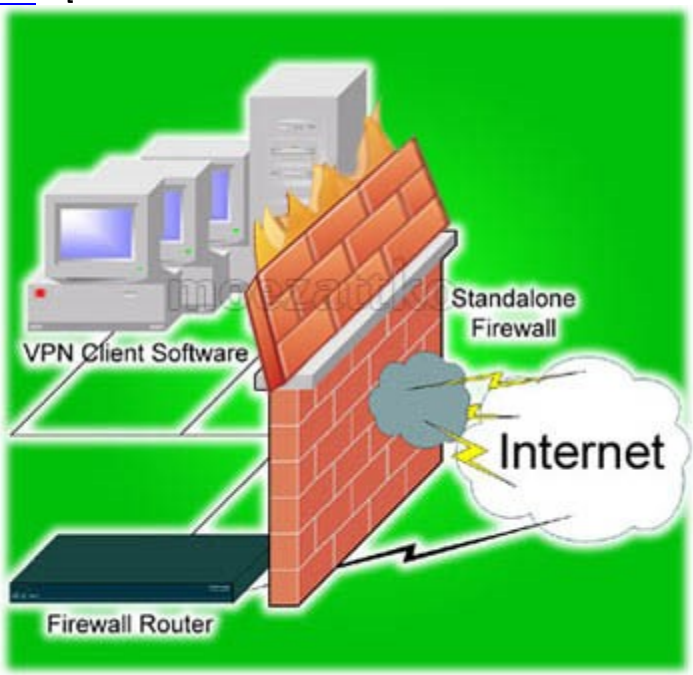
# Firewall အကြောင်းနှင့် ပက်သက်၍

[color=blue]Firewall (သို့မဟုတ်) ဂိတ်မျူး

Firewall အခေါ်အဝေါ်စတင်ပုံ

Firewall ဆိုတဲ့ အခေါ်အဝေါ်ဟာ မူလအားဖြင့် Construction ဘက်ကလာတဲ့ အခေါ်အဝေါ်တစ်ခုဖြစ်ပါတယ်.. မီးကိုကာကွယ် တားဆီးတဲ့နေရာမှာ သုံးခဲ့သလို တံခါးတွေအဖြစ်လည်း အသုံးပြုခဲ့ကြပါတယ်.. နောက်ပြီး ကားတွေရဲ့အင်ဂျင်ခန်း ဒါမှမဟုတ် လေယာဉ် တွေရဲ့ အင်ဂျင်ခန်းတွေမှာ ကာပေးထားတဲ့ Metal sheet အကာအကွယ်ကိုလည်း Firewall လို့ခေါ်ပါတယ်.. ကွန်ပျူတာမှာ သုံးနေတဲ့ Firewall အခေါ်အဝေါ်ကတော့ 1980 နှစ်များနောက်ပိုင်း အင်တာနက်ကြီးလွမ်းမိုးစပြုလာတဲ့ အချိန်ကျမှ..Internet Security မလုံခြုံမှု များကြောင့် ပေါ်ပေါက်လာခဲ့တာဖြစ်ပါတယ်.. ဘာဖြစ်လို့လဲဆိုတော့ .. security ချိုးဖောက်မှုများကြုံတွေ့လာရသောကြောင့် .. ဖြစ်ပါတယ်..

Firewall ဆိုတာ




Firewall ဆိုတာဘာလဲလို့ဆိုတော့။ Firewall ဆိုတာ အရပ်စကားနဲ့ပြောမယ်ဆိုရင် ပြင်ပ ပယောဂအနှောက်အယှက်များ မဂင်ရောက် နိုင်အောင် နှင့် ကိုယ့်ဖက်က လုံခြုံရေးချို့ယွင်းကြောင့် ပြင်ပကို မပေါက်ကြားနိုင်အောင် ကာကွယ်တားဆီးပေးနိုင်တဲ့ နည်းပညာတစ်မျိုးဘဲဖြစ်ပါတယ်.. ဒါက.. အလွယ်တကူပြောလိုက်တာ .. တကယ်တမ်း သီအိုရီအရ ပြောရမယ်ဆိုရင် Firewall ဆိုတာ Network Computer System တွေကို Electronically အရ Network တွေတစ်ခုနဲ့တစ်ခုကြားမှာ

