COMPUTER NETWORK SECURITY SYSTEM USING METHOD WATCHGUARD FIREBOX

Yudha Christianto F.[1)], Sofyan Pariyasto[2)], Wahyu Wijaya W.[3)]

[1, 2, 3]Program Studi Magister Teknik Informatika Program Pascasarjana
Universitas Amikom Yogyakarta
Jalan Ring Road Utara, Condongcatur, Depok, Ngringin,
Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281
Emai : [1]yudha.christianto.f@gmail.com, [2]sofyan@gmail.com, [3]wahyuwijaya8@gmail.com

Abstrak

Keamanan jaringan komputer sebagai bagian dari sistem informasi sangat penting untuk menjaga validitas dan integritas data dan memastikan ketersediaan layanan bagi pengguna, karena sistem jaringan komputer harus dilindungi dari segala macam serangan dan gangguan pada saat atau pemindaian oleh pihak yang tidak berwenang. Komputer yang terhubung ke jaringan, ada banyak ancaman keamanan yang lebih besar dari pada host atau komputer yang terputus di mana saja, sehingga dengan mengendalikan keamanan jaringan, risikonya bisa dikurangi, sehingga jaringan dirancang sebagai komunikasi data yang tinggi dengan Tujuan meningkatkan akses ke sistem komputer, sementara keamanan dirancang untuk mengontrol akses, sehingga penyediaan keamanan jaringan adalah tindakan penyeimbang antara akses terbuka dengan keamanan. Firewall adalah sarana untuk mengendalikan informasi apa yang diizinkan masuk dan keluar dari jaringan lokal dan umumnya host atau firewall komputer yang terhubung ke internet dan LAN lokal, dan akses LAN ke Internet hanya diizinkan melalui firewall, sehingga dengan bantuan firewall dapat mengontrol sistem keamanan jaringan komputer dari apa yang diterima dan dikirim oleh Internet dan LAN. Ada beberapa jenis dan metode dalam pengaturan firewall, melalui pemindaian kode firewall dibangun langsung ke dalam kernel, seperti bantuan ipfw adm ruang pengguna memungkinkan untuk mengubah jenis lalu lintas jaringan atau dengan merekam jenis lalu lintas jaringan, sehingga metode pengaturan firewall dapat menggunakan peralatan bantuan WatchGurad Firebox M400.

Kata Kunci : Komputer, Jaringan, Keamanan, LAN, Firewall

1. INTRODUCTION

Computer network is a necessity that can not be avoided anymore, and in general, the so-called computer network is a group or group of several computers that are interconnected with one another using communication protocols with help through communication media to be able to share information, applications, and also hardware together. Besides that computer networks can also be interpreted as a collection of a number of communication terminals located in various locations consisting of more than one computer that is interconnected.\

Computer networks continue to develop, both from scalability, the number of nodes, and the technology used, because it requires good network management, so that network availability is always there, but in network management there are many problems including those related to network security.

Computer network security (computernetwork security) is a major concern, when we build a network infrastructure. Most network architectures use routers with an integrated firewall system (built-in integrated firewall), as well as support for network software that can facilitate access control, data packet monitoring and the use of tightly regulated protocols.

Network security can also be controlled by adjusting network sharing properties on each computer, which can limit folders and files to be visible to certain users on a network system. In connection with computer security network systems, there are still many uses of

computers - autonomous computers that become incompatible anymore because there are more jobs (jobs) available in the system data integration, and data security on the computer network. Therefore, computer network technology was developed with various methods of security systems used.

a. Aim

The purpose of this writing is used to share knowledge or Knowledge Sharing, to users (Users) and to Organizations / companies that will invest in the field of information and communication technology (ITC), which in particular the utilization of Computer Network System Technology.

1) With computer networks How to set the main data path (backbone) from an ISP (Internet Service Provider) to connect to all users (Users) and service support devices (Servers).
2) Building a computer network security system that refers to the standardization of international network security.

b. Benefits

Benefits of using System Technology This Computer Network Security, namely:

1) Make it easier to monitor existing local computer networks.
2) Make efficient use of the internet in an efficient and effective manner.
3) Building new discipline in the minds of internet users that integrity and responsibility for maintenance are needed in limiting user access rights, because of the many attacks received from the internet.

2. LITERATURE REVIEW

a. OSI Layer Reference

A multinational body founded in 1947 called the International Standards Organization (ISO) as a body that gave birth to international standards. This ISO also issued communication network standards covering all aspects, namely the OSI (Open System Interconnection) model.

b. The purpose

The purpose of this OSI is to facilitate how communication can be established from different systems without the need for significant changes to Hardware and Software at the level of under lying.

