

પ્રકરણ 3 : માઈક્રોસોફ્ટ આઉટલુક

પ્રસ્તાવના

- 3.1 આઉટલુક (Outlook)
- 3.2 ઇ-મેઇલ ઉમેરવા/કન્ફીગર કરવા (Adding and Configuring E-Mail)
- 3.3 ઇ-મેઇલમાં બીડાણ અને સહી (Attachment and Signature in E-Mail)
- 3.4 આઉટલુકમાં કેલેન્ડર (calendar)
- 3.5 આઉટલુકમાં સરનામાં (Contacts)
- 3.6 કાર્ય અને નોંધ (Task and Note)
- 3.7 વર્ચુઅલ પ્રાઇવેટ નેટવર્ક (Virtual Private Network – VPN)
- 3.8 સામાન્ય સુરક્ષાનો પરિચય (General Security Concepts)
- 3.9 ફાયરવોલ (Firewall)
- 3.10 આધારરૂપ માળખાકીય સુરક્ષા (Infrastructure Security)
- 3.11 નેટવર્ક ટ્રબલશુટિંગ (Network Troubleshooting)
- 3.12 સ્વાધ્યાય

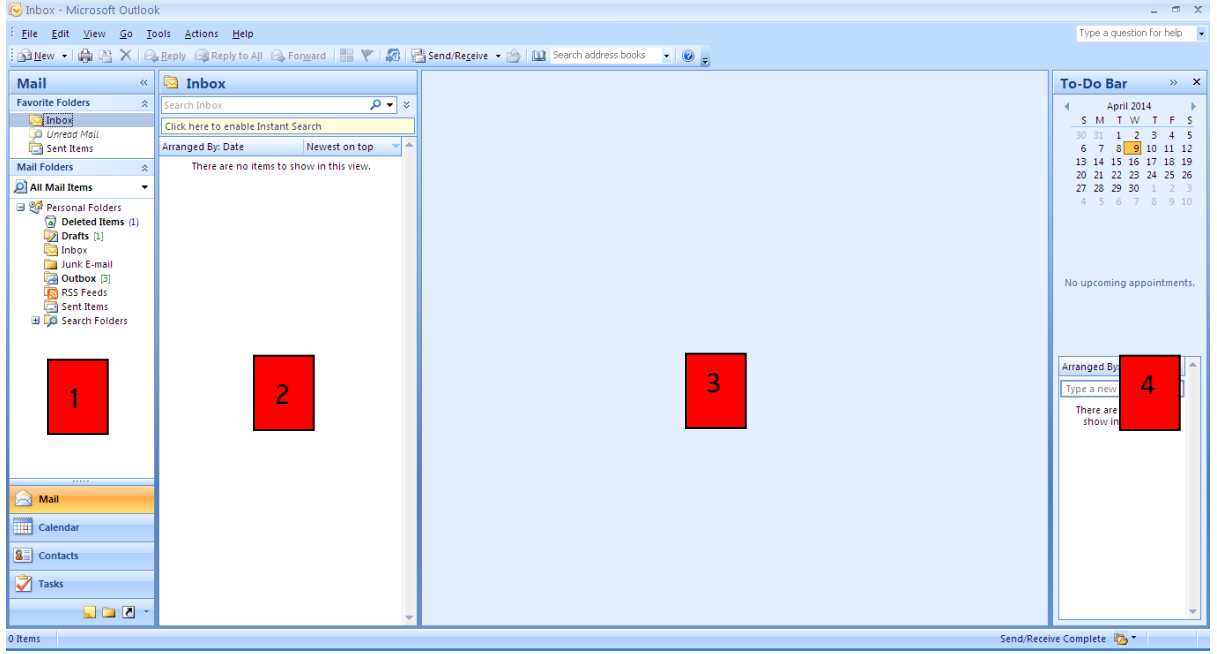
ઉદ્દેશ

- E-mail સેવાઓ તેમજ માઈક્રોસોફ્ટ આઉટલુકનો અભ્યાસ કરવો.

3.1 આઉટલુક (Outlook)

આઉટલુક એ માઈક્રોસોફ્ટ દ્વારા બનાવવામાં આવ્યું છે. જેમાં E-Mail, Calendar, Contact, Address ને Create અને Store કરવા માટેની સુવિધા છે. ઇન્ટરનેટ સાથે જોડી આઉટલુકનો ઇ-મેઇલને આપવા કે લેવા માટે ઉપયોગ કરી શકીએ છીએ. આઉટલુક પ્રોગ્રામનો ફાયદો એ છે કે ઇ-મેઇલને ઇન્ટરનેટ વગર પણ જોઈ શકાય છે. આજે આઉટલુક ઘણી કંપનીમાં વપરાય છે. જેનો ઉપયોગ ખૂબ જ સરળ છે. જે આપણે જોઈએ.

આકૃતિ 2.5માં દર્શાવેલ સ્ક્રીન તમે જ્યારે આઉટલુક ખોલશો તેવું તરત જ જોવા મળશે. એમાં સ્ક્રીન પર ચાર ભાગ પડશે. અને અન્ય ઓફિસ પ્રોગ્રામમાં દર્શાવ્યા મુજબ જ મેનુબારની ગોઠવણી હશે. ભાગ-1માં તમને Mail વિષે માહિતી જોવા મળશે. તેમાં તમે જે કંઈ સિલેક્ટ કરશો તે ભાગ-2માં જોવા મળશે. ભાગ-1માં Inbox છે. તેથી ભાગ-2ની શરૂઆતમાં Inbox લખેલ છે. બીજા દ્વારા મળેલ ઇ-મેઇલ Inboxમાં Save થાય છે. ભાગ-2માં મેઇલ પર ક્લિક કરતાં જ તેનું નાનું Preview ભાગ-3માં બતાવશે. અને ભાગ-4માં Calendar છે જે ભાગ-1માં પણ છે. Calendarનો ઉપયોગ માત્ર તારીખ જોવા જ નહીં પરંતુ, કંઈ તારીખે શું કામ કરવાનું છે તથા કોની સાથે મિટીંગ છે, અગત્યના કામની યાદી વગેરે save કરી શકાય છે.