လုံးဝဆက်သွယ်မှု ဖြတ်တောက်ထားခြင်းမဟုတ်ဘဲ မသက်ဆိုင်တဲ့ ကူးလူးဆက်သွယ်မှုတွေကို ပိတ်ပင်တားဆီးပြီး သက်ဆိုင်လိုအပ်တဲ့ကူးလူး ဆက်သွယ်မှုတွေကို လိုအပ်သလို စီစစ်ခွင့်ပြုမှတ်တမ်းတင်ထားနိုင်တဲ့ လုံခြုံရေးဆိုင်ရာ နည်းပညာတစ်ရပ်ပါပဲ... Firewall က ဘာတွေလုပ်ပေးလဲဆိုတော့ .. သူ့ကို .. Administrator က သတ်မှတ်ပေးထားတဲ့ Rules တွေ အခြေအနေတွေ အခြားသော Criteria တွေပေါ်မူတယ်ပြီး မတူညီတဲ့ Security Domain တွေကြား အားလုံးသော Network Traffic များကို Allow လုပ် မှာ လား Deny လုပ်မှာလား Encrypt လုပ်မလား Decrypt လုပ်မလား Proxyfy လုပ်မလား စသဖြင့် အလုပ်တွေကို လုပ်ဆောင်ပေးမှာပါ.. အထူးသဖြင့် Network Traffic များကို perimeter (zone ပတ်ပတ်လည်) စစ်ဆေးပြီး ကာကွယ်ပေးနိုင်တယ်လို့ဆိုလိုတာပါ ..

အဲဒီ Firewall နည်းပညာဟာ Hardware-Based အနေနဲ့လည်းရနိုင်ပါတယ်။ Software-Based အနေနဲ့လည်းရနိုင်ပါတယ်။

Hardware-Based တွေကိုတော့ Firewall တစ်လုံးမှာ ရှိသင့်ရှိထိုက်တဲ့ Commector Ports တွေနဲ့ Built-in Firewall OS တစ်ခု ပါဝင်ဖွဲ့စည်းထားတဲ့ Special Purpose Computer တစ်လုံးအသွင်နဲ့ တွေ့မြင်ရနိုင်ပါတယ်။

ဒါပေမဲ့ သူ့ရဲ့ ပုံစံကတော့ Computer တစ်လုံးအသွင်ရှိနေမှာ မဟုတ်ပါဘူး။ သူ့ရဲ့ Firewall Configuration တွေကို ပြင်ဆင်ချင်ရင်တော့ သူ့မှာပါလာမယ့် Console Port နဲ့ Computer နဲ့ တိုက်ရိုက်ချိတ်ဆက်ပြီး Browser မှ (သို့မဟုတ်) DOS မှဝင်ရောက်ပြင်ဆင် Configured လုပ်ပေးရမှာ ဖြစ်ပါတယ် အဲဒီလိုမျိုး နည်းပညာကို

တကယ့် Enterprise Level Company ကြီးမှာ သာအသုံးပြုတာများကြပါတယ် ..သူတို့က စျေးအရရော နည်းပညာအရမှာပါ မြင့်မားရှုပ်ထွေးမှုရှိပါတယ်။ လုံခြုံရေးအရလည်း အထူးပိုပြီးအားကောင်းပါတယ်။

Software-Based Firewall တွေကတော့ စျေးနှုန်းအရမှာရော နည်းပညာအရမှာပါ သက်သာလွယ်ကူပါတယ်။
သူတို့ကိုတော့ မိမိနှစ်သက်ရာ Performance ကောင်းတဲ့ Computer တစ်လုံးမှာ Install လုပ်ပေးထားရမှာပါ။ Install လုပ်ထားမယ့် Firewall အဖြစ်သုံးဖို့ ရွေးချယ်ထားတဲ့ Computer ဟာ Performance ပိုင်းမှာတော့ စိတ်ချရဖို့လိုအပ်ပါတယ်။
ဒါမှသာ လိုအပ်တဲ့ Processing လုပ်ဆောင်မှုတွေကိုမြန်မြန်ဆန်ဆန် ဆုံးဖြတ်လုပ်ဆောင်ပေးနိုင်မှာပါ။ သူတို့အများစုကတော့ Installed လုပ်ထားတဲ့ Computer ကနေပဲ

