JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2025, Vol 5, No 2, Hlm. 36 – 42
Available online at http://jurnal.goretanpena.com/index.php/teknisi

INTERNET SECURITY DESIGN ON WIFI NETWORKS USING VIRTUAL PRIVATE NETWORK

Rismawati[1*], Hidayatullah[1]
[1]Informatics Management, AMIK Polibisnis Perdagangan
Email:[1]Rismawatipangaribuan25@gmail.com, [2]dayatscorpio2@gmail.com

Abstract : The rapid development of internet technology has increased the need for secure data transmission, especially when using public WiFi networks that are highly vulnerable to threats such as account tapping, data theft, and unauthorized access. This research aims to design a secure internet system using a Virtual Private Network (VPN) on a WiFi network at the Bireuen Technology Innovation Store. The proposed solution involves implementing a VPN system that ensures encrypted and secure communication between clients and servers. The study employs a multi-stage method: data collection, system analysis, design, implementation, and testing. The system was developed using the Ubuntu 14.04 (32-bit) operating system and OpenVPN software. Testing results show that the VPN successfully encrypts user data and secures communication channels from public WiFi to the VPS server. This proves that VPN implementation is an effective solution to enhance internet security in public network environments. The study concludes that a VPN system is essential for protecting data transmission and user privacy, especially in unsecured wireless networks.

Keywords: security; ubuntu 14.04 (32 bit)*;* VPN.

Abstrak: Perkembangan teknologi internet yang pesat telah meningkatkan kebutuhan akan transmisi data yang aman, terutama saat menggunakan jaringan WiFi publik yang sangat rentan terhadap ancaman seperti penyadapan akun, pencurian data, dan akses tidak sah. Penelitian ini bertujuan untuk merancang sistem internet yang aman menggunakan Virtual Private Network (VPN) pada jaringan WiFi di Toko Inovasi Teknologi Bireuen. Solusi yang diusulkan melibatkan penerapan sistem VPN yang memastikan komunikasi terenkripsi dan aman antara klien dan server. Penelitian ini menggunakan metode multi-tahap: pengumpulan data, analisis sistem, perancangan, implementasi, dan pengujian. Sistem ini dikembangkan menggunakan sistem operasi Ubuntu 14.04 (32-bit) dan perangkat lunak OpenVPN. Hasil pengujian menunjukkan bahwa VPN berhasil mengenkripsi data pengguna dan mengamankan saluran komunikasi dari WiFi publik ke server VPS. Hal ini membuktikan bahwa implementasi VPN merupakan solusi yang efektif untuk meningkatkan keamanan internet di lingkungan jaringan publik. Penelitian ini menyimpulkan bahwa sistem VPN sangat penting untuk melindungi transmisi data dan privasi pengguna, terutama dalam jaringan nirkabel yang tidak aman.

Keywords: keamanan; ubuntu 14.04 (32 bit)*;* VPN.

JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2025, Vol 5, No 2, Hlm. 36 – 42
Available online at http://jurnal.goretanpena.com/index.php/teknisi

INTRODUCTION

The rapid advancement of technology today has created people who often use the internet . The internet also has a great influence on science, information and education. Users can easily search for various information from the internet . In addition to books and libraries, the internet makes the spread of knowledge, information and data quickly and comprehensively.

The development of the internet has also influenced economic development. Various buying and selling transactions that previously could only be done face to face and some by post or telephone, are now very easy and often done via the internet . Financial transactions can now also be done with internet banking, viewing employee data can be done via remote desktop, managing websites can be done from anywhere as long as there is an internet network , checking email or retrieving important data can be done on the internet network .

Along with the increasing development, new problems have emerged, namely in terms of internet security, especially for general or public internet access or often called wifi, which is usually very vulnerable to security, the problems that arise are usually in the form of tapping of internet accounts, theft of data on our computers, taking over access, spreading viruses , and others that are often done on the internet network, for current prevention, most people use free and unupdated anti-viruses, so they are very vulnerable to infection and data tapping.

This research have a purpose to find a solution to overcome things that happen when using a WiFi network, by using a Virtual Private Network , which is a private network that uses a non-private medium (for example the internet) to connect. A Virtual Private Network is a way to create a network that is " private " and secure by using a public network, for example the internet (Rosyidah & Parenreng, 2023).