આકૃતિ 2.5 આઉટલુક એક્સપ્રેસ

3.2 ઇ-મેઇલ ઉમેરવા / કન્ફિગર કરવા (Adding and Configuring E-Mail)

ઈ-મેઇલ એટલે ઇલેક્ટ્રોનિક મેઇલ (ઇલેક્ટ્રોનિક ટપાલ). ઇન્ટરનેટની મદદથી ઈ-મેઇલ દ્વારા ઝડપથી કોઇપણને ટપાલ મોકલી શકાય છે. ઈ-મેઇલ મેળવવા માટે ઈ-મેઇલ એડ્રેસ (ઈ-મેઇલ આઈ.ડી) હોવું જ જોઈએ જે અનન્ય હોય છે. આઉટલુકથી ઈ-મેઇલ મોકલવા કે લેવા માટે તેને configure કરવાની જરૂર પડે છે. Configure માત્ર એક જ વખત કરવાની જરૂર પડે છે. આઉટલુક ને ખોલતા સ્ક્રિન પર Configuring Outlook નામનું ડાયલોગ બોક્સ જોવા મળશે. ત્યારબાદ બીજું આઉટલુક Startup થશે. તેમાં Next પર ક્લિક કરો. ત્યાંથી E-mail Account વિશે પૂછવામાં આવશે. જો તમે Configure કરવા તૈયાર હોય તો (Yes) હા નહીંતર ના (No) પર ક્લિક કરો.



આકૃતિ 2.6 આઉટલુક એક્સપ્રેસ 2010માં ઇ-મેઇલ એડ કરવા (Add an Email Account to MS Outlook 2010)

હવે, આઉટલુકમાં માંગવામાં આવતી માહિતીની વિગત લખો ત્યારબાદ Next પર ક્લિક કરો. અને જો Configure સફળતાપૂર્વક થઇ જશે તો Finish પર ક્લિક કરી શકશો નહીંતર Error બતાવશે.

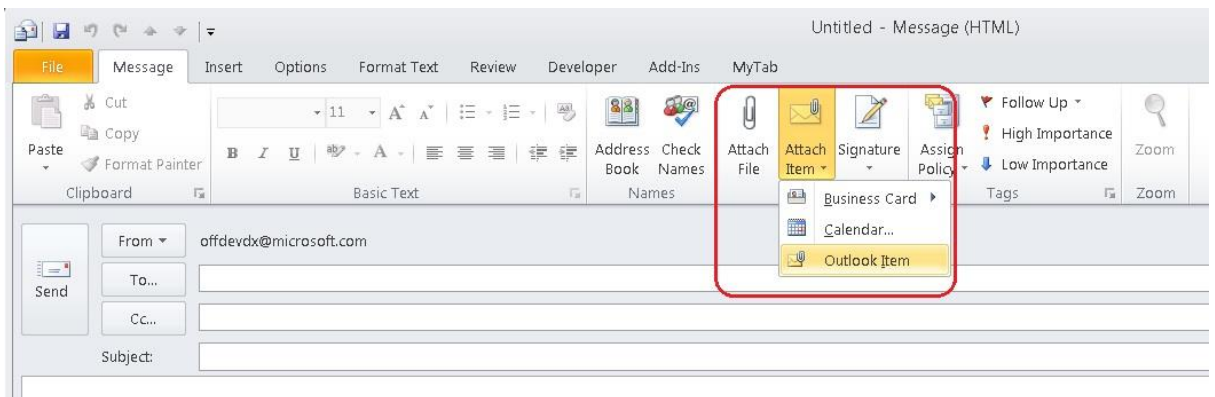
ત્યારબાદ પોતાનું નવું એકાઉન્ટ ખોલવા માટે ડાબી બાજુ સૌથી ઉપર આઉટલુકમાં Sign હશે. તેના પર ક્લિક કરી Profileમાં જવું. તેમાં Info અને Infoમાં Add Account પર ક્લિક કરો. તેમાં તમારી વિગત માગવામાં આવશે તે પ્રમાણેની વિગત ભર્યા બાદ સંમતી પૂછશે જો તમે માટે હા, પાડો તો તમારું એકાઉન્ટ ઉમેરશે.

3.3 ઇ-મેઇલમાં બીડાણ અને સહી (Attachment and Signature in E-Mail)

ઇ-મેઇલમાં કોઇ ફાઇલ કે ડેટાને ઉમેરવા માટે Insert મેનુ પર જઇ Attach પર ક્લિક કરવી અને ફાઇલ સિલેક્ટ કરવી. અને એ ફાઇલ તમારા ઇ-મેઇલમાં Attach થયેલી જોવા મળશે અને પોતાના કોઇપણ વ્યક્તિને તે ફાઇલ મોકલી શકાશે.

હવે, કોઇ વ્યક્તિને કોઇ ફાઇલ કે કોઇપણ વસ્તુ મોકલવા માટે સૌ પ્રથમ Filesમાં જઇ New પર ક્લિક કરો અને ઉપર દર્શાવેલી સ્ક્રિન ખૂલશે. ત્યારબાદ Attach File પર ક્લિક કરી બ્રાઉઝ કરી ફાઇલને ઓપન કરો અને Attach થવા દો, આમ, ફાઇલ, લખાણ કે અન્ય ચીજ વસ્તુઓનું જોડાણ (Attachment) આપણે સરળતાથી કરી શકીએ છીએ તથા મોકલી પણ શકીએ છીએ.

ઇ-મેઇલમાં સહી ઉમેરવા માટે Signature પર ક્લિક કરી જોઈતી માહિતી ભરતા સહી તૈયાર થઈ જશે. જ્યારે કોઈ ઇ-મેઇલ મોકલવામાં આવે છે ત્યારે ઇ-મેઇલના લખાણના અંતમાં સહી ઉમેરાઈ જાય છે.