တိုက်ရိုက် GUI နဲ့ဖြစ်စေ DOS နဲ့ဖြစ်စေ Configured လုပ်ထားနိုင်ပါတယ်။ ဒါပေမယ့် Astaro လိုတချို့ Firewall မျိုးကတော့ Installed လုပ်ထားတဲ့ Computer က direct မရဘဲ အခြား Computer တစ်လုံးကနေသူ့ရဲ့ IP Address ကို Browser ကခေါ်ပြီး Configured လုပ်ရပါလိမ့်မယ်။ ဘယ်လိုပင် ဖြစ်စေ Software Firewall တွေဟာ Hardware Firewall တွေနဲ့ယှဉ်ရင် စျေးနှုန်းအရလည်း လေးငါးဆမကကွာခြားသက်သာပါတယ်။ နည်းပညာရှုပ်ထွေးမှုလည်း နည်းပါးပါတယ်။ ဒါကြောင့် တော်ရုံတန်ရုံ Company ကြီးတွေမှာတောင် Software Firewall ကိုသုံးစွဲတာများကြပါတယ် ဒါပေမဲ့ အရာရာတိုင်းဟာ အကောင်းနဲ့အဆိုးဒွန့်တွဲနေတာ ပါဘဲ။ တစ်ချို့.. သိပ်ကို အရေးကြီးတဲ့နေရာတွေမှာဆိုရင် Firewall ကို ပုံစံအမျိုးမျိုးနဲ့ အဆင့်ဆင့် ခံထားတတ်ကြပါတယ် .. အထူးသဖြင့် ISP လိုနေရာမျိုးတွေမှာပါ.. တခြား သုံးတဲ့နေရာတွေလည်း အများကြီးရှိပါတယ်.. ထပ်ပြီး ပြောရမယ်ဆိုရင် .. Firewall ဆိုတာ http://en.wikipedia.org/wiki/Private_network"]private Network[/URL] တစ်ခု နဲ့ Public Network (Internet Connection) တို့ရဲ့ ကြားသူတို့ နှစ်ခု ချိတ်ဆက်တဲ့ နေရာမှာ ကြားခံထားရမယ့် Security ထိန်းချုပ်ပေးတဲ့ ပစ္စည်း ကိရိယာ (Hardware_based) သို့မဟုတ် နည်းပညာ software (Software _based) တစ်ခုပဲဖြစ်ပါတယ်။ ကိုယ်ရဲ့ Network က Public Network (Internet) နဲ့ ချိတ်ဆက်ထားခြင်းမရှိရင် (သို့မဟုတ်) အရေးကြီးတဲ့ Data မျိုးတွေ မရှိဘူးဆိုရင် တော့ Firewall မတပ်ဆင်ထားလဲ ပြဿနာ မရှိနိုင်ဘူးပေါ့။ တကယ်လို့ ကိုယ့်ရဲ့ Network က Public Network နဲ့လည်းချိတ်ဆက်ထားတယ်။ Data တွေကလည်းအရမ်းအရေးကြီး တယ်လို့ထင်ရင် .. Firewall ကို တပ်ကိုတပ်သင့်ပါတယ် .. အဲဒါကြောင့် Router တွေမှာပါ Firewall Function တွေကို ထည့်သွင်းလာရခြင်းဖြစ်ပါတယ်.. မဟုတ်ရင် .. http://en.wikipedia.org/wiki/Packet_sniffer"]packed sniffer [/URL] တွေရဲ့ရန်က ကင်းနိုင်မှာမဟုတ်ပါဘူး..

Firewall နဲ့ပတ်သက်ပြီး နောက်ထပ်နည်းနည်းပြောစရာရှိတာက Firewall ဆိုတာကို တပ်ထား/သုံးထား ပေမဲ့ သုံးမဲ့ Administrator က configuration ကို သေသေချာချာသတ်မှတ်ပေးရပါဦးမယ်.. ဒါမှမဟုတ်ရင် .. Firewall ကို သေချာ Rule တွေ သတ်မှတ်မထားရင် တပ်ထားတာ အလကားဖြစ်နိုင်ပါတယ် .. တစ်ချို့ Firewall များဟာ Configure လုပ်ရတာ တော်တော် ခက်ခဲ ပါတယ်.. နောက်ပြီး Rules တွေကို တော်တော်အသေးစိတ်သတ်မှတ်ပေးရတယ်.....ဒါကြောင့် တစ်ချို့ Firewall များကို Default Deny အတိုင်းထားကြပြီး လိုအပ်မယ်ထင်တဲ့ ခွင့်ပြုစေချင်တဲ့ traffic များကို Manually တိုက်ရိုက် Explicity နည်းနဲ့ပြန်ပြီး Allow လုပ်ပေးကြတာများပါတယ်.. Firewall ကို Administrator ကအခါအားလျော်စွာစောင့်ကြည့်နေဖို့လိုပါတယ် .. တစ်ခါတစ်ခါ .. အကြောင်းအမျိုးမျိုးကြောင့် ... Default Allow ဖြစ်သွားတတ်တာတွေရှိပါတယ် .. အဲဒါဆိုရင် တော့ အနောက်အယှက် ပေးနိုင်တဲ့ http://en.wikipedia.org/wiki/Network_traffic"]Network Traffic[/URL]

တွေရဲ့ရန်ကလည်း မကင်းနိုင်ပါဘူး.. ဂင်ရောက်ပြီး .. ဒုက္ခပေးသွားနိုင်ပါတယ် ..ုံ

Firewall ဘယ်နှစ်မျိုးရှိသလဲ..
ဘယ်နှစ်မျိုးရှိလဲဆိုတော့ လွယ်လွယ်ပြောရရင် ..၂ မျိုးဘဲရှိပါတယ် ..Software Firewall နဲ့ Hardware Firewall ပါ..

ဒါပေမဲ့ .. Firewall ကို အုပ်စု ၄ မျိုးခွဲထားပါတယ်.. ဒါတွေကတော့

1. Free Firewall
2. Desktop Firewall
3. Software Firewall
4. Hardware Firewall တို့ပါဘဲ..

Free Firewall ဆိုသည်မှာ..
Free Firewall တွေဟာ Software များဖြစ်ကြပြီး များသောအားဖြင့် ၄င်းတို့ဟာ အလွယ်တကူ Setup လုပ်နိုင်ကြပါတယ် သူတို့တွေ ဟာ ကုမ္ပဏီအသေးလေးတွေကနေ အလယ်အလတ်တန်းအစား အထိအသုံးပြုနိုင်ကြပါတယ်.. Free Firewall တွေဟာများသောအားဖြင့် Desktop Firewall ပုံစံနဲ့လာတတ်ကြပါတယ်.. ၄င်းကို Personal Firewall လို့လည်း ခေါ်ပါတယ်..

