International Journal of Multidisciplinary Research and Growth Evaluation

International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 10-12-2020; Accepted: 14-01-2021
www.allmultidisciplinaryjournal.com
Volume 2; Issue 1; January-February 2021; Page No. 87-91

Overview of network and security management on internet facilities (WiFi) in the Covid-19 Pandemics

Rizwandha Imawan[1], **Refna Tri Megahaeni Lase**[2], **Iskandar Muda**[3]
[1, 2, 3] Universitas Sumatera Utara, Medan, Indonesia

Corresponding Author: **Rizwandha Imawan**

Abstract

Recently, the use of wireless networks as a form of the Covid-19 outbreak is increasing. This is because the wireless network system is one of the public facilities and activities. So that people need a fast and safe internet network. But wireless networks have security problems, namely the configuration and encryption used. To solve this problem, companies really need network security on each LAN port (local area network), namely by using the default method or static port security, dynamic learning port security and sticky port security on the port located in the room. This is useful for blocking network access to users who do not report workplace changes and can prevent data theft by strangers or non-employees of the company.

The purpose of this literature review is to describe an overview of network management and security in internet (wifi) facilities during the Covid-19 pandemic. This study uses a literature study, which is a study whose preparation is the same as otheSr research, but the sources and methods of data collection are by taking data from libraries, reading, taking notes, and processing research materials. Network security is not only a computer system handler, but there is a need for management to be done to analyze all the risks that might come attacking. With this analysis we do not have to spend very large funds but can use funds efficiently to make it economically feasible.

Keywords: Covid-19, Network, and Security Management

1. Introduction

(Susilo *et al.*, 2020) [9] In early 2020, the world was caught off guard by the outbreak of unknown pneumonia that began in Wuhan, Hubei Province. It spread rapidly throughout more than 190 countries and territories. This outbreak is named coronavirus disease 2019 (COVID-19), caused by severe acute respiratory syndrome coronavirus-2 (SARS-CoV-2). The spread of this disease has had wide social and economic impacts. There are many controversies surrounding this disease, such as diagnosis, management, and prevention.

With the current condition of the Covid-19 pandemic in a number of countries including Indonesia, of course, it has quite a serious impact on various aspects. The determination of the Covid-19 standby and emergency response status has caused many activities that invite crowd to be disbanded. The corona virus epidemic does not only affect the health world in Indonesia, but also industry and business so that activity and mobility are limited. This makes many people have to be smart in using their time in the middle of a social distancing atmosphere. Moreover, those who have to carry out activities and various content really need activities in their respective homes in order to remain productive.

So far, there are still a number of regulations that prevent procedures and mechanisms from being carried out online in the field of community life. The bureaucratic rules that have been asking for face-to-face meetings between the public and the government or certain parties can no longer be maintained. For example, several types of monthly bills, bureaucratic regulations and others. Therefore The spread of the corona virus cannot be denied that it has a profound impact on the technology industry. Changes in society also occur, for example work can be done at home and changes that occur to consumers who shop without meeting with producers. The impact of this has resulted in increased use of technology. Many companies have enforced work from home regulations in order to avoid transmission of the corona virus.

By working from home, everyone needs internet access to stay connected to the office. However, it is necessary to pay attention to the principle of network security in transmitting data to protect any data stored in the computer. Computer network security is a problem that every computer user must pay attention to. It must be noted the need to clean phishing sites, illegal links, spam, etc. on the computer. Negligence that occurs can have a serious impact on computer security such as data damage and leakage of computer data information.

One of the ways to maintain network security is to use network security management. Namely implementing Firewall Security Port network security. According to Maiwald in (M. Ryansyah: 2019) [7], a firewall is a frontline defense system on a network, as a device that protects data flow on a network. A firewall is a network device that is in the Layer 3 (Network layer) and Layer 4 (Transport layer) device category of the OSI layer 7 protocol. As is known, layer 3 is the layer that takes care of IP addressing problems, and layer 4 is dealing with problems of communication ports (TCP / UDP). Data security and confidentiality issues are an important aspect of an information system. One of the features that are able to manage the network well is the ability to create a firewall as security or an antidote from intruders and hackers. However, along with the development of information technology, the technology used by intruders and hackers is also getting higher, to anticipate this, information is needed about an overview of network management and security in internet (wifi) facilities.