With a virtual private network, data is encapsulated (wrapped) with a header containing routing information to obtain a connection to the server so that data can pass through the public network safely and reach its destination. While the data sent has been encrypted first to maintain its confidentiality so that the packets caught when passing through the public network cannot be read because they have to go through the decryption process. To create a Virtual private network requires a server that is always connected to the internet , because the price of the server is expensive, so here the VPN that is built will use a Virtual Private server as a solution for the VPN server (Arfind et al., 2023).

METHOD

Method is a way or path to obtain return solution to everything problem. In the research It is known that there are several types of theories to apply one of the criteria.The method that relevant to certain problems. In this research stage, the author divides the stages into: in several parts, namely:
a). Data collection stages, b). Analysis Stages, c). Design Stages, d). Implementation Stages,
e). Testing Stages

Literature review

According to Rayport (2003), Around the end of 1970 IBM released the results of their experiments in designing WLAN with IR technology, other companies such as Hewlett-Packard (HP) tested WLAN with RF, both companies only achieved a data rate of 100 Kbps, because it did not meet the IEEE 802 standard for LAN which is 1Mbps then the product was not marketed. And in 1985 the Federal Communication Commission (FCC) determined the Industrial, Scientific and Medical (ISM band) namely 902-928 MHz, 2400-2483.5 MHz and 5725-5850 Mhz which were unlicensed, so that the development of WLAN commercially entered a serious stage.

It was only in 1990 that WLAN could be marketed with products using spread spectrum (SS) techniques on the ISM band, licensed frequencies of 18-19 GHz and IR technology with data rates of more than 1Mbps. With the existence of various brands of hardware and software, a standard is needed where devices of different brands can function on devices of other brands, and the WLAN standards are EEE 802.11, WINForum and HIPERLAN.

Wireless Information Network Forum (WINForum) was born by Apple Computer and aimed to achieve unlicensed Personal

JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2025, Vol 5, No 2, Hlm. 36 – 42
Available online at http://jurnal.goretanpena.com/index.php/teknisi

Communication Service (PCS) bands for data applications offering very minimal regulations and fair access. High Performance Radio Local Area Network (HIPERLAN) was born by the European Telecommunications Standards Institute (ETSI) which focuses on the 5.12-5.30 GHz and 17.1-17.3GHz bands, IEEE 802.11 was born by the Institute of Electrical and Electronics Engineers (IEEE) and focuses on the ISM band and utilizes spread spectrum (SS) techniques namely Direct Sequence (DS) and Frequency Hipping (FH), this standard is the most widely used.

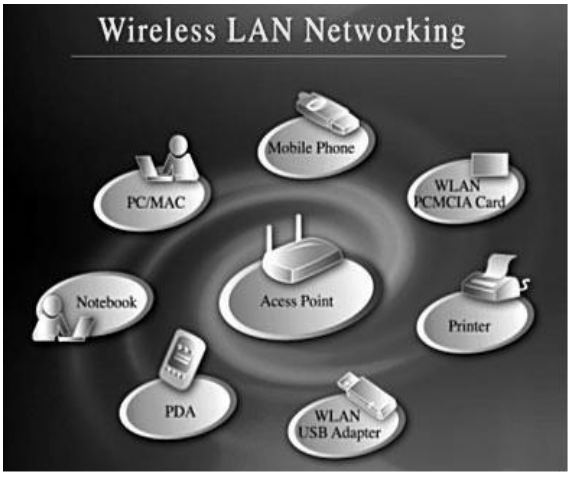

Image 1. LAN Network

Wireless is a wireless network that uses air as a transmission medium to transmit electromagnetic waves. The development of wireless has actually started a long time ago and has been scientifically proven by scientists with the discovery of radio and then continued with the discovery of radar. Then with the development of information needs for humans, the use of wireless is increasing and not only for the use of radio and radar. Some models of equipment that use *wireless* include the following:

1. Cellular telephones and radio pagers (pagers).
   Services provided for mobile and portable applications, both for individuals and businesses.
2. GPRS for navigation.
   Used to facilitate traffic users, such as cars, airplanes, ships and others.
3. Wireless computer devices such as mouse and keyboard.
   Mouse and keyboard sometimes experience problems in the form of difficulty in installing the connector on the CPU, sometimes also experiencing damage to the connector. Mouse and keyboard with wireless technology allow to overcome these obstacles, even users will be more free to move.
4. Cordless Phones .
   Wireless technology is also used by telecommunications companies in the form of cordless telephones , so that they can be carried anywhere.