Desktop Firewall ဆိုသည်မှာ..
ကွန်ပျူတာ တစ်လုံးတည်းအတွက် ကာကွယ်ဖို့ဘဲ အဲဒီကွန်ပျူတာရဲ့ OS မှာ Installed လုပ်ထားတဲ့ မည်သည့် Software ကိုမဆို Desktop Firewall လို့ခေါ်တာဖြစ်ပါတယ်.. Desktop Firewall ကိုလည်း Personal Firewall လို့လည်းခေါ်ပါတယ်.. ဒီ Desktop Firewall များ ဟာ Single Desktop Computer တွေအတွက်ဘဲ ဒီဇိုင်းလုပ်ထားတာကဖြစ်ပါတယ်.. ဒါပေမဲ့.. Single Firewall ကို Network Firewall နဲ့တွဲပြီး သုံးလို့ရပါတယ်.. အဲဒီလိုလုပ်လိုက်ခြင်းအားဖြင့် .. စွမ်းဆောင်ရည်ပိုမိုကောင်းမွန်လာပါတယ်.. Windows မှာပါလာတဲ့ Firewall ဟာ Basic Firewall ဖြစ်ပါတယ်.. အဲဒါကို တစ်ခြား သောDesktop Firewall များနဲ့ အစားထိုးပြီးလုပ်ခိုင်းနိုင်သလို Hardware Firewall များနဲ့ လည်းတွဲဖက် အလုပ်လုပ်ခိုင်းလို့ရပါတယ်..

Desktop Firewall တွေရဲ့အကျိုးကျေးဇူးများ
1. Purchase version Desktop Firewall တွေဆိုရင် Virus Scanner များနှင့်တွဲဖက်လုပ်ဆောင်နိုင်ခြင်း..
2. Hardware Firewall မဟုတ်တာကြောင့် .. ကြိုးများနှင့်တစ်ခြား Installation

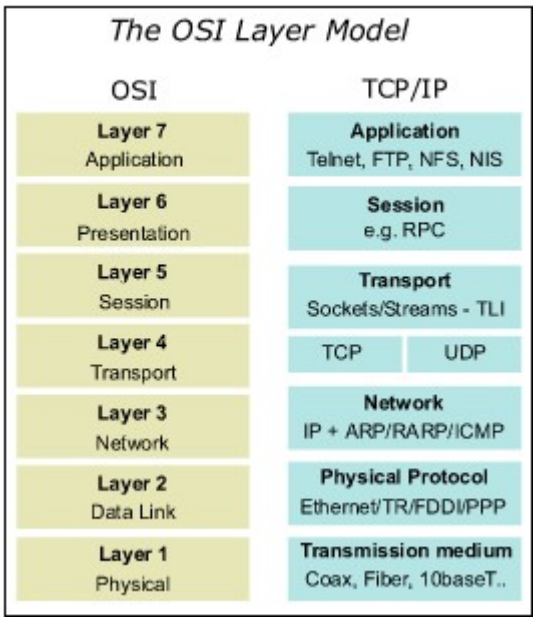
အပိုင်းများတွင်လွယ်ကူခြင်း
3. နောက်ပြီး Portable Computer တွေမှာ(ဥပမာ-Laptop ) တွေမှာ Software Firewall တင်ထားလို့ရှိရင် ဘယ်နေရာကိုသွားပြီး

အင်တာနက်ချိတ်ချိတ် .. ကာကွယ်ပေးနိုင်ခြင်း စသည့်ဖြင့်.. လုပ်လည်းလုပ်ထားသင့်ပါတယ်..

Software Firewall ဆိုသည်မှာ..
ဒီ Software Firewall ဆိုတာ server OS တွေမှာ install လုပ်ရတဲ့ software package ဘဲဖြစ်ပါတယ်.. ဒီအမျိုးအစားကတော့ အလွန်ကို Secure ဖြစ်စေတဲ့ Firewall အမျိုးအစားဖြစ်ပါတယ်.. ဘာဖြစ်လို့လဲဆိုတော့ အဲဒီ OS ကနေပြီး ခွဲသုံးကြတဲ့ Client တွေကို ကာကွယ် ပေးနိုင်တဲ့ security နည်းပညာများပါရှိနေလို့ပါဘဲ.. ဒီ Firewall ကို Application Firewall အဖြစ်လဲအသုံးချလို့ရပါသေးတယ်.. ဆိုလိုတာက Web Application တွေ Email server တွေကို အကောင်းဆုံး ကာကွယ်ပေးနိုင်ပါတယ်.. ဒါပေမဲ့.. ဒီလိုကာကွယ်ပေးနိုင်စေဖို့ အရမ်းကို ရှုပ် ထွေးတဲ့ Network Traffic Filter များကိုသတ်မှတ်ပေးရပါတယ်.. နည်းနည်းတော့ configure လုပ်ရတာ ခက်တယ်ပေါ့..

