The development of computer technology, in addition to causing the many benefits also have many bad side. One of them is an attack on a computer system connected to the Internet. As a result of the attack, many computer systems or networks disrupted even become corrupted. To overcome this, the necessary security systems to cope with and prevent activities that may attack our network system.

Security is paramount in a network. To perform such security, such planning can be done to determine what data or information that must be protected. In addition, it is necessary to carry out some methods of planning that is restricting access to a network where there are passwords, encryption, and monitoring scheduled on the network.

Administrator account on a server should be renamed and preferably only one account can access. Giving proper password security policy in the admin account, the password must have a unique character and difficult to predict.

To test the password created. There are utilities that can be used to test the reliability of the password, using software such as Avior aimed to perform a brute-force passwords. Authority access to other users in an enterprise need to be documented, this is done to meet the needs of clients. The authority of a user other than the administrator include the input data according to the latest data for the specific purpose of meeting the needs of clients.

Encryption can use cryptographic methods that are designed to ensure the privacy, prevent the spread of information without permission. However, privacy is not the only service provided cryptography. Cryptography can also be used to support authentication (verifying user identity) and integrity (ensuring that the message has not been modified).

Cryptography is used to prevent unauthorized people to enter the communications, so that data privacy can be protected. Broadly speaking, cryptography is used to send and receive messages. Cryptography is essentially based on the key that has been selectively plated on a computer in the same network and is used to process a message.

The threat to the network can be monitored and wary by the network administrator as destructive programs (viruses) that can compromise the security of a network. Administrators can install an antivirus program on the workstation. Anti-virus device has a function to define and eradicate the virus will enter into a workstation such as Norton, McAfee, etc..

However, the virus will not become a useful deterrence if the administrator does not perform virus definition updates to anti-virus software has been installed on the workstation. Monitoring can also be done by auditing the system log on a particular server by a network administrator. The goal is to identify security threats and interference that will occur on the network. Administrators can also use software like NSauditor aimed to evaluate network security and may conduct audits to handling errors. In addition, there are tools that can be used to diagnose as GFI Network Server Monitoring, MRTG, etc..

Intrusion Detection System (IDS) is a system for detecting network abuse and computer resources. IDS has a number of sensors are used to detect intrusions. IDS system is responsible for collecting data from sensors virgin-and then analyze it to give to the network security administrator. The aim is to give a warning against interference in the network.

A firewall is a means or mechanism applied both to hardware, software or system itself in order to protect, either by filtering, limit or even reject any or all relationships / activities of a segment on a private network with external networks that are not in scope. These segments can be a workstation, server, router, or local area network (LAN) you.

Characteristics of a firewall, like the whole relationship / activity from the inside out, pass through the firewall. This can be done by block / limit both physically all access to the local network, except through the firewall. There are so many forms of network configurations that allow it to happen, only the activities listed / known to pass through / have sex, this can be done by adjusting the local security policy on the configuration. There are so many types of firewalls that can be selected at the same time to offer different types of policy, as well as firewall itself should be relatively strong or invulnerable to attacks / weaknesses. this means the use of a reliable system and the system is relatively safe.

This type of firewall that is divided into two types of firewall software which background programs running on your computer. This software evaluates each request from the network and determines whether the request is valid or not. Those advantages include low price and easy to configure. Meanwhile, drawbacks such as consuming the resources of the computer (CPU, memory, disk space) that can lead to incompatibilities in operating systems. There are different versions for different operating systems, so it must be ensured that the firewall software is installed the appropriate version of your operating system. It takes several different copies for each system in the network.

Hardware firewall is a firewall that is installed on the computer, the computer connects to the modem. Those advantages include providing more protection than a software firewall. A hardware firewall can protect the entire network; operates independently of the operating system and application software so that system performance will not be compromised. Meanwhile, such shortcomings tend to be more expensive than a software firewall. However, if you have multiple machines to be protected would be cheaper to buy one

Hardware firewall than buying multiple copies of a software firewall, for not walking independently, firewall hardware configuration is quite difficult. Apart from a safety perspective, the problem of tissue damage can occur due to various things, such as natural disasters or obsolete components. This section will discuss how to tackle the problems that exist on the network.