2. Literature review

This research was developed from some literature and literature as a reference for making applications, including:

2.1 Mikrotik Firewall

Analysis and Optimization of Network Security Simulation Using a Mikrotik Firewall. in Taman Pintar Yogyakarta by utilizing various features available on Mikrotik such as firewalls and other network security support features at Taman Pintar Yogyakarta. In general, this research produces a configuration for the Taman Pintar Yogyakarta computer network security system using a Mikrotik router firewall which includes configuration for firewalls, service port management and filter configuration for bridges. This research applies four firewall configurations that function to block user activity or attacks from outside that can compromise the network security system. These configurations are blocking the use of free VPN applications, blocking the use of torrent applications, blocking DDOS attacks and doing camouflage for port scanning using NMAP.

2.2 Firewall Security Port

Implementation of a Network Security System Using a Firewall Security Port on Vitaa Multi Oxygen (M. Ryansyah, 2019) [7]. In the case that happened at PT Vitta Multi Oksigen, there was frequent data theft when the employee moved rooms or left the company so that it requires data security using a device that can control network access rights (firewall security port) which is very much needed, especially now in companies does not use security such as implementing a firewall security port or the like. This research focuses on network management that will be proposed to deal with the problems faced by the Vitta Multi Oxygen office is the implementation of network security Firewall Security port which functions to provide network security and is a technique that will allow access rights through available ports on the branch switch with monitoring IT (Information Technology). This allows all employees in the office to report if there is a workplace change or a new employee will use the network at this office, because automatically the access rights on new devices that employees connect to the switch port will be blocked by port security. With the report unable to access the network,

2.3 Nmap Software

Monitoring Analysis of Computer Network Security Systems Using Nmap Software (Case Study at Public High School 1 in Serang City) by (Dwi Bayu, 2020). The problem in this research is where the computer network at SMK Negeri 1 Kota Serang often experiences problems or difficulties accessing the Web E-Raport to input values, even though internet network access is quite smooth. Here we have also experienced a server down where all those who will access the Website, E-Report Card, Dapodik cannot enter the server network, which then affects all computers connected to the network. Where in the research, testing was carried out using Nmap, the authors used several target hosts for analysis. The target host includes IP 192.168.0.1 (IP of the Access Point) and tested using the author's laptop, IP 192.168.105. 254 (ip of LAN connection) was tested using the MM User Lab computer, the smkn1serang.sch.id host was tested with the author's laptop, and the eraport.smkn1serang.sch.id host was tested using the author's laptop. Where the result of this test is that the Nmap software can be used to scan the target network in the form of an IP address and a website. Capable of performing network port scanning with service version and operating system detection engine. Can create nmap results in the form of xml files. Where the result of this test is that the Nmap software can be used to scan the target network in the form of an IP address and a website. Capable of performing network port scanning with service version and operating system detection engine. Can create nmap results in the form of xml files. Where the result of this test is that the Nmap software can be used to scan the target network in the form of an IP address and a website. Capable of performing network port scanning with service version and operating system detection engine. Can create nmap results in the form of xml files.

3. Research Method

This study uses a literature study, which is a study whose preparation is the same as other research, but the sources and methods of data collection are by taking data from libraries, reading, taking notes, and processing research materials. The variables in the literature study research are non-standard. The data obtained were analyzed in depth by the author. The purpose of this paper is to know a general description of network security management.

Previous literature researched to complement this paper is the journal published around 2018 to 2020.

4. Result and Discussion

4.1 Result

Security Management

Security tends to be considered just a matter of technology used. The higher the technology we have, the safer the data we have. However, this contradicts Schneier (Crypto-Gram Bulletin: 2000) "Security is a process, not a product". One thing that differentiates security management from other aspects of network management and IT management in general is that security teams must battle intelligent adversaries, not just human error and technical unreliability. Companies are currently engaged in an escalating arms race with attackers, and threats and security defenses are expanding at a frightening rate. So that at this time not only using the latest technology but also having management to deal with various threats.

- **Planning**

In the planning phase, it is necessary to first assess what kind of network is used in order to see threats and formulate the strategies used to decide future threats by closing any network gaps.

In other words, in planning it is necessary to carry out a risk analysis. Stopping all attacks is something that can't happen. Strong security measures, there is still a risk of compromise and will continue to spend a lot of money, so reducing the risk of attack needs to be analyzed to make it economically feasible.

- **Protect**

In the protect phase, provide real-time protection every day, see protection like a firewall. By establishing periodic checks This emphasizes the fact that the protection phase is much larger than the other two phases in terms of time.