આકૃતિ 2.7 ઇ-મેઇલમાં એટેચમેન્ટ

તમારી પ્રગતિ ચકાસો

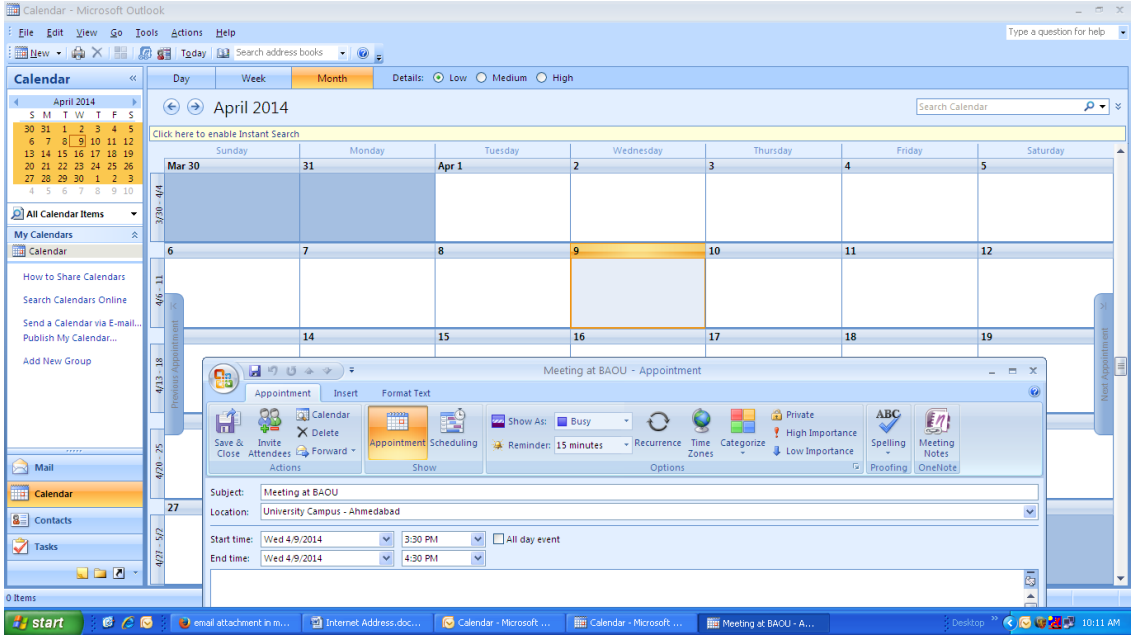
1. તમારા ઈ-મેઇલ આઇડી પ્રમાણેનું આઉટલૂક કન્ફિગર કરો.
2. આઉટલૂક માંથી તમારા મિત્રને ઈ-મેઇલ કરો.
3. આઉટલૂક માંથી તમારા મિત્રને Signature અને Attachment ઉમેરી મેઇલ કરો.

3.4 આઉટલૂકમાં કેલેન્ડર (Calendar)

કેલેન્ડર (Calendar) વિકલ્પ પર ક્લિક કરતા તમને એ મુજબની સ્ક્રિન જોવા મળશે જે ઘરેલું કેલેન્ડર જેવું હશે તેમાં પણ હાલથી ઘણાં વર્ષો આગળ-પાછળ કે કોઈ પણ મહિનો કે તારીખ દર્શાવેલી હોય છે. જેમાં કઈ તારીખ પર આપણે શું કામ કરવાનું છે કે ક્યારે કરવાનું છે? તે અંગેનું સમયપત્રક તૈયાર કરી શકાય છે. આ વસ્તુ ઉમેરવા

- i) New બટન પર ક્લિક કરવાથી નવી Window ખુલશે
- ii) Action મેનુમાં જઈને New Appointment વિકલ્પ પર ક્લિક કરવાથી નવી Window ખુલશે
- iii) જેમાં જગ્યા, સમય, અંતર, કારણ પૂછશે, તે લખવાનું રહેશે.

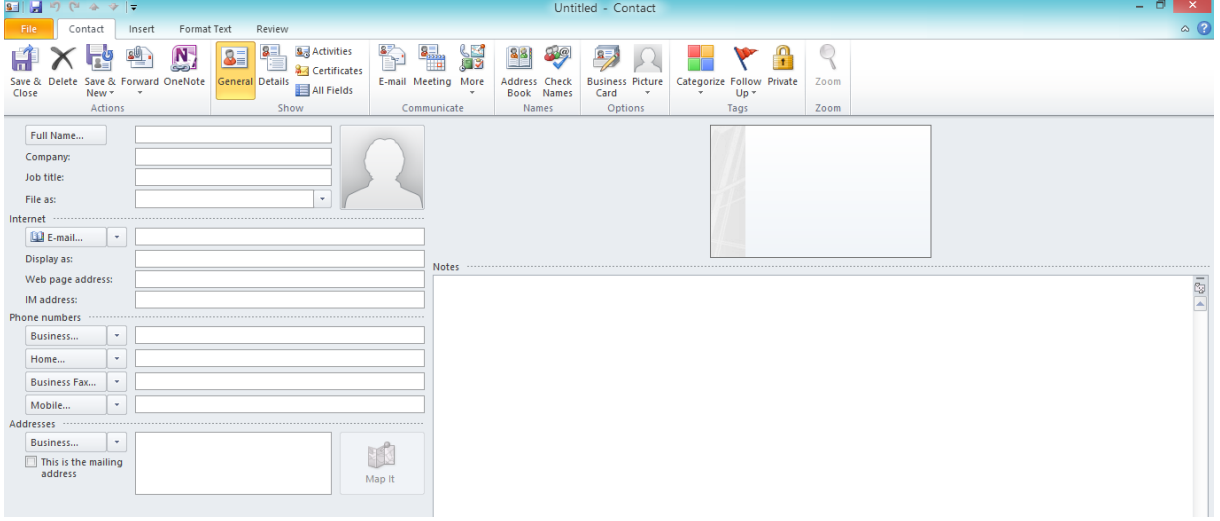
આકૃતિ 2.8માં કેલેન્ડર દર્શાવેલ છે જેમાં દરેક મહિનાની દરેક તારીખ લખેલ છે. અને ખૂબ મોટી જગ્યા છે. તે દરેક તારીખ કે દિવસને વારંવાર યાદ ન કરવા આપણે તેમાં પોતાનું કાર્ય એન્ટર કરી શકીએ છીએ અને રોજબરોજનાં કાર્યની જાણકારી મેળવી શકાય છે.