"Open" in the OSI is to state the network model that interconnects regardless of the hardware / "hardware" used, as long as the communication software complies with the standard.

"Modularity" refers to the exchange of protocols at a certain level without affecting or damaging relationships or functions from other levels.

The OSI reference model illustrates how information from an application software in a computer moves through a network media to a software application on another computer.

c. OSI Layer Reference Model

The OSI reference model is conceptually divided into 7 layers or layers where each layer has a specific network function, namely:

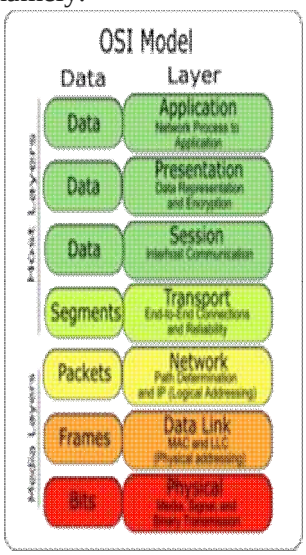

Figure 1. OSI Reference Model

1) Application Layer:
   a) Providing services for user applications. This layer is responsible for exchanging information between computer programs, such as e-mail programs, and other services that are networked, such as printer servers or other computer applications.
   b) Functioning as an interface with applications with network functionality, managing how applications can access the network, and making error messages. The protocols in this layer are HTTP, FTP, SMTP and so on.

2) Presentation Layer:
   a) Responsible for how data is converted and formatted for data transfer. Examples of ASCII text format conversions for documents, gif and JPG for images. This layer forms the conversion code, data translation, encryption and conversion.
   b) Function to translate data that will be sent by the application into a format that can be transmitted through the network.
3) Session Layer:
   a) Determine how the two terminals maintain, maintain and manage connections, how they relate to each other. Connection in this layer is called "session".
   b) Function to define how connections can be made, maintained, or destroyed.
4) Transport Layer:
   a) Responsible for dividing data into segments, maintaining "end-to-end" logical connections between terminals, and providing error handling.
   b) Function of breaking data into data package packages and giving sequence numbers to these packages so that they can be rearranged on the destination side after they are received. At this level a sign is also made that the packet is received with acknowledgment, and retransmits the lost packet in the middle of the road.
5) Network Layer:
   a. Responsible for determining the network address, determining the route that must be taken during the trip, and maintaining the traffic queue in the network. The data in this layer is a package.
   b. Function defines IP addresses, creates headers for packets, and then routes through internetworking by using routers and switches.
6) Data Link Layer:
   a. Providing links for data, packaging them into frames related to "Hardware" then transported through the media. Its communication with a network card, regulates the physical layer communication between the connection system and error handling.
   b. Functioning how bits of data are grouped into formats called frames. In addition, at this level there is error correction, flow control, hardware addressing (MAC Address), and determining how network devices such as hubs, bridges, repeaters, layer 2 switches operate. IEEE 802 specification, divides this level into 2 child levels, namely the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer.
7) Physical Layer:
   a) Responsible for processing data into bits and transferring it through media, such as cables, and maintaining physical connections between systems. This physical layer determines the specification of the physical connection of a computer network.
   b) Function defines network transmission media, signaling methods, bit synchronization, network architecture (eg Ethernet, token ring), network topology and cabling. In addition this level also defines how network interfaces (NICs) can interact with cable or radio media

d. TCP / IP Protocol

1) Definition of TCP / IP TCP / IP (Transmission Control Protocol / Internet Protocol) is one of the protocols or standard network rules that are often used on large and large scale networks. TCP / IP is used because it is flexible and easy to use. TCP / IP consists of several layers of protocol. In its application, TCP / IP protocols are unique in placing on computer addresses.
2) Internet Protocol (IP)
   The IP layer is the core of the TCP / IP protocol where all data originating from all layers above IP must be passed, processed by the IP protocol and sent as an IP packet, IP characteristics, including:
   a) Unreliable
      The Internet Protocol does not guarantee that the sent datagram must arrive at its destination, but does everything possible to send it and if there is a problem in sending

the datagram package it will be notified to the sender of the packet via ICMP (Internet Control Message Protocol) protocol.

b) Connectionless
To send a datagram from the place of origin to the destination both the sender and the recipient do not make an exchange (handshake) first.

c) Datagram delivery service Each packet of data sent is independent of another data packet. Therefore the path taken by each IP data packet to reach the destination will vary from one to the other and the arrival of the package at the destination cannot be successive. This method is used to ensure that the data continues to reach the destination, even though one of the destination paths is interrupted, which is part of the IP package, namely the Network Layer that contains TCP and UDP packages.

e. IP Address

1) Definition of IP Address

Internet Protocol uses an IP Address as an identity, sending data data will be wrapped in a package with a label in the form of the sender's IP Address and the recipient's IP Address. If the recipient sees the packet sending with the appropriate IP Address identity, then the datagram will be retrieved and routed to TCP via the port that corresponds to the application used. IP Address consists of two parts, namely Network ID (network identity) and Host ID (computer identity).

