to change the IP address to ethernet. Changing the address is only for IP packets sent. When a host sends a data packet, beside the destination IP address, the ethernet address of the destination also must be known. Ethernet address is precisely what is recognized by fellow ethernet device.

**DHCP** is a protocol that allows the allocation of IP addresses in a network with the same network address. If you are not using this protocol, the administrator must provide the ip manually - one on the PC. If using DHCP, all PCs connected in a network will get the ip automatically.

Variable Length Subnet Mask (VLSM) means allocating IP addressing resources to subnets according to their individual need rather than some general network-wide rule. Network protocols are the rules that are used in the network so that computers can communicate with each other network members.

**VLAN** is a network model that is not limited to a physical location such as a LAN, this has resulted in a virtual network can be configured without having to comply with the physical location of the equipment. The use of VLANs will create a highly flexible network setting which can be made segments that depend on the organization or department, without relying on the workstation location.

**EIGRP** is the routing protocol that is CISCO. Include EIGRP routing protocol with hybrid algorithms. (CCNA Exploration 2, 2010). The device EIGRP hello packet exchange information to ensure the area around. In a large bandwidth, the routers exchange information every 5 seconds, and 60 seconds at a lower bandwidth.

**Point-to-Point Protocol (PPP)** is a network packet encapsulation protocol that is widely used in the wide area network (WAN). Challenge Handshake Authentication Protocol (CHAP) is one-one PPP authentication. CHAP uses three levels of authentication. The server will send a string that contains the name of the server and the random challenge to the client.

**Network Address Translation or NAT** more commonly called is a method to connect more than one computer to the Internet using a single IP address. Widespread use of this method due to the limited availability of IP addresses the need for security, and the ease and flexibility in network administration.

**Access Control List (ACL)** is a method used to select the packages in and out of network. If we are not sure of the origin of the incoming packet then the packet should be "removed" only. This transforms and avoids the possibility of the entry of "intruders" into the network that we manage. This principle applied by the ACL.

**Frame Relay** is a WAN protocol that operates at the first and second layer of the OSI model, and can be implemented in many types of network interfaces. Frame relay is a high-speed communications technology that has been used on thousands of networks worldwide to connect LAN, SNA, Internet and even application of sound / voice.

**Cisco® Packet Tracer®** is software developed by Cisco® and serves to help simulate the network topology and configuration. Version to be used is Cisco® Packet Tracer® version 5.3.3.0019. Features that are provided by packet tracer is to be able to create logical and physical topology and its configuration on each element. Element - element includes network devices such as cables, routers, switches, hubs, and end users.

**Microsoft® Visio®** 2010 is software developed by Microsoft® Developer and serves to help drawing the technical design. Version to be used is 14.0.4760.1000. Features that are provided by Microsoft® Visio® is to design the logical network diagram using the Visio® Stencil. We used the Shapes of Cisco® products Stencils that previously provided on www.cisco.com for designing the logical network diagrams.

## III. METHODOLOGY

In this scenario, the company has three offices located in different area: a headquarter and two branches. The offices do not have any network that can access the internet or data transmission between offices. The company wants to build a network that is needed. All transactions at the branch offices can be done through the internet. To that end, the company wanted a network that always available for data transmission so that all transactions can be run well.

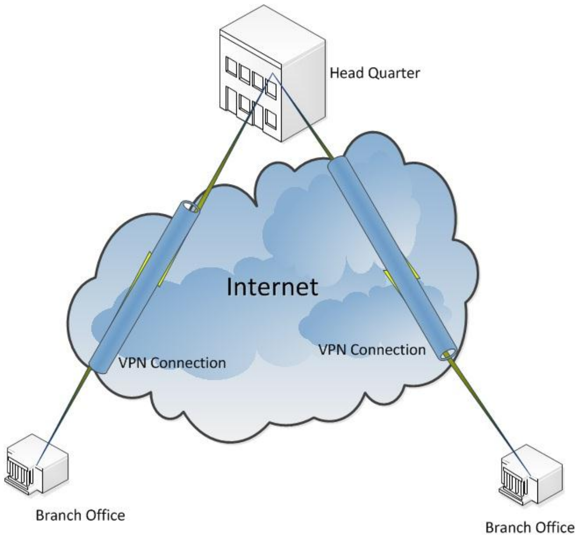

**Fig.1**. Network Topology

The company wants a secure network to prevent data theft or destruction of the network system is running. The company wanted a network that is structured so that it can be easily to manage all parts; the part that is in the corporate structure and easy in network development. The company wanted the head quarter office can find out all financial transactions in the all branch offices. To that end, a secure WAN network is needed so that information exchange can easily be done and there are no obstacles in the delivery of data.

