Weekly find the perpetrator. firewall systems usually have

Weekly Activity This week start with a excellent seminar in Medipol University which is about 6G. Big names from big companies presented significant informations. It was a unique experience to participate in that program. I also have the opportunity to do more extensive work on the firewall this week. More detailed reviews were made.

TCP/IP is the basic protocol * package of the internet. Since TCP / IP, which controls the flow of data over the Internet, is created by assembling many protocols, we call it the protocol package. TCP deals with the " Points to note in point-to-point data transfer" part of this protocol package, while IP deals with " Specifying the path to move data". Basic services of TCP / IP; – DNS (Domain Name System) – SMTP (Simple Mail Transfer Protocol) – POP (Post Office Protocol) – FTP (File Transfer Protocol) – Telnet (Terminal Emulation) – NEWS Firewall is a software-based system that controls the communication between the local network and the Internet. Our local area is under the control of the firewall system that comes from the internet or from the local area.

The purpose of this system is to protect the data on our local network, to protect it against any dangerous activity that could come from the outside world and possibly make it impossible to find the perpetrator. Firewall systems usually have a simple set of rules. For example; To drop all kinds of data packets that want to access the local area directly from the outside world, to not interfere with any packet that wants to access the outside world from the local network.

We can decide together some basic rules together. For example, any package coming directly from the outside world should be discarded. If any package is allowed to enter directly, even for an innocent purpose, a malicious hacker can hide any harmful work he or she has done using this path in this seemingly innocent way. It can reach its evil goals by using this path. So our basic rule must be very precise and rigid. No direct package from the outside will enter !. But on the other hand, it is also imperative to allow some requests to enter. Because some parts of the corporate network such as web server, ftp server, mail server have to respond to requests from the outside world.

If so, we must create an intermediate region that we can define neither as the inner world nor as the outer world. This zone is usually called the Demilitarized Zone word DMZ, which means the demilitarized zone. Entrance into the internal network from the DMZ is strictly not allowed.

Because a hacker can capture the DMZ by catching some of the exploits of the limited rights in the DMZ. This point should not find a way to go in again. We understand from this information that some hackers are CIA, NASA, etc. Attacks on their web sites often do not mean that they can infiltrate very confidential information. One consequence of the information provided so far is that the firewall is actually some sort of router.