Hardware Firewall ဆိုတာ ..
Hardware Firewall ဆိုတာ ပစ္စည်းတစ်ခုဖြစ်ပါတယ်.. အများအားဖြင့်တော့ Network Router တွေနဲ့တွဲပြီး Build in Firewall Function ပါလေ့ရှိကြပါတယ်.. Firewall Function ပါတဲ့ Router နဲ့ မပါတဲ့ Router ဟာစျေးနည်းနည်းဘဲကွာပါတယ်.. Firewall ပါတဲ့ဟာက ပိုကောင်း တာပေါ့ .. ဒီ Hardware Firewall များကို အရေအတွက်များပြားလှတဲ့ Network Traffic တွေကို ထိန်းချုပ်ကိုင်တွယ် နိုင်အောင် တီထွင် ထုတ် လုပ်ထားတာဖြစ်ပါတယ်.. Hardware Firewall များကို လုပ်ငန်းရဲ့ Boundry မှာထားလေ့ရှိပြီး အင်တာနက်ကနေ မလိုအပ်တဲ့ Traffic တွေကို ဖယ်ထုတ်ပြီး ကြိုတင်သတ်မှတ်ထားရှိတဲ့ Traffic များကိုဘဲ Internal Networking ထဲသို့ ဝင်ခွင့်ပေးတာပါ.. တစ်ခါတစ်ခါကျတော့ ဒီ Hardware Firewall များဟာ Software Firewall များနဲ့အတူတွဲပြီးလုပ်ရတာတွေလည်းရှိပါတယ်.. ဒီလိုသုံးရင် .. ပိုပြီး လုံခြုံသလို.. လုပ်ဆောင်ချက်များကိုလည်း ပိုမိုမြင့်တင်ပေးနိုင်ပါတယ်..

OSI နှင့် TCP/IP Networking Models အကြောင်း
Firewall Types အကြောင်းတွေကို မပြောခင် ကြားဖြတ်ပြီး ပြောပြချင်သေးတာက OSI 7 layer နှင့် TCP/IP Network Models အကြောင်း တို့ပါဘဲ.. OSI ဟာ အလွှာ(၇) ခုနဲ့ ဖွဲ့စည်းထားပြီးတော့ တစ်လွှာချင်းစီမှာ သက်ဆိုင်ရာ တာဝန်ကိုယ်စီ ရှိကြပါတယ်..ကြုံလို့ OSI 7 Layer




အကြောင်းအနည်းငယ်ပြောရရင်..

http://en.wikipedia.org/wiki/Osi_7_layer_model"]OSI ဆိုတာဟာဘာလဲ။[/URL]
အရှည်ပြောရရင်တော့ Open System Interconnection လို့ခေါ်ပါတယ်။ သူဟာ Network တွေ တစ်ခုနဲ့တစ်ခု အပြန်အလှန် ချိတ်ဆက်ကြရာမှာ အခက်အခဲမရှိ လွယ်ကူချောမွေ့ စေဖို့အတွက် International Organization for Standardization (ISO) အဖွဲ့ ကြီးက သတ်မှတ်ထားတဲ့ စံတစ်ခုဖြစ်ပါတယ်။
ကမ္ဘာပေါ်မှာ ကွန်ပျူတာ ထုတ်လုပ်ရောင်းချတဲ့ ကုမ္ပဏီကြီးတွေ အများကြီးရှိပါတယ်။ အဲဒီလိုပဲ ကွန်ပျူတာတွေ တစ်လုံးနဲ့
တစ်လုံးချိတ်ဆက်တဲ့အခါမှာသုံးတဲ့ Networking Devices တွေကို ထုတ်လုပ်တဲ့ ကုမ္ပဏီတွေလည်း အများကြီးရှိပါတယ်။ အဲဒီလိုမျိုး နည်းပညာပိုင်းဆိုင်ရာ မတူညီကြတဲ့ အမျိုးအစားအမျိုးမျိုးသော ကွန်ပျူတာတွေ၊ Networking Devices တွေကို အသုံးပြုထားကြတဲ့ Network တွေအသီးသီးဟာ တစ်ခုနဲ့တစ်ခု လွယ်လင့်တကူ အပြန်အလှန် ချိတ်ဆက်မိချင်တယ်ဆိုရင် သူတို့အားလုံးကြားထဲမှာ ပုံသေစံနှုန်း(ဘုံတူညီချက်များ) ရှိဖို့တော့လိုအပ်နေပါတယ်။ ဒါမှသာ အဲဒီ Network တွေဟာ အတူတကွ ချောမွေ့စွာ ချိတ်ဆက် အလုပ်လုပ်နိုင်ကြမှာဖြစ်ပါတယ်။ဒါကြောင့် ISO အဖွဲ့ကြီးဟာ အဲဒီလိုအပ်ချက်ကို ပြေလည်စေဖို့အတွက် OSI Layers (7)ခုကို ၁၉၇၄ ခုနှစ်လောက်ကတည်းက စတင်ဖော်ထုတ်ခဲ့တာပဲဖြစ်ပါတယ်။
အခုအချိန်မှာတော့ OSI(7) Layers စံနှုန်းများနဲ့ တိုက်ဆိုင်ကိုက်ညီမှုမရှိဘဲ ကွဲပြားနေတဲ့ Networking နဲ့ပတ်သက် ဆက်နွယ်နေသော Device ရယ်လို့ ဈေးကွက်ထဲမှာ မရှိတော့တဲ့အထိ တစ်ကမ္ဘာလုံးက OSI Layers (7) ခုကို အသိအမှတ်ပြုလက်ခံ နေကြပါပြီ။ ဘာဖြစ်လို့လဲဆိုတော့ လူသားတွေဟာ ယနေ့ခေတ်မှာ ဆက်သွယ်ရေးစနစ်ရဲ့အရေးကြီးပုံနဲ့အသုံးဝင်ပုံ တွေကိုပိုမိုခံစား