આકૃતિ 2.8 આઉટલૂકમાં કેલેન્ડર

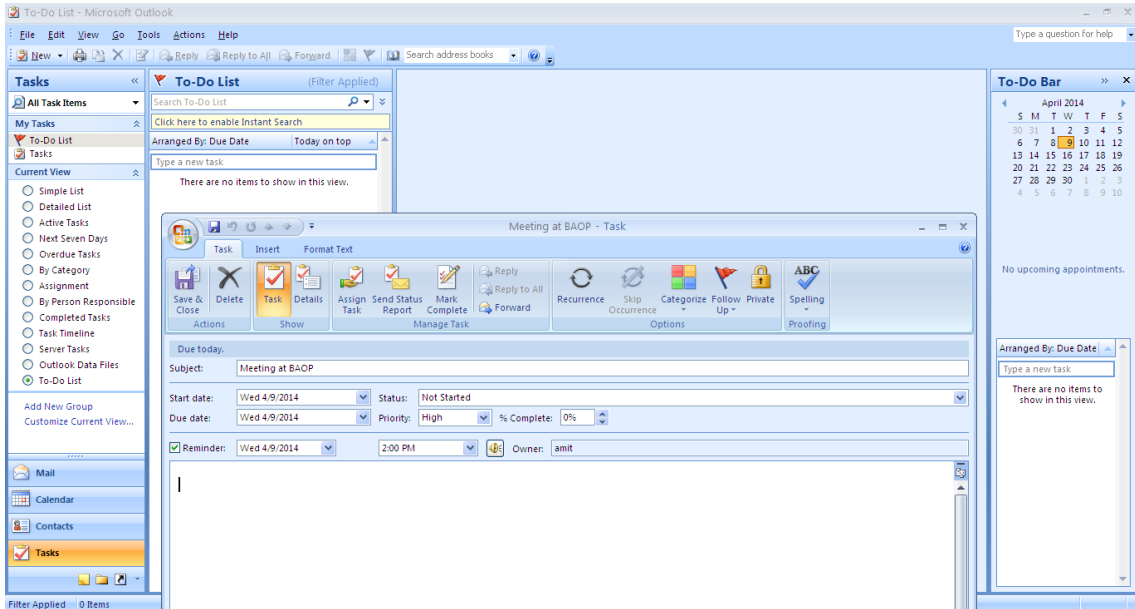
3.5 આઉટલુકમાં સરનામાં (Contacts)

નવો ઇ-મેઇલ લખીને મોકલ્યા બાદ તે ઇ-મેઇલ એડ્રેસ વાળી વ્યક્તિની માહિતી કે નામ સંગ્રહિત કરવાની સુવિધા આઉટલુકમાં છે. Address Cards List મુજબ તેને Current Viewમાં Phone List Select કરતાં Phone Numberની list પ્રમાણે જોવા મળશે. તેમાં મોકલેલ ઇ મેઇલને પસંદ કરી જરૂરી માહિતી ભરવાનું કહેશે. તે માહિતી ભરી Save અને Close કરો.



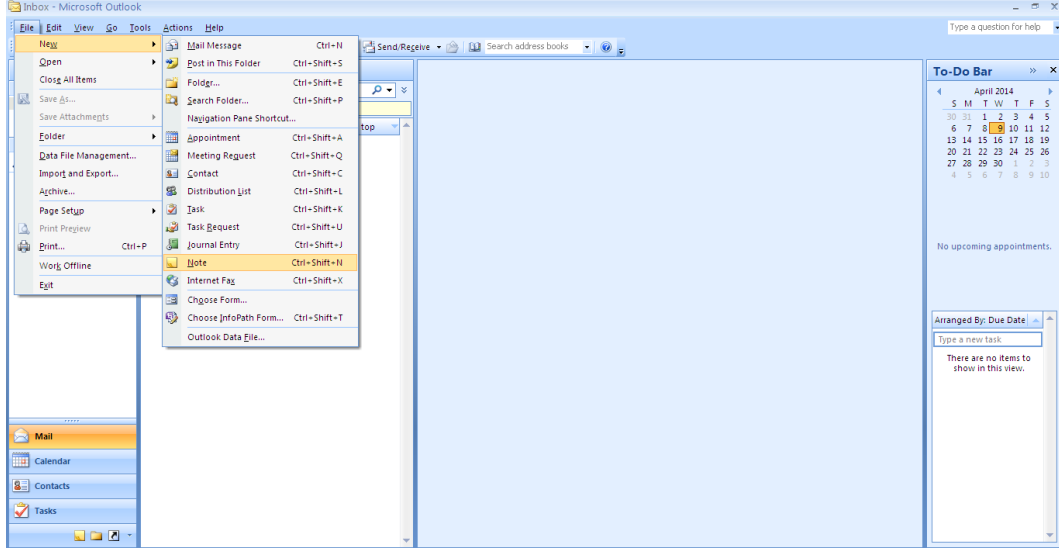
આકૃતિ 2.9 આઉટલુક માં સરનામું ઉમેરવું

3.6 કાર્ય અને નોંધ (Task and Note)