- **Respond to cycles**

In the phase of responding cycle, is the part of how to respond to attacks and the security that is carried out successfully. It would be nice if the compromise never happened. In fact, they will. Like the fire department, the security team must respond promptly and effectively. This requires careful planning and practice because every second is so important in reducing violation costs.

4.2. Discussion

Technology in Covid-19 Virus Prevention

Information technology is very helpful for the public in preventing the covid-19 virus. Technological developments are considered to have a positive impact in inhibiting the spread of the Covid-19 virus. Information technology plays a role in spreading positive information or messages so that it can reduce the number of victims of the Covid 19 Pandemic. Technology makes it easier for everyone to share information by making use of the media and the use of the latest technology tools such as smartphones and notebooks. Thus technology plays an active role in social interaction by providing communication convenience to do various things from anywhere and anytime, such as studying and working remotely while connected to a network.

Network

The development of the world of telecommunications is currently very fast in line with the increasing need for fast and efficient services. Likewise with data communication, from the connection between two computers to computer networks. A computer network is a group of computers that can be connected to one another by using communication media, so that they can share data, information, programs, and hardware.

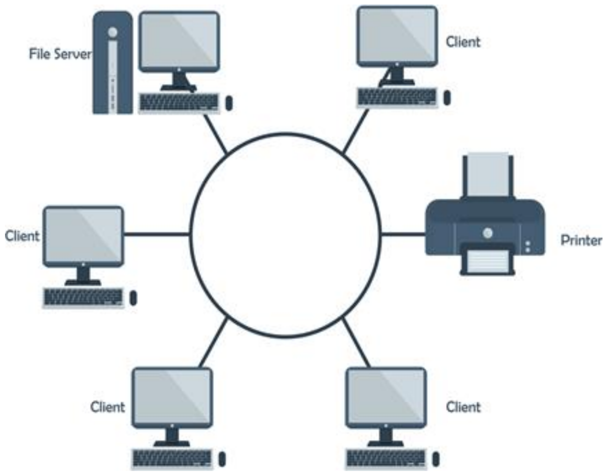

Fig 1: Network Topology

Computer network topology is a way of connecting one computer to another to form a network. The methods currently used are buses, token rings and stars.

Big Data is data that has a large volume so that it cannot be processed using ordinary traditional tools and must use new methods and tools to get value from this data. According to (Zen Munawar, 2020) [5], Big data can be described as high volume, high speed, and high variation of information that demands innovative forms of information processing for insight and decision making.

Data is something that must be protected by its security both in terms of damage and from its confidentiality. Computer network security is a problem that every computer user must pay attention to. It must be noted the need to clean phishing sites, illegal links, spam, etc. on the computer. Never give a chance to criminals because it is a negligence that can have a serious impact on computer security.

Network Security

In maintaining network security, a basic concept or law commonly called the CIA is applied, which is Confidentiality, Integrity, and Availability. Confidentiality is a set of rules that limit access to information. Integrity is a guarantee that information can be trusted and accurate, as well as Availability, which is a concept where information is always available when needed by people who have access or authority.

All forms of threats that come directly or indirectly will interfere with ongoing activities on computer networks. In order to protect against these possible attacks, a firewall concept is necessary. Where the firewall is designed to prevent unwanted access coming from both internal and external networks. The application of the firewall concept looks quite simple, that is, if there is traffic coming to a network, the firewall will then check and control the traffic and send it to its destination.

The aspects and threats to security include

1. Privacy is something that is confidential or private. The point is to prevent this information from being accessed by unknown or unauthorized persons. For example, e-mail or other files that cannot be read by other people even though he is an administrator.
2. Confidentiality is data that is provided to other parties for a specific purpose but its dissemination is maintained. An example is personal data such as: Name, Address, KTP No, Telephone and so on.
3. Integrity or the emphasis is that information cannot be changed except by the owner of the information. Sometimes the integrity of encrypted data is not maintained because there is a possibility that the chaper text of the encryption has changed. Example: An integrity attack when an e-mail is sent in the middle of the road and then its contents are intercepted and changed, so that the e-mail that reaches its destination has been changed.
4. This authentication will be done when the user logs in by using his username and password. This usually relates to a person's access rights, whether he / she is a legitimate accesser or not.
5. Availability, in this aspect relates to whether the data is available when needed or needed by the user. If the security of data or information is too tight, it will make it difficult to access the data. In addition, slow access can also hinder the fulfillment of the availability aspect. The attack that is often carried out in this aspect is Denial of Service (DoS), which is the failure of service when there is a data request so that the computer cannot serve it. Another example of this Denial of Service is sending an excessive request so that it can cause the computer to no longer accommodate the load and eventually the computer goes down.