သိရှိလာကြတာနဲ့အမျှ ကောင်းမွန်မြန်ဆန်တဲ့ ဆက်သွယ်ရေးစနစ်တွေကို အသုံးပြုခွင့်ရဖို့ လိုအပ်လာပါတယ်။ ဒီတော့ ကွန်ပျူတာ ကွန်ယက်တွေကြားမှာ နည်းပညာ Platform မတူသည်ဖြစ်စေ၊ အမျိုးအစားတံဆိပ်မတူသည်ဖြစ်စေ အတူတကွ ချိတ်ဆက်လုပ်ဆောင်နိုင်ကြဖို့ဆိုတာ ဟာလည်း အမှန်တကယ်အရေးကြီးတဲ့လိုအပ်ချက် တစ်ခု ဖြစ်ပါတယ်။ ဒါမှသာ ကျယ်ပြန့်ကြီးမားတဲ့ ကွန်ပျူတာကွန်ယက်တွေ စီမံဖန်တီးချိတ်ဆက်နိုင်မှာပါ။ Networking ကိုစိတ်ဝင်စားတယ်ဆိုတဲ့ လူတစ်ယောက်အနေနဲ့ ဒီ OSI Layers (၇) ခုဟာ ဘာတွေလဲဆိုတာလောက်တော့အနည်းဆုံး သိထားမယ်လို့ထင်ပါတယ်။

(၇) Application Layer
(၆) Presentation Layer
(၅) Session Layer
(၄) Transport Layer
(၃) Network Layer
(၂) Data Link Layer နဲ့
(၁) Physical Layer တို့ပဲဖြစ်ပါတယ်။ (အောက်ကနေ အပေါ်ကို ရေတွက်ပါတယ်)

Layer လုပ်ဆောင်ချက်
Physical Layer Transfer Medium ပေါ်မှာ Data သွားလာနိုင်ဖို့ ကူညီပေးပါတယ်။ Data တွေကို Transfer Medium နဲ့လိုက်လျောညီထွေရှိမယ့် Signal ပုံစံအဖြစ်ပြောင်းလဲပေးပါတယ်။ အဲဒီ Data Signal တွေကို Transmission လုပ်နိုင်ဖို့ရောပြန်ပြီး Synchronization လုပ်နိုင်ဖို့ရော လိုအပ်တဲ့ Voltage Levels ကိုဆုံးဖြတ်ပေးပါတယ်။

Data Link Layer Network လမ်းကြောင်းတစ်လျှောက်မှာအဆင်ပြေပြေသွားနိုင်မယ့် Frame လေးတွေဖြစ်လာအောင် Data ကိုတည်ဆောက်ပေးပါ တယ်။ Network Connection တစ်လျှောက်မှာ Collision မဖြစ်အောင်စောင့်ကြပ်ထိန်းသိမ်းပေးပါတယ်။ Collision ဖြစ်သွားရင် ဒါမှမဟုတ် Error Control Information နဲ့မတိုက်ဆိုင်ပဲ Error တွေ့နေရတယ်ဆိုရင် အဲဒီFrame ကိုချက်ချင်းထပ်ပို့ပေးပါတယ်။

Network Layer မတူညီတဲ့ Network တွေကြားမှာ Connection ရအောင် ၊ Data Transfer လုပ်နိုင်အောင် ကြားခံဆက်သွယ်ပေးပါတယ်။ Network လမ်းကြောင်းတွေကိုလည်းရှာဖွေပေးပြီး Data Transfer လုပ်ရာမှာပိုမိုမြန်ဆန်အောင်ကူညီပေးပါတယ်။