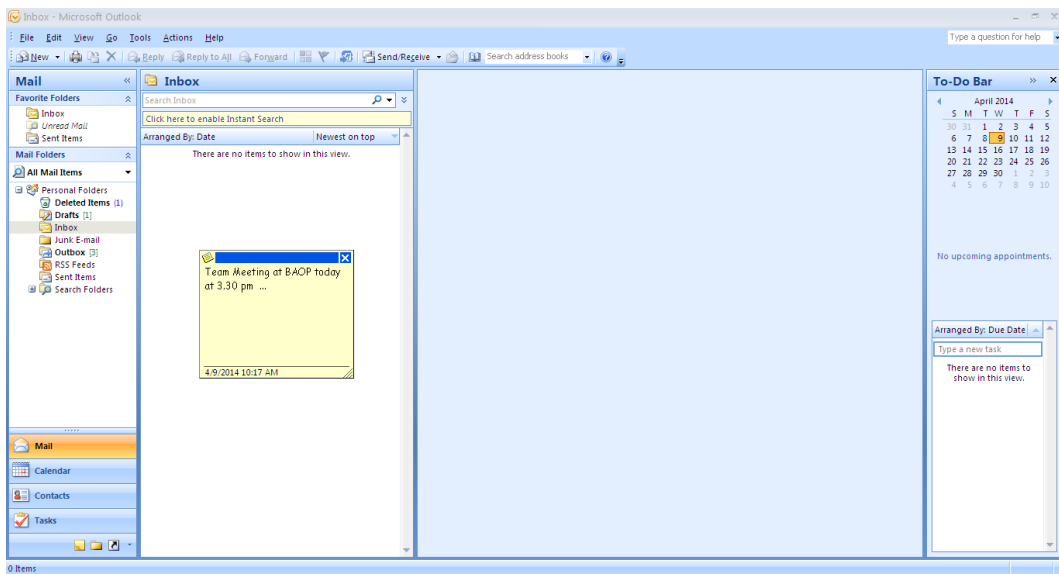
આકૃતિ 2.10 Task in આઉટલુક

Task (કાર્ય) બટન પર ક્લિક કરતા અત્યાર સુધીની બધી યાદી બતાવે છે. દરેક કાર્યની છેલ્લી તારીખ કઇ છે તે પણ દર્શાવે છે. નવું કાર્ય ઉમેરવાં New પર ક્લિક કરતા એક ડાયલોગ બોક્સ જોવા મળશે. કાર્યની વિગત તે ક્યારે શરૂ કરવું અને છેલ્લી તારીખ કઇ છે, તે અંગેની માહિતી ઉમેરી Save and Close પર ક્લિક કરો. જેથી ભરેલ માહિતી તે જ ડાયલોગ બોક્સમાં દેખાશે યાદીમાં ઉમેરાયેલી જોવા મળશે.



આકૃતિ 2.11 આઉટલુક નોટની સુવિધા

આપણે કેલેન્ડરનો ઉપયોગ કરી દરરોજનું કાર્ય જોઇ શકીએ છીએ. પરંતુ ધારો કે આપણાથી એક દિવસ ન જોવાયું તો આખું શિડયુલ વેડફાય જાય છે. તેથી આઉટલુકમાં Task હોય છે. જે આપણને કામ માટે અગાઉથી તથા સામેથી માહિતી જણાવી દે છે અને તે કાર્યને ભૂલી જતા બચાવવામાં મદદ કરે છે.



આકૃતિ 2.12 રીમાઇન્ડર નોટ (Reminder Note)

આઉટલૂકમાં એવી સુવિધા ઉપલબ્ધ છે કે જેથી યુઝર તેમને સમયાંતરે કરવાના કાર્યની વિગતવાર નોંધ “Note” માં કરી શકે છે અને આઉટલૂક દ્વારા તેનું સંચાલન પણ કરી શકાય છે.

તમારી પ્રગતિ ચકાસો

1. આઉટલૂકમાં તમારા માટે હાલના મહિનાનું શિડ્યુલ બનાવો.
2. આઉટલૂકમાં તમારા મમ્મી પપ્પાના જન્મદિન માટે રીમાઈન્ડર નોટ બનાવો.
3. આઉટલૂકમાં તમારા મિત્રોની માહિતી Contacts માં ઉમેરો.

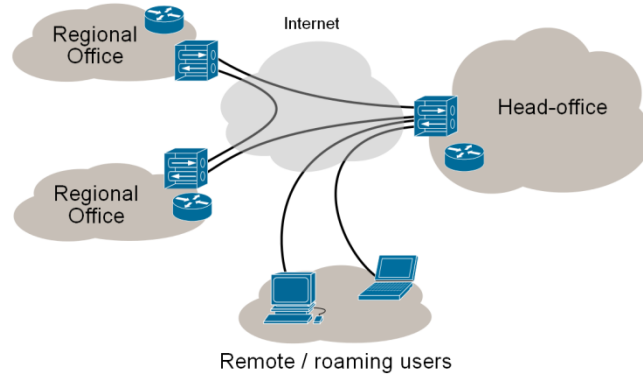
3.7 વર્ચ્યુઅલ પ્રાઇવેટ નેટવર્ક (Virtual Private Network – VPN)

VPN આપણે ઉદાહરણથી સમજવાનો પ્રયત્ન કરીશું. ધારો કે કોઈ કંપનીની બે શાખાઓ છે જેમાંથી એક શાખા જામનગરમાં આવેલી છે જ્યારે બીજી શાખા મુંબઈમાં છે. આપણે આ બન્ને શાખા વચ્ચે એક નેટવર્ક પ્રસ્થાપિત કરવું છે. આ નેટવર્કને આપણે Private network તરીકે ઓળખીશું કારણકે તે ફક્ત કંપની પૂરતું સિમિત રહેશે. આ પ્રકારના જોડાણ માટે ત્રણ વિકલ્પ છે.

- (i) બન્ને શાખાનું વાયર દ્વારા જોડાણ કરવું
- (ii) બન્ને શાખાનું ઉપગ્રહ વડે જોડાણ કરવું
- (iii) બન્ને શાખાનું ઈન્ટરનેટના માધ્યમથી જોડાણ કરવું

ઉપર જણાવેલ વિકલ્પોમાંથી (i) અને (ii) ખૂબજ ખર્ચાળ વિકલ્પ છે તેમજ અમુક સંજોગોમાં અશક્ય પણ હોય છે જ્યારે વિકલ્પ (iii) અત્યંત વ્યાજબી તેમજ સરળ ઉપાય છે.