Because only has three separate buildings that frame relay and leased line is more suitable because it is the logical pick the relationship point-to-point inter-office, so that the resulting low delay. There is a back-up on the WAN communication lines so that if one was a dead link, communication still runs fine. Configuring DHCP on the switch layer distributors help facilitate the provision of IP addresses to users.

The device - a device that will be used in this network using routers, switches, firewall, intrusion prevention system, access points from vendors CISCO®.

The head quarter uses the enterprise routers (Cisco® ASR 1013 Aggregation Services Router), enterprise firewalls

(Cisco® ASA 5585-X Adaptive Security Appliance), intrusion prevention systems (Cisco® IPS 4500 Series), core switches (Cisco® Catalyst® 6500 Series), distribution switches (Cisco® Catalyst® 3750 Series), access switches (Cisco® Catalyst® 2960 Series), wireless controller (Cisco® 8500 Wireless LAN Controller) and wireless access points (Cisco® Aironet® 3600).

Every branch uses the branch routers (Cisco® 3945 Integrated Services Routers), branch firewall (Cisco® ASA 5500 Adaptive Security Appliance), distribution switches (Cisco® Catalyst® 3560), access switches (Cisco® Catalyst® 2960) and wireless access points (Cisco® Aironet® 2600).

## IV. Implementation

Implementing enterprise network system is done using Cisco® Packet Tracer® simulation program and Microsoft® Visio® for designing the network diagrams. To meet the desired needs of the designed network topology can be found in figure 1. Network is designed using the concept of redundancy, which is mounting a back-up of their devices. Each device is located at the distribution layer and core layer, until the router is directly related to the WAN. So if there is damage to a device or cable, the data transfer is not interrupted. Configure dynamic routing protocol on the LAN and WAN using EIGRP and VPN with consideration. Consideration of the following: a backup route feature, where if there is a change in the EIGRP network does not have to do a recalculation to determine the best route because it can directly use the backup route. If the backup route is also failed, the best route will be recalculated.

Load balancing via paths with equal and unequal cost, so the bandwidth usage on each link to be more effective and guaranteed delivery of packets to all neighbors and sequenced. In this case choose the path with the lowest cost and free looping to reach destination is very important. For branch office topology requiring high security is designed using the concept of network topology configuration required a functioning ACL DMZ (Demiliterized Zone). So the network to filter what data can be external only has access to equipment in the access into the corporate network. DMZ. To support the security system is directly related to the Router WAN has a NAT configuration. In addition to saving public ip NAT is also useful to increase security because NAT will automatically provide protection to only allow connections from the network.

Configuring VLANs on the LAN network is designed to improve network performance, has a good network management, and enhanced security. Communications WAN using Frame Relay technology and point-to-point (leased line) with the following considerations: frame relay technology allows the network to be more stable because it has a parameter CIR (committed Information Rate), which is the lower limit throughput guaranteed by the provider Frame Relay network .

Hierarchical network topology divides a network into multiple layers. This model was chosen because the design of the network to be modular so that it can facilitate the addition of network scale and accelerate performance. Now will be described one by one configuration that will be used on the network at headquarter office. The design of the headquarter offices network topology in figure 2 (after the references of this paper).

There are several protocols that will be illustrated in Figure 2 and the design topology of branch office is configured in the topology in Figure 3 (after the references of this paper)

## V. Conclusion

The conclusions that can be drawn from the analysis is VPN and DHCP useful for building and designing a computer secure network, always available, and easy to perform network management and development. The experiment results showed that the design of the network has a strong security, the availability connection, good load balancing, and easy network management. Redundancies have improved network availability when there is an interruption to abolish single-point-failure.

The system is made with modular thus simplifying the development of the network. With load balancing the load will be evenly distributed on all cables / components. For further development, to reduce the cost, Cisco 3560 series switches can be replaced with a Cisco 1841 series router. If the company has more than two branches, Frame Relay technology should be replaced with MPLS technology.

## References

[1] Winarno, Sugeng. *Jaringan Komputer dengan TCP/IP*. Bandung: Penerbit Informatika, 2006.

[2] Sofana, Iwan. *Membangun Jaringan Komputer (Membuat Jaringan Komputer (Wire dan Wireless)) Untuk Pengguna Windows dan Linux*. Bandung: Penerbit Informatika, 2006.

[3] Soetedjo, Budi, Dharma Oetomo. *Konsep dan Perancangan Jaringan Komputer*. Yogyakarta: Penerbit ANDI, 2004.