Wireless technology is very suitable and widely used as a replacement for LAN network cables and even WAN (Wide Area Network) cables. The further the wireless range, the higher the hardware requirements. Popular wireless technology for LAN groups is wifi. The current wifi data transfer speed has reached 54 Mps. It is still not comparable to the speed with UTP cables that have reached 1 Gbps. The types of topology in computer networks are:

Bus Topology Network

Bus topology all terminals are connected to the communication path. The information sent will pass through all terminals on the path. If the address listed in the data or information sent matches the address of the terminal passed, then the data or information will be received and processed. If the address does not match, then the information will be ignored by the terminal passed.

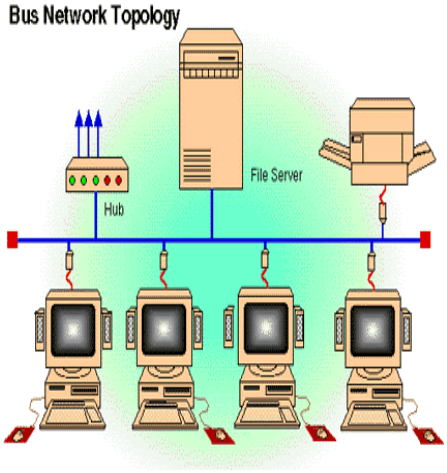

Image 2. Topology Network

JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2025, Vol 5, No 2, Hlm. 36 – 42
Available online at http://jurnal.goretanpena.com/index.php/teknisi

The number of terminals can be added and reduced flexibly. However, the number of terminals should be limited, because in this model topology, if there are too many connected terminals, the network performance will drop drastically. Another disadvantage of this topology is that if a terminal dies, the network operation will be disrupted.

Superiority:

1. Network expansion or the addition of new workstations can be done easily without disrupting other workstations .
2. Save cables.
3. Simple cable layout.

Weakness:

1. If there is interference along the central cable, the entire network will experience interference.
2. Congestion on the traffic lane.
3. Repeater is required for long distance.

Star Topology .

In a star topology , a central terminal acts as the regulator and controller of all data communications that occur. Other terminals are connected to it and data is sent from one terminal to another through the central terminal. The central terminal will provide a special communication path for the two terminals that will communicate. As one example of the use of Star topology is the telephone network.

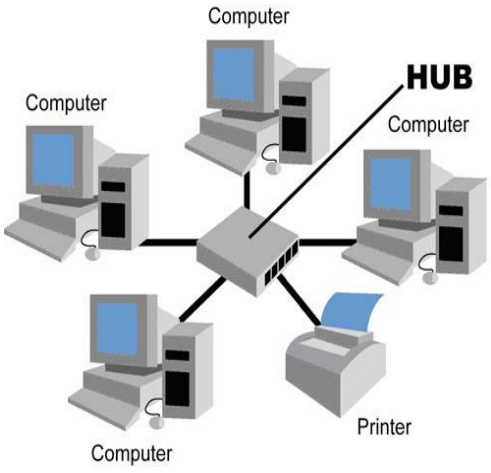

Image 3. Star Topology Network

This topology is easy to develop , both for additions and deletions terminal.

Superiority:

1. Damage to one channel will only affect the network on that channel and the linked *stations* .
2. The security level is quite high.
3. Resistant to busy network traffic.
4. Adding and removing stations can be done easily.
5. Centralized access control.
6. Ease of detection and isolation of network management errors/damages and the most flexible.

Weakness:

1. If the middle node fails, the entire circuit stops.
2. Wasteful in cable usage.
3. HUB becomes a critical element because of centralized control.
4. The role of the hub is very sensitive so that when there is a problem with the hub, the network will *go down* .
5. The network depends on the central terminal.
6. If using *a switch* and heavy data traffic can cause the network to be slow.
7. Network costs are more expensive than bus or ring.

Hybrid Topology.

Topology hybrid is a combine from some topologies (bus, ring, star or mesh). Topologi hybrid was built for can combine advantages which are owned every topology.

Example topography This is a topology tree (tree topology). Topology tree namely mix between the topologi bus and the topology star.