VPNમાં કોઈપણ સંસ્થાના અલગ-અલગ નેટવર્કનું જોડાણ ઈન્ટરનેટના માધ્યમ દ્વારા કરવામાં આવતું હોય છે. તે એક Private Network હોવાથી સંસ્થા સિવાય અન્ય વ્યક્તિ તેનો ઉપયોગ કરી શકશે નહિ. VPNમાં કોઈપણ સંસ્થાની અલગ-અલગ શાખા વચ્ચે ડેટાનું પ્રત્યાયન ઈન્ટરનેટના માધ્યમ દ્વારા થતું હોય છે. VPN માટે ડેટાની સુરક્ષા સૌથી વધુ જરૂરી બને છે, કારણકે સંસ્થાનો ખાનગી ડેટા ઈન્ટરનેટ દ્વારા વહન થતો હોય છે. VPN માં ડેટાની સુરક્ષા માટે IPsec જેવી ટેકનોલોજીનો ઉપયોગ થતો હોય છે. IPsecથી ડેટા Encrypt (વાંચી ન શકાય તેવું) થઈને Internet પર મોકલવામાં આવે છે જેથી તે ડેટામાં કંઈ માહિતીનો સમાવેશ છે તે જાણી શકાતું નથી. ડેટા destination networkમાં પહોંચ્યા બાદ Decrypt (મૂળ સ્વરૂપમાં ફેરવવું) કરવામાં આવે છે. VPN પ્રસ્થાપિત કરવા સંસ્થા દ્વારા ખાસ પ્રકારના VPN Routerનો ઉપયોગ થતો હોય છે.



આકૃતિ 2.13 વર્ચ્યુઅલ પ્રાઇવેટ નેટવર્ક (Virtual Private Network - VPN)

VPN ના પ્રકાર: VPN મુખ્યત્વે ત્રણ સંજોગોમાં વાપરવામાં આવે છે જેથી VPNના ત્રણ પ્રકાર હોય છે. ચાલો આપણે આ દરેક પ્રકારનો સંક્ષિપ્તમાં પરિચય મેળવીએ.

- વર્ચ્યુઅલ પ્રાઇવેટ ડાયલ-અપ નેટવર્ક (Virtual Private Dial-up Network - VPDN): જ્યારે સંસ્થાના કોઇ કર્મચારી બહારગામથી સંસ્થાનું નેટવર્ક ઉપયોગ કરવા માગે ત્યારે તે VPDN કહેવાય. જે-તે કર્મચારી પોતાના કમ્પ્યુટરને Internet સાથે જોડીને સંસ્થાના નેટવર્કમાં લોગીન કરી શકે છે. આ માટે કર્મચારીના કમ્પ્યુટરમાં VPN ક્લાયન્ટ સોફ્ટવેર ઇન્સ્ટોલ થયેલું હોવું જોઈએ.
- ઈન્ટરનેટ આધારિત (Intranet based VPN): જ્યારે કોઇપણ સંસ્થાની બે કે તેથી વધુ શાખાઓ વચ્ચે VPN પ્રસ્થાપિત કરવામાં આવે ત્યારે તેને Site-to-Site VPN કહેવાય છે. તેમાં સંસ્થાની એક LANને અન્ય શાખાની LAN સાથે Internetના માધ્યમ વડે જોડાય છે.
- ઈન્ટરનેટ આધારિત (Extranet based VPN): જ્યારે અલગ-અલગ સંસ્થાઓના LANનું જોડાણ ઈન્ટરનેટના માધ્યમ દ્વારા કરવામાં આવે ત્યારે તેને Extranet based VPN કહેવાય છે. ઉદાહરણ તરીકે કોઇપણ કંપનીના ગ્રાહકના (Customers) નેટવર્ક અને માલ મોકલનારના (Suppliers) નેટવર્કનું જોડાણ કરવું.

3.8 સામાન્ય સુરક્ષાનો પરિચય (General Security Concepts)

દરેક કમ્પ્યુટર માહિતીનો ભંડાર હોય છે કે જેમાં વ્યક્તિગત અથવા કોઇપણ સંસ્થાની પુષ્કળ માહિતીનો સંગ્રહ થઇ શકે છે. આમાંથી મોટાભાગની માહિતી ખાનગી હોય છે કે જેને સામાન્ય લોકોથી અથવા અન્ય લોકોથી સુરક્ષિત રાખવી જરૂરી બને છે. સુરક્ષા માટેના ઘણા આયામો છે જેમ કે

- કમ્પ્યુટરની સુરક્ષા
- નેટવર્કની સુરક્ષા-ખાનગી નેટવર્કને બહારના લોકોથી સુરક્ષિત કરવું
- પ્રત્યાયન થતા ડેટાની સુરક્ષા
- અન્ય સર્વર પર રહેલા ડેટાની સુરક્ષા

ઉપર દર્શાવેલ આયામો માટે અલગ-અલગ પ્રકારની સુરક્ષા વ્યવસ્થાનો ઉપયોગ થતો હોય છે જેમકે Username અને Password દ્વારા થતી પ્રમાણીકરણ વ્યવસ્થા અથવા Encryption અને Decryption દ્વારા સુરક્ષિત રીતે ડેટાનું પ્રત્યાયન વિગેરે. હવે આપણે આ દરેક આયામને વિગતવાર રીતે જોઈશું:



આકૃતિ 2.14 સામાન્ય સુરક્ષાનો પરિચય (General Security Concepts)

પાસવર્ડની ઉપયોગિતા: આપણે જ્યારે પણ Gmail કે Yahoo mailનો ઉપયોગ કરતા હોઈએ છીએ ત્યારે Username અને Password એક અગત્યની ભૂમિકા ભજવે છે. તેના દ્વારા કમ્પ્યુટર, જે-તે વ્યક્તિનું પ્રમાણીકરણ (Authentication) કરે છે. આથી કોઈપણ એક વ્યક્તિના ઈ-મેઈલ અન્ય કોઈ વ્યક્તિ જોઈ ન શકે. સંજોગો પ્રમાણે Username અને Password અલગ-અલગ હોય શકે છે. ઉદાહરણ તરીકે આપણા ઘરના કમ્પ્યુટરને સુરક્ષિત રાખવા માટે જે username અને passwordનો ઉપયોગ કર્યો હોય તે e-mail ના Username અને Passwordથી અલગ હોય શકે છે.