2) Format for Writing IP Address

Format IP Address consists of 4 numbers separated by dots and each of which has a maximum value of 255. This maximum value is obtained from 28. This is because the format of the IP Address is a binary number consisting only of 0 and 1. So the value obtained from 0 - 255. The format of writing the IP Address is as follows:

- binary form Address:
0000000.0000000.0000000.0000000
11111111.11111111.1111111.1111111
1
- Decimal form of IP Address:
255.255.255.255

3) IP Address Class

Basically the IP Address has two parts, namely Network ID and Host ID. Network ID determines the network address while Host ID specifies the host / computer address. IP Address is divided into three classes as shown in the table below:

Table 1. Net-ID

Kelas	N- ID	H- ID	Subnet Mask
A	8 bit	24 bit	255.0.0.0
B	16 bit	16 bit	255.255.0.0
C	24 bit	8 bit	255.255.255.0

In order for the equipment to know the class of an IP Address, each IP Address must have a subnet mask. Decimal number 255 or binary 11111111 a default subnet mask indicates that the octet of an IP Address is for network ID.

While the decimal number 0 or binary 00000000 indicates that octets are for host ID. By paying attention to the default subnet that is given, the class of an IP Address can be known.

To distinguish one class from another, several rules are made as follows:

a. The first octet of class A must begin with binary number 0
b. The first octet of class B must begin with binary number 10
c. The first octet of class C must start with a binary number 110
d. The first octet of class D must begin with a binary number 1110
e. The first octet of class E must begin with a binary number 1111

Table 2 Class IP Address

Kelas	Kelompok oktet pertama dalam decimal
A	1 – 126
B	128 – 191
C	192 – 223
D	224 – 239
E	240 – 247

Besides the rules about the IP Address class there are also some additional rules that need to be known, namely:

a. The number 127 in the first octet is used for loopback.
b. Network ID may not all consist of numbers 0 or 1.
c. Host ID may not all consist of numbers 0 or 1.

f. Subnetting
Networks with certain sizes are rarely used directly to form a network. Usually companies have more than one network (LAN), each of which has more hosts than the maximum number of hosts provided by one IP class. Addresses in groups A, B and C are grouped in a group called sub networks or subnets. The uses of subnetting include:
   a. Integrating different technologies, such as Ethernet and token rings.
   b. Avoid limited number of nodes in one segment.
   c. Reducing traffic caused by broadcasts or collisions on Ethernet networks.

g. Benefits of Network Systems
Understanding Computer networks are a group of separate computers that are connected to one another by using communication protocols through transmission media or communication media. so that they can share information, programs, and shared use, namely:

Resource Sharing

By implementing the network, you can use the resources together. And also can overcome the problem of distance or can connect with other people from various countries.

Hardware and Software Sharing Can share hardware and software simultaneously, so that all files can be saved or copied to computers connected to the network. So if one of the machines is damaged, then another copy of the machine can be used.

Effective and Efficiency

Computer Networks can share or share between Users and the process of sending data faster (effectively), can also reduce operational costs, such as paper use, sending and receiving letters and documents, telephone use and purchasing network equipment that is not expensive (Efficiency).

h. Network Architecture
Client - Server network A computer functions as a server, and other computers as clients. The server computer is in charge of serving all the computers contained in the network. Komputerclient who will receive services from a server computer.

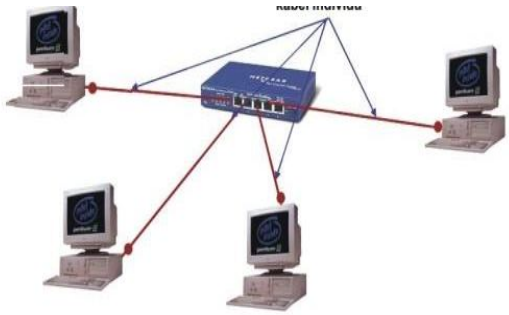

Figure 1 Client - Server Network

3. RESULTS AND DISCUSSION

a. Firewall

Firewall is a technique that is very useful and important in securing networks, and Firewall is a model or system of mechanisms that is applied both to hardware devices, software or to the system itself with the aim of protecting, either by filtering, limiting or even rejecting a relationship or all the activity of a segment on a private network with an outside network that is not its scope, the segment can be a workstation, server, router and or LAN network.