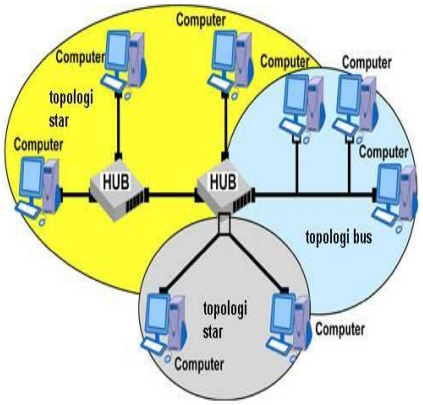

Image 4. Hybrid Network

JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2025, Vol 5, No 2, Hlm. 36 – 42
Available online at http://jurnal.goretanpena.com/index.php/teknisi

Hybrid Topology
Superiority:

1. One of the prominent advantages of hybrid topology is flexibility. Hybrid network topology is designed in such a way that it can be applied to a number of different network environments.
2. Hybrid combines different configurations but can work perfectly for different amounts of network traffic.
3. Compared to other types of computer topology, this topology is reliable.

Weakness:

1. Because it is a combination of several forms into a hybrid topology , managing the topology will become more difficult.
2. From an economic perspective, hybrid networks are difficult to maintain because they require higher costs, higher topology compared to pure network topologies in one form, cost factors can be related to the cost of adding hubs and increased cabling costs to build this form of topology.
3. The installation and configuration of this topology is difficult because there are different topologies that have to be connected to each other, at the same time it has to be ensured that none of the nodes in the network fails to function which makes the installation and configuration of hybrid topology very difficult.

RESULTS AND DISCUSSION

Testing is a process that aims to ensure that all system functions are working properly and to find errors that may occur in the system.

Server testing and Client VPN In this section, the connection from the client to the VPN server is discussed before testing, an installation is first carried out on the Client side using Openvpn, because in terms of licensing, Openvpn is free software , for the Openvpn installation, for more details about the VPN connection, it can be seen as follows:

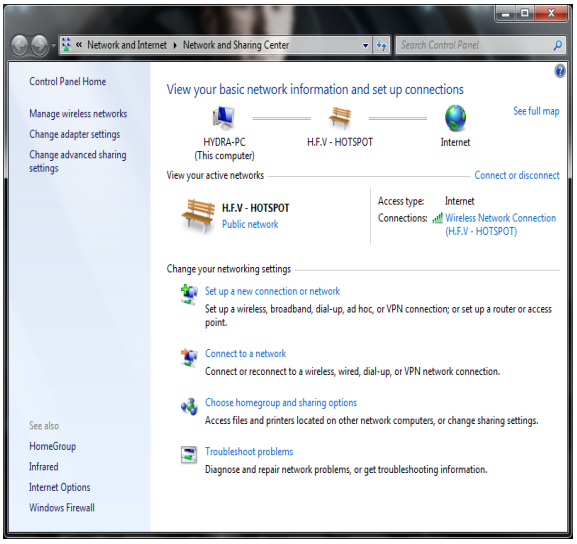

Image 5. VPN Connection

The client's condition can be seen before connecting to the VPS because the image still uses 1 (one) network, namely the public area network.

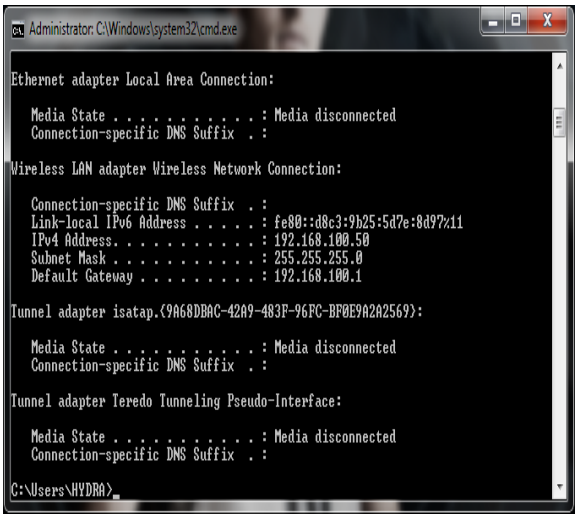

Image 6. Coding to Connection

Screen command contains 1 (one) IP The client executes the ipconfig command on the command then only one IP is visible, namely from the wireless adapter 192.168.1.50 with Gateway IP 192.168.100.1 which is the wireless server. public area

To create an account for a VPN client to be able to use a VPN, you need to log in to the server using the PuTTY program to remotely access the server and fill in the Host Name zapto.org with port 22, it can be seen in image 7.

JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2025, Vol 5, No 2, Hlm. 36 – 42
Available online at http://jurnal.goretanpena.com/index.php/teknisi

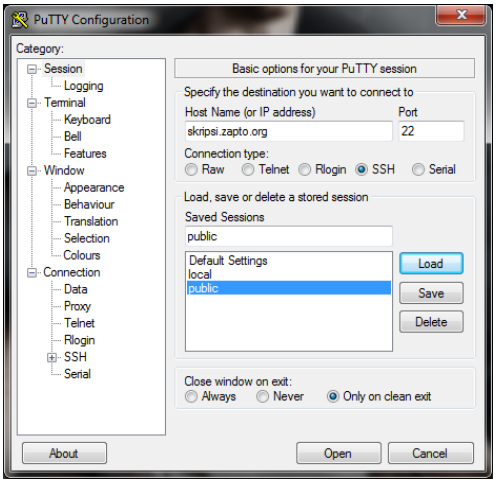

Image 7. PuTTY view logged into VPS

Table 1. Deep Analysis of The Implementation VPN

ASPECT	THE IMPLEMENTATION BY VPN	ANALYSIS
Client IP Address	Additional IP from VPN Server (via tunneling)	VPN adds an encrypted virtual IP, increasing security and obscuring real identity.
Data Security	Data is encrypted before sending, not easily read by third parties	VPN encrypts data packets, making them secure even over public networks.
User Privacy	Identity and activities are more protected	VPN hides internet traffic from external surveillance.
Server Access Protocol	Access via secure protocol (PuTTY, port 22 to VPS)	Remote login to the server using a more secure method (SSH).
Infrastructure Costs	Using VPS (cheaper and more flexible)	VPS is an economical solution with stable performance for small to medium scale.
Application	Safe for a variety of online activities, including remote desktop and email	VPN provides an additional layer of security in communicating sensitive data.

CONCLUSION

This research successfully designed and implemented a network security system on a public Wi-Fi network using Virtual Private Network (VPN) technology based on Ubuntu 14.04 (32-bit). Tests were conducted on both the server and client sides, with the client connecting to the VPN server through the open-source OpenVPN application. The results showed that before the VPN connection was activated, the client only had a single IP address from the public network (192.168.x.x), which was vulnerable to eavesdropping and data theft. However, after connecting to the VPN server via a VPS using a secure protocol (e.g., port 22 via PuTTY), the client gained an additional IP layer that protected encrypted data communications. Using a VPN, user data is encapsulated and encrypted, making it unreadable when passing

through the public network without decryption. This process ensures data confidentiality and integrity, which is crucial when users access sensitive information such as email accounts, banking accounts, or corporate information systems. Furthermore, using a VPS as a VPN server is an economical and efficient solution compared to using a dedicated server.

BIBLIOGRAPHY

Arfind, R., Supendar, H., & Fahlapi, R. (2023). Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik. Jurnal Komputer Antartika, 1(3), 108–116. https://doi.org/10.70052/jka.v1i3.28

Rosyidah, A., & Parenreng, J. M. (2023). Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN). Internet of Things and Artificial Intelligence Journal, 3(3), 239–249. https://doi.org/10.31763/iota.v3i3.613

Andy Rachman, Ricky Eka P, Tri Wahyu H, 2010; "Virtual Private Server (VPS) as an Alternative to Dedicated Server" Informatics Engineering – ITATS, Surabaya

Dian Palumi Rini, Deris Stiawan, 2009; "Optimizing Virtual Private Network (VPN) Interconnection Using Hardward Based And Lix (Indonesia Internet Exchange) As An Alternative Wide Scale Network (WAN)" Faculty of Computer Science, Sriwijaya University.

Dwi Suta Admaja, Arya Astawa, March 2012; " Implementation of VPN on the Campus Computer Network of Bali State Polytechnic" Department of Electrical Engineering, Bali State Polytechnic.

Muhammad Izwan, 2010; "Implementation of Virtual Private Network Remote Access with Openswan (Case Study at UIN Syarif Hidayatullah Jakarta)", Faculty of Science and Technology, Syarif Hidayatullah State Islamic University Jakarta.

Napianto, Riduwan and Utami, Ema and Sudarmawan, 2005; "Virtual Private Network (VPN) on Windows Server Operating System as a Company Data Delivery System Through Public Network (Case Study: Tomato Digital Printing Network)", Informatics Engineering STMIK AMIKOM Yogyakarta.