There are 4 forms of network security threats

1. Misuse of Internet of Things information: Usually when using a computer, users will usually download files, photos, or documents, and they are not used after use. Files, photos or documents that are downloaded usually carry a built-in virus which will become a danger if there is no application to filter the virus.
2. Background attack denial of service: Denial of service is the use of deliberately delaying network services provided when visiting a certain web. It causes certain network damage to a computer.
3. Damage to the integrity of the computer network environment: Damage to the integrity of the computer network environment can be caused by hackers who deliberately want to hack into a network's security system.
4. Computer information leak: When information in a computer network is transmitted directly to an unauthorized entity without the user's permission, it is certain that the information becomes vulnerable. Common forms of vulnerable computer information due to such holes include the following aspects: virus or Trojan horse intrusion into computers, user's own system vulnerability, tapping radio frequency waves on computer information, installation of monitoring equipment, computer network security.

In Langobelen (2019) [4] there are several security handlers to secure computer network systems, namely

1. Block External VPN: External VPN works by hiding the local IP and replacing it with the IP from the VPN, so that users can open certain blocked websites or applications.
2. Block the use of torrent applications: The use of torrent applications does provide various types of programs, films, photos, videos, even paid ebooks can be obtained easily and for free. This media also allows one to share files (file sharing) with other people without the need to download them all at once.
3. Anti DDOS: Flooding attacks via the ICMP protocol or often known as Distributed Denial of Service (DDOS) using TCP port services.
4. Network Security Analysis: The analysis carried out in this study is by penetrating various network-connected devices. The following are the results of penetration that have been tested
   - Penetration on Router Devices
   - Penetration on Server Devices

5. Conclusion

Information technology will continue to grow in line with the fast number of internet users. Based on the latest report We Are Social (2020), it states that there are 175.4 million internet users in Indonesia. This proves that there is an increase of 17% or 25 million internet users in this country. Based on the total population of Indonesia, which amounts to 272.1 million, it means that 64% of the Indonesian population has experienced internet access. Based on the results of internet analysis, it has become a medium that provides information to the public about the dangers and efforts to prevent Covid 19.

Technology is never enough. How well people manage the network and security management makes all the difference and will continue to improve the ways to attack critical data. Network designing is a complex process demanding innovative forms of information processing for gain insights and for decision making.

We see that network security is not only a computer system handler, but there is a need for management to be done to analyze all the risks that might come attacking. With this analysis we do not have to spend very large funds but can use funds efficiently to make it economically feasible.

6. References

1. Corne TC. Legal Protection of Data Privacy Through the Use of Encryption Technology. Essay. University of Lampung. Bandar Lampung, 2019.
2. Dahlan, Zulianto A. Computer Network Design Security In Layer Application Based On Intrusion Prevention System (IPS) Integrated With Access Control List (ACLs), 2019.
3. Hasyim H, Suroso R. The Role of Information Technology in the Prevention of the COVID-19 Virus in the University Environment. Scientific Journal of Electrical Engineering Education. 2020; 4(2):124-128.
4. Langobelen ESROL, Rachmawati RRY, Iswahyudi C. Analysis and Optimization of Network Security Simulation Using Mikrotik Firewall:Case Study in

Taman Pintar Yogyakarta. Journal of Computer Network. 2019; 7:92-102.

5. Munawar Z, Indah N. Computer Network Security In The Era of Big Data, Journal of Information System. 2020; 2(1):14-20.
6. Nugraha F. Wireless Lan Security Analysis on Networks With Captive Portal Authentication. Journal of Informatics Buffer. 2019; 5(1):16-22.
7. Ocanitra R, Ryansyah M. Implementation of Network Security With Firewall Filtering Method Using Mikrotik. Journal of Technology and Information System. 2019; 7:52-59.
8. Rendro BD, Wahyu NA. Monitoring Analysis of Computer Network Security Systems Using NMAP Software (Case Study at SMK Negeri 1 Kota Serang). 2020; 7:2.
9. Susilo A *et al*. Coronavirus Disease Review of Current Literatures. Indonesian Journal of Internal Medicine. 2019-2020; 7(1):45-67.