Transport Layer Data Transfer လုပ်ရာမှာအစမှအဆုံးတိုင် Data Packet

တစ်ခုချင်းစီအတိုင်းအတာအထိ စိတ်ချရတဲ့ Data Transmission တစ်ခု ဖြစ်အောင်လုပ်ဆောင်ပေးပါတယ်။ Error Control နဲ့ Flow Control ကို ဆောင်ရွက်ပါတယ်။ အကယ်၍ Data Packet တစ်ခုမှာများနဂို Packet အတိုင်းမဟုတ်ကြောင်းတွေ့ရှိပါကချက်ချင်းထပ်ပို့ပေးပါတယ်။

Session Layer Data Transfer လုပ်ဖို့အတွက် Sender နဲ့ Receiver ကြားမှာ Logical Connection တစ်ခုကို အစပြုတည်ဆောက်ပါတယ်။ အဲဒီ Connection ကို Data Transmission မပြီးမချင်းထိန်းသိမ်းထားပါတယ်။ Data တွေကိုလည်းအဲဒီ Connection ပေါ်မှာ အဆင်ပြေ ပြေသွားနိုင်မယ့်အပိုင်းလေးတွေအဖြစ်ပိုင်းပါတယ်။ လက်ခံမယ့်ဘက်ရောက်တဲ့အခါမှာနဂိုမူရင်း Original Data ပြန်ရအောင် ပြန် လည်စုစည်းပါတယ်။

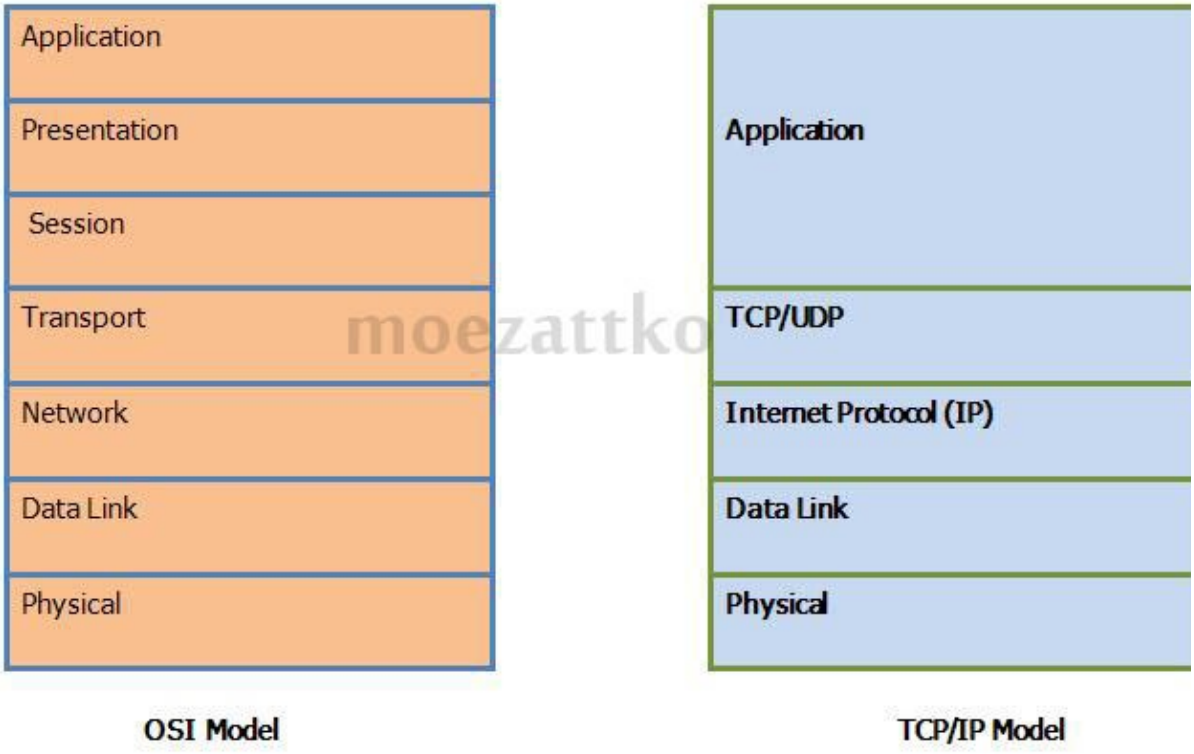
Presentation Layer Data တွေကိုအောက်ပိုင်း Layer တွေကနားလည်အဆင်ပြေမယ့် Format ပုံစံမျိုးပြောင်းလဲပေးပါတယ်။ လိုအပ်တဲ့ Encryption တွေနဲ့ Compression တွေကိုလည်းလုပ်ဆောင်ပေးပါတယ်။ လက်ခံမယ့်ဘက်မှာကျတော့ Decompression တွေနဲ့ Decryption တွေကိုလိုအပ်သလို လုပ်ဆောင်ပါတယ်။ User နားလည်လက်ခံနိုင်မယ့် Format မျိုးပြန်ရအောင် Data ကိုပြန်ပြီး Format ပြောင်း ပေးပါတယ်။