[4] Yani, Ahmad. *Panduan Membangun Jaringan Komputer*. Jakarta: Penerbit Kawan Pustaka, 2007.

[5] Derfler, Jr, Frank J. *Panduan Menggabungkan LAN*. Jakarta: PT Elex Media Komputindo, 1992.

[6] Stalling, William. *Jaringan Komputer*. Terjemahan Thamrin Abdul Hafedh Al Hamdani. Jakarta: Penerbit Salemba Teknika, 2000.

[7] Purbo, Onno W. *Jaringan Workgroup, LAN & WAN*. Jakarta: PT Elex Media Komputindo, 1998.

[8] Iskandarsyah, M.H. *Dasar-dasar Jaringan. Ilmu Komputer*. www.ilmukomputer.com accessed by January 17th 2010, 10am.

[9] Intel E-business, IEEE 802.16* and WiMAX, *Broadband Wireless Access for Everyone*. www.intel.com/ebusiness/pdf/intel/80216_wimax.pdf, accessed by January 17th 2010, 10am.

[10] http://www.digituck.com/pengertian-jaringan-komputer.html, accessed by January 16th 2010, 3pm.

[11] http://en.wikipedia.org/wiki/jaringan local, accessed by January 16th 2010, 3pm.

[12] http://www.cangkruk.com/topologi-mesh45, accessed by January 16th 2010, 4pm.