To be able to connect to the Internet (other networks) it must enter the firewall server (can be remote or direct), a software system that allows network traffic that is considered safe to be able to pass through and prevent network traffic that is considered unsafe. Generally, a firewall is applied to a dedicated machine, which runs on the gateway between the local network and the Internet network, firewall (wall-fire) is used to limit or control access to anyone who has access to private networks from outside parties. At present, the term firewall is a common term that refers to a system that regulates communication between two different types of networks. Given that currently many companies have access to the Internet and of course, the network has legal entities in it, so the protection of the

company's digital devices from attacks by hackers, spies, or other data thieves becomes a reality.

Firewall is divided into two types, namely as follows:

a. Personal Firewall.

Personal Firewall is designed to protect a computer connected to the network from unwanted access. This type of firewall has recently evolved into a collection of programs that aim to secure the computer in total, with the addition of several security features plus some kind of protection against viruses, anti-spyware, anti-spam, and others. In fact, several other firewall products are equipped with the function of detecting network security problems (Intrusion Detection System). An example of this type of firewall is Microsoft Windows Firewall (which has been integrated into the Windows XP Service Pack 2 operating system, Windows Vista and Windows Server 2003 Service Pack 1), Symantec Norton Personal Firewall, Kerio Personal Firewall, and others. Personal Firewall generally only has two main features, namely Packet Filter Firewall and Stateful Firewall.

b. Network Firewall.

Network Firewall is designed to protect the network as a whole from various attacks. Generally found in two forms, namely a dedicated device or as a software installed on a server. Examples of these firewalls are Microsoft Internet Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, WatchGuard, Juniper SRX, Fortigate, IPTables in the GNU / Linux operating system, pf in the BSD Unix operating system family, and SunScreen from Sun Microsystems , Inc. which is bundled in the Solaris operating system.

Basically, a firewall can do the following:

1) Manage and control network traffic.
2) Authenticate access.
3) Protecting resources in private networks.
4) Record all events, and report to the administrator.

Figure 2. Firewall

c. Rules and Policy

Rules and Policy are the main technicalities in a firewall where through a rule and policy a network administrator can control the firewall's working system and can dynamically monitor and maximize the productivity of network devices.

d. Port Interface

Understanding the Interface (Interface) is a communication mechanism between users (users) with the system. Interfaces (interfaces) can receive information from users (users) and provide information to users (users) to help direct the search path to find a solution.

The interface, functions to input new knowledge into the expert system knowledge base (Expert System), by displaying an explanation of the system and providing guidance on the overall use of the system or step by step so that the user understands what will be done on a system. The most important thing is the ease of using or running a system, interactive, communicative, while the difficulty in developing or building a program should not be overly demonstrated. Existing interfaces for various systems, and provide ways:

1) Input, allows users to manipulate the system.
2) Output, allows the system to show the effect of user manipulation.

e. Routing

1) Routing is the process of selecting the path that a packet must pass. Good paths depend on network load, datagram length, requested type of service and traffic patterns.
2) In general, routing schemes only consider the shortest path.
   There are 2 forms of routing, namely:
   - Direct Routing (direct delivery); packets are sent from one machine to

another directly (the host is on the same physical network) so there is no need to go through another machine or gateway.

- Indirect Routing (indirect delivery); packets are sent from one machine to another machine that is not directly connected (different networks) so that the packet will pass through one or more gateways or other networks before reaching the destination machine.

f. Routing Table

Routers recommend about the path used to pass packets based on the information found in the Routing Table.

The information contained in the routing table can be obtained by static routing through administrator intermediaries by manually filling the routing table or dynamically routing using the routing protocol, where each connected router will exchange routing information in order to find out the destination address and maintain the routing table.

Routing tables generally contain information about:

1) Destination Network Address.
2) Router interface that is closest to the destination network.
3) Metric, which is a value that indicates the distance to reach the destination network. Metric uses techniques based on the number of jumps.

g. NAT (Network Address Translation)

NAT (Network Address Translation) or Interpretation of network addresses is a method for connecting more than one computer to an internet network using one IP address. The number of uses of this method is due to the availability of limited IP addresses, the need for security (security), and the ease and flexibility in network administration.