Application Layer User တွေပို့ချင်တဲ့ သတင်းအချက်အလက်တွေ၊ Data တွေကို အောက်ပိုင်း Layer တွေက နားလည်လက်ခံပြီးဆက်လက် Process လုပ်နိုင်ဖို့အတွက် Interface တစ်ခုအဖြစ်ကြားခံပြီး User တွေကို ပိုမို လွယ်ကူအဆင်ပြေစေပါတယ်။ လက်ခံမယ့်ဘက်မှာလည်း User တွေအနေနဲ့လက်ခံရရှိလာတဲ့ Data တွေကို အသုံးချချင်သလိုအသုံးချနိုင်ခွင့် ရရှိအောင် Interface တစ်ခုအနေနဲ့ Userတွေကို ပိုမိုအဆင်ပြေစေရန် လုပ်ဆောင်ပေးပြန်ပါတယ်။

## TCP/IP Network Model

TCP/IP Network Model ကတော့ (၅) လွှာဘဲရှိပါတယ်.. အဲဒီအလွှာတွေကတော့...

Click this bar to view the full image.




Firewall တွေဟာ ကန့်သတ်ချက်အမျိုးမျိုးကို ပြုလုပ်နိုင်ရန်အတွက် သူတို့ဆီမှာ မတူညီတဲ့ အခြေအနေ Criteria တွေကို သတ်မှတ်ရပါတယ် ယင်းမတူညီတဲ့ Criteria တွေဟာလည်း မတူညီတဲ့ (Network Model ) အလွှာတွေကို အသုံးပြုကြပါတယ်.. Firewall တွေဟာ အဲဒီအလွှာတွေ ထဲမှာမှ အနိမ့်ဆုံးအလွှာ အနိမ့်ဆုံး Layer 3 မှာ အလုပ်လုပ်ကြပါတယ်.. Layer 3 ဆိုတာ OSI မှာဆိုရင် Network Layer ဖြစ်ပြီး TCP/IP Model မှာကျတော့ .. Internet Protocol Layer မှာ အလုပ်လုပ်တာဖြစ်ပါတယ်.. ထပ်ပြောရရင် Layer 3 မှာ အလုပ်လုပ်ကြတဲ့ Firewall တွေက Packet

တွေ စစ်ဆေးတဲ့အခါမှာ သိပ်ပြီး စစ်ဆေးခွင့်မရှိဘူး.. နောက်ပြီး ဒီ packet နဲ့ တစ်ခြား Packet နဲ့ဘယ်လိုပတ်သက်မှုရှိသလဲ ဆိုတာကိုလည်း စစ်ဆေးလို့မရဘူး .. ဘာဖြစ်လို့လဲဆိုတော့ Layer 3 mode မှာ အလုပ်လုပ်နေတဲ့ အတွက်ကြောင့်ပါ.. Transport Layer မှာ အလုပ်လုပ်တဲ့ Firewall ကျတော့ packet နဲ့ပတ်သက်ပြီး နည်းနည်းစစ်ဆေးခွင့်ပိုရှိတယ် .. ဒါကြောင့် ပိုမိုရှုတ်ထွေးတဲ့ ခက်ခဲနက်နဲတဲ့ Criteria များဖြင့်စစ်ဆေးပြီး အထဲကို ဝင်ခွင့်ပြုမပြုဆိုတာကို သတ်မှတ်လို့ရတယ်.. Application Layer mode မှာအလုပ်လုပ်တဲ့ Firewall ကျတော့ အရင် layer တွေထက် အာဏာပိုရှိတယ်လို့ပြောရရင်ရပါတယ် .. ဘာဖြစ်လို့လဲဆိုတော့ အဆင့်အဆင့်တက်လာခဲ့ Layer များကိုစစ်ဆေးပြီး ဒီ packet ဟာ ဘယ်ကို သွားမလဲဆိုတာကို မူတည်ပြီး ကိုပေးချင်တဲ့ လုပ်ခွင့်မျိုးကိုဘဲပေးပိုင်ခွင့်ရှိလို့ပါ.. နားလည်အောင်ပြောရမယ်ဆိုရင် Firewall တွေဟာ Networking Model တွေမှာ အပေါ်ပိုင်းအလွှာကို ရောက်ရှိလေလေ packet အကြောင်းကိုပိုသိရှိပြီး ပိုပြီးထိန်းချုပ်နိုင်တယ်..

## Firewall အမျိုးအစားများ

ထပ်ပြီး Firewall အမျိုးအစားများကို ခွဲလိုက်လို့ရှိရင် မတူညီတဲ့ Types ပေါင်း 4 မျိုးရှိပါသေးတယ်.. အဲဒါတွေကတော့

1. Packet Filters
2. Ciruit Filters or Circuit Level Gateways
3. Application Filters or Application Level Gateways နဲ့
4. Stateful Multilayer Inspection Firewall တို့ပါဘဲ..