ક્યારેક ફાઈલને સુરક્ષિત રાખવા માટે ફક્ત Passwordની જરૂરિયાત રહે છે. Usernameનો ઉપયોગ કરવામાં આવતો નથી. અમુક સંજોગોમાં Username, Passwordની સાથે મોબાઇલમાં SMS થી આવેલ OTP (One-time password) ની જરૂર પણ રહેતી હોય છે.

આપણા Username અને Password જો અન્ય કોઈ વ્યક્તિને જાણ થઈ જાય તો આપણા ખાનગી ડેટાની અસલામતી રહે છે. મોટાભાગે Username ની જાણ અન્ય કોઈને થઈ શકે પણ Password હમેશા સુરક્ષિત રાખવો જોઈએ. Password એક પ્રકારની ચાવી નું કામ કરે છે કે જેના દ્વારા આપણે કમ્પ્યુટર તેમજ ડેટાને સુરક્ષિત કરી શકીએ છીએ.

નોંધ મોટાભાગની વેબસાઈટમાં કેપ્ચાનો (Captcha) ઉપયોગ થતો હોય છે કે જેમાં આપણે અમુક પ્રકારના અક્ષર ઓળખીને ટાઇપ કરવાના હોય છે. Captcha અને Password બન્ને અલગ બાબત છે. Captcha નો ઉપયોગ માહિતી કોઈ વ્યક્તિ દ્વારા જ દાખલ કરવામાં આવે છે તેની ખાતરી કરવા વપરાય છે.

પાસવર્ડ પસંદ કરવા માટેના સૂચનો

- Password ખૂબ નાનો હોવો જોઈએ નહિ.
- આદર્શ Password 6-20 અક્ષરનો હોવો જોઈએ.
- Passwordમાં અંક (0-9), અક્ષર (a-z) તેમજ ખાસ સંજ્ઞાનો (\$, @, #,) મિશ્ર ઉપયોગ થયેલ હોવો જોઈએ.
- Password કોઈ શબ્દકોશનો (ડિક્શનરી) શબ્દ ન હોવો જોઈએ નહિ.
- મોબાઇલ નંબર, ગાડી નંબર કે જન્મ તારીખનો ઉપયોગ પાસવર્ડમાં કરવો નહિ.

પાસવર્ડના ઉદાહરણ

Username	Password	વિગત
Mahesh	Mahesh	અસલામત
Mahesh	Mahesh123	અસલામત
Mahesh	M123	અસલામત
Mahesh	9879100000	અસલામત
Mahesh	29feb	અસલામત
Mahesh	GJ-6	અસલામત
Mahesh	Vanilla	અસલામત
Mahesh	lw@nt2fly	સલામત
Mahesh	Lx2\$a33pqr	સલામત
Mahesh	TobeOrNotzb	સલામત
Mahesh	Trouble\$hoot!ng	સલામત

પાસવર્ડ બાબતે ધ્યાનમાં રાખવા જેવી બાબત:

- પાસવર્ડ નિયત સમયના અંતરે બદલતા રહેવું.
- શક્ય હોય તો અલગ-અલગ એકાઉન્ટ માટે એકજ પાસવર્ડ વાપરવો નહિ.
- પાસવર્ડને ક્યારેય પણ લખીને સાથે ફેરવવા નહિ.
- પાસવર્ડ કોઈને કહેવા નહિ.

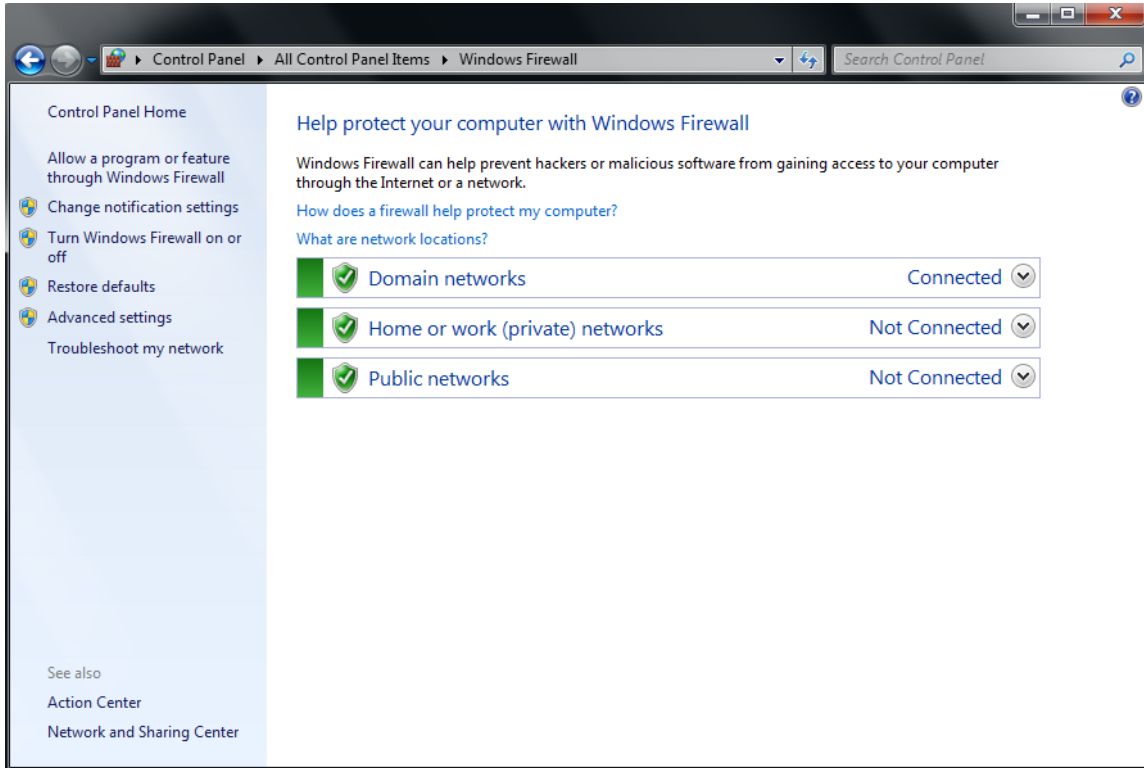
3.9 ફાયરવોલ (Firewall)