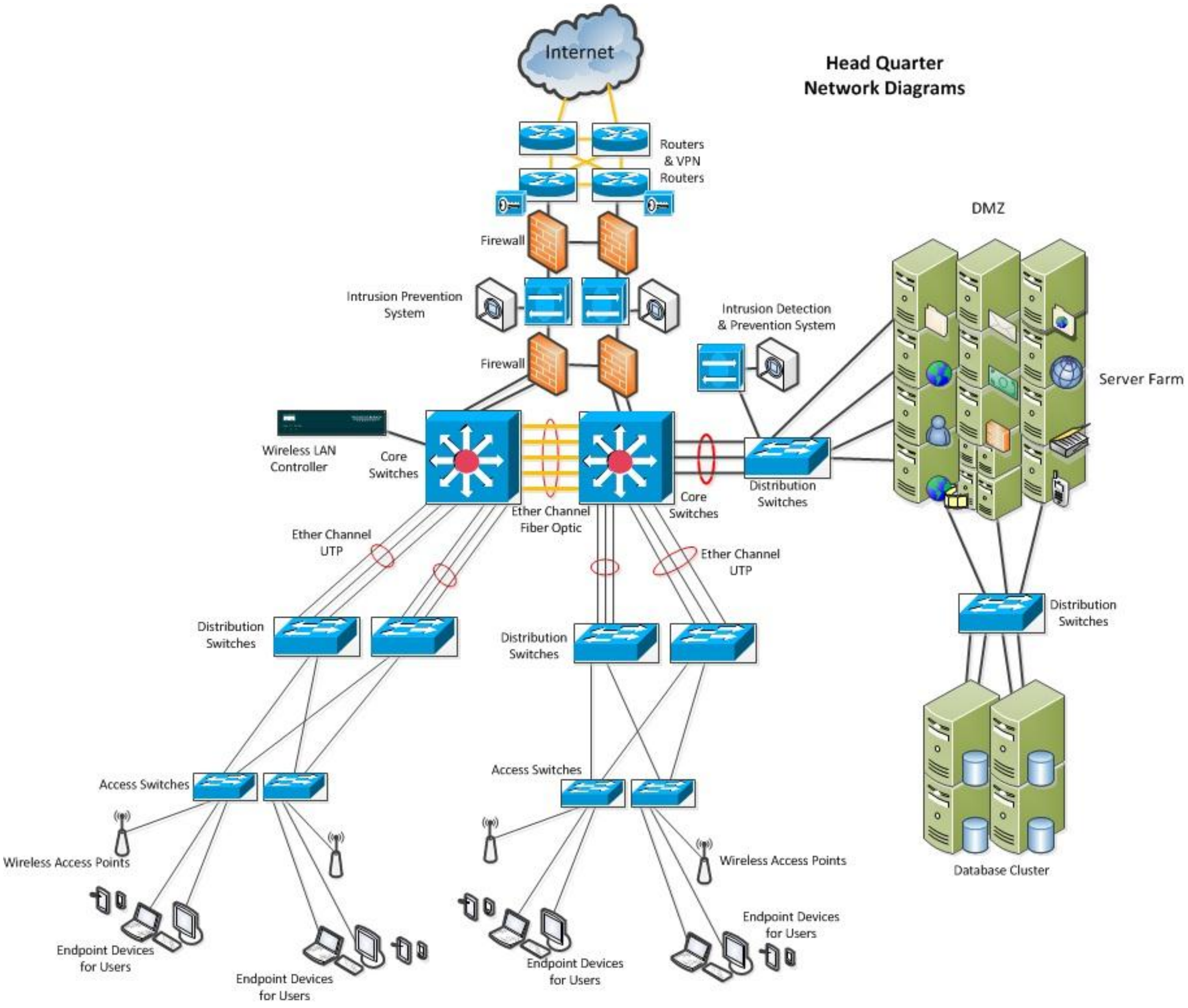

**Fig.2**. Head Quarter Network Topology

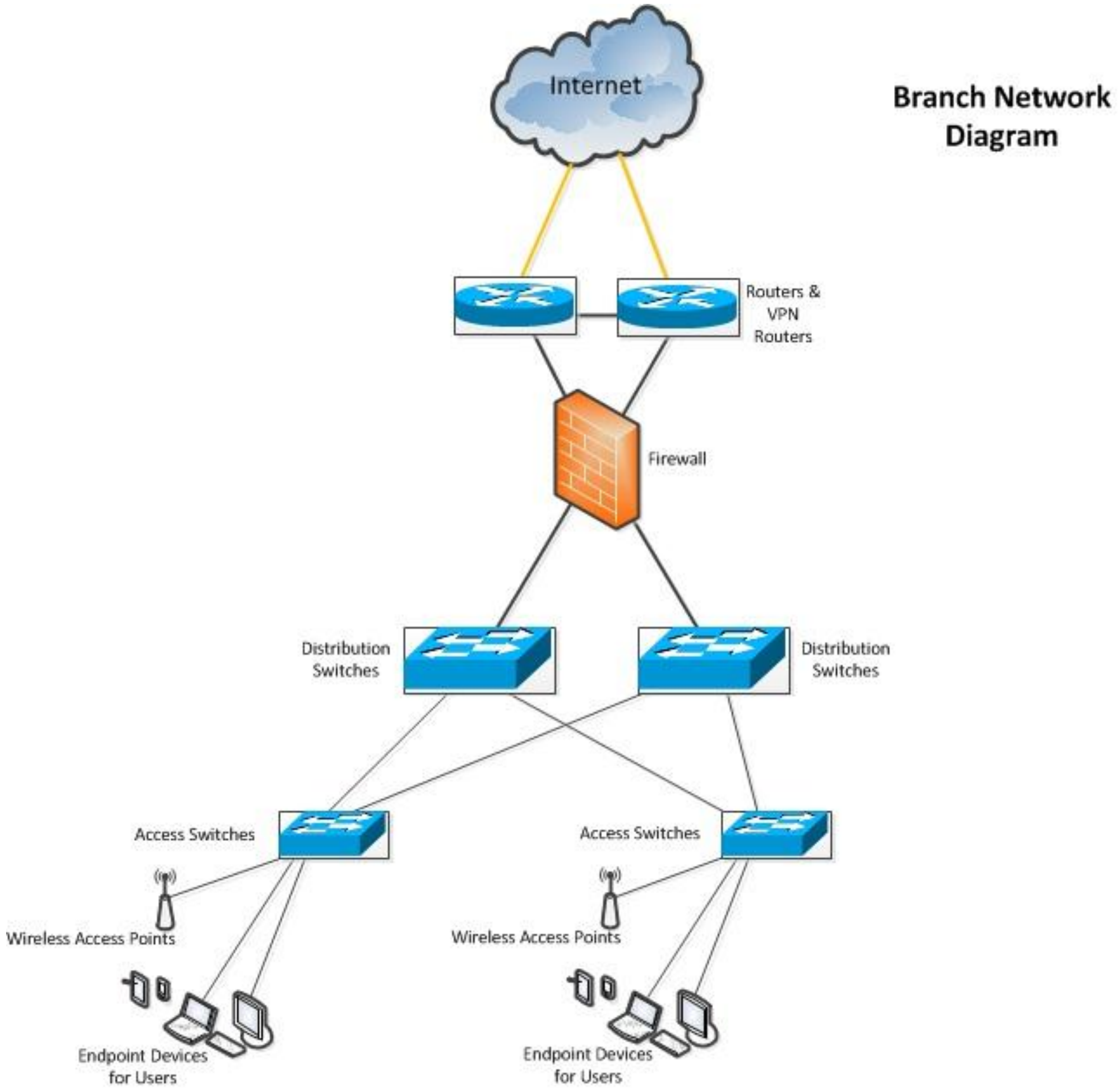

**Fig.3**. Branch Office Network Topology