1) Understanding Static NAT

Static NAT or static NAT uses a fixed routing table, or translational allocation of ip addresses set according to the original address or source to the destination address or destination, so it does not allow the exchange of data in an ip address if the translation of the ip address has not been registered in the nat table. Static translation occurs when a local address (inside) is mapped to a global address / internet (outside). Local and global addresses are mapped one by one statically. NAT will statically make a request or retrieve and send data packets in accordance with the rules that have been set in a NAT.

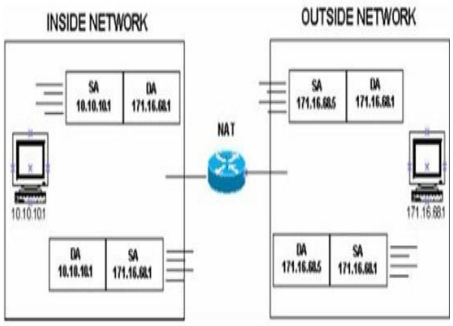

Figure 8. Static NAT

2) Understanding Dynamic Type NAT.

NAT with dynamic type uses logic balancing or uses load-setting logic, where the logic of its own possibilities and solutions has been embedded in the table, NAT with dynamic type is generally divided into 2 types, namely NAT system pool and NAT system overload.

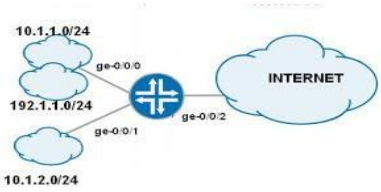

Figure 9. Dynamic NAT

h. Blocking / Filtering

In its simplest form, a firewall is a router or computer equipped with two NICs (Network Interface Cards), a network interface card that is capable of filtering or filtering incoming packets. This type of device is generally called a packet-filtering router.

This type of firewall works by comparing the source addresses of these packages with access control policies registered in the Access Control List firewall, the router will try to decide whether to forward the incoming packet to its destination or stop it.

In a simpler form, the firewall only tests the IP address or domain name that is the

source of the package and will determine whether to forward or reject the package. However, packet-filtering routers cannot be used to provide access (or reject it) using the basis of the rights owned by users, for example:

1) Blocking Internal to Internet Web Filtering
   - Gateway Antivirus
   - IPS (Intrusion Prevention Services)
   - Application Control
   - Web Filtering

Blocing External to Internal

- Spam Blocker
- Data Lost Prevention (DLP)
- Quarantine Server
- APT Blocker

4. CONCLUSION

In this conclusion, research uses the SWOT method on the WatchGurad Firebox M400 device.

a. Strength
   1) Have a good level of security.
   2) Features that are needed by large and medium-sized companies.
   3) Has quite a lot of VPN features from low-end and high-end ones.
   4) Can be integrated with several different brands and operating systems.

b. Weakness
   1) There are still many bugs if configured in different modes.
   2) This device has subcription on its license and it is quite expensive for a newly developing company.
   3) This device is quite hot and needs an AC cooler.

c. Opportunities
   1) This device has the opportunity to win some hearts from IT managers in each company that have not used it.
   2) This device has a fairly high configuration level with its interface.
   3) This device can also be implemented in several types of modes.

d. Threats
   1) This device has many threats with the presence of several firewall devices that are similar to different products.
   2) This device cannot compete if there is a firewall device that is lower in price.
   3) This device cannot stand when there is interference from nature, for example: lightning and wind when implanted in the shellter.

5. REFERENCES

Hasnul Arifn, 2011, *Jaringan Komputer & Koneksi Internet,* Cetakan pertama, MediaCom, Jakarta.

Kristanto Andi, 2003, *Jaringan Komputer*, Cetakan pertama, Graha ilmu, Yogjakarta.

Kercheval Berry, 2002, *DHCP Panduan Untuk Konfigurasi Jaringan TCP/IP Yang Dinamis*, Cetakan kedua, Andi,Yogjakarta.

Sugiyono, 2006 *Panduan Teknik Komputer* Edisi ke3, PT. Puspa Swara, Cimanggis – Depok.

Turban, dkk, 2006, *Pengantar Teknologi informasi,* Edisi ke-3, Salemba Infotek, Jakarta.

Yani Ahmad, 2007, *Panduan Membangun Jaringan Komputer, PT. Kawan Pustaka*, Jakarta.

Agus, Sumin. "Pengantar Teori Jaringan Komputer"**.** Jakarta : Gunadarma. 1995.

Imam, Ghozali. "Aplikasi Analisis Multivariate Dengan Program SPSS". Universitas Diponegoro Semarang. 2009.

Jogiyanto. "Metode Penelitian Sistem Informasi"**.** Andi. Yogyakarta. 2008.

Rifki, Amalia. "Analisis Keamanan Sistem