Network Firewall દ્વારા આપણે કમ્પ્યુટરના ડેટાને સુરક્ષિત રાખી શકીએ છીએ છે. ફાયરવોલ આપણા કમ્પ્યુટરને કિલ્લા જેવી સુરક્ષા પ્રદાન કરે છે જેથી કમ્પ્યુટરમાંથી network પર જતી માહિતી તેમજ networkમાંથી કમ્પ્યુટરમાં આવતી માહિતી સુરક્ષિત રહે જે રીતે “Great Wall of China” ચીનની સુરક્ષા કરે છે તેવીજ રીતે ફાયરવોલ આપણા કમ્પ્યુટરને તેમજ networkને સુરક્ષિત રાખવામાં મદદગાર છે.

મૂળભૂત ફાયરવોલ Configurations: એડમિનિસ્ટ્રેટર લોગીન દ્વારા આપણે ફાયરવોલને સક્રિય (on) અથવા નિષ્ક્રિય (off) કરી શકીએ છીએ. મુખ્ય બે રીતે ફાયરવોલ કન્ફિગર (Configure) કરી શકાય:

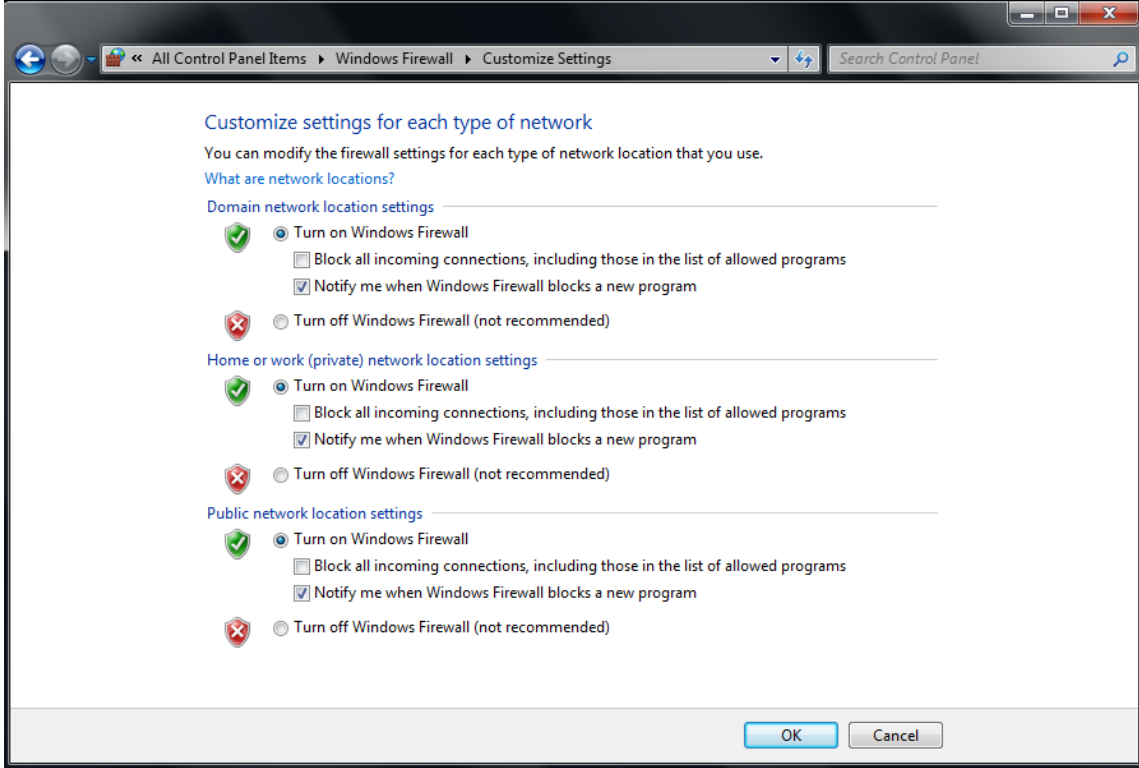
- Start બટન → Control Panel → Windows Firewall Icon ક્લિક કરવાથી
- Left Pane પર ક્લિક કરવાથી તેમજ “Turn Windows Firewall On or Off”

Computer Network દ્વારા આપણા કમ્પ્યુટરમાં જ્યારે બહારથી ડેટા આવે ત્યારે ઇનબાઉન્ડ કનેક્શન (Inbound Connection) કહેવાય અને જ્યારે આપણા કમ્પ્યુટરમાંથી ડેટા બહારના નેટવર્ક પર જાય ત્યારે આઉટબાઉન્ડ કનેક્શન (Outbound Connection) કહેવામાં આવે છે.



આકૃતિ 2.15 ફાયરવોલ ના basic Configurations

ફાયરવોલ Configuration દરમ્યાન આપણે કયા પ્રકારના ડેટાને કમ્પ્યુટરમાં આવવા દેવા છે તેમજ કયા પ્રકારના ડેટાને બહાર જવા દેવા છે તે જાણવું જરૂરી બને છે. જેમકે Http દ્વારા આવતા ડેટાને પરવાનગી આપવી તેમજ Https દ્વારા આવતા ડેટાને પરવાનગી આપવી પરંતુ Ftp દ્વારા આવતા ડેટાને પરવાનગી ન આપવી. આ પ્રકારની દરેક નેટવર્ક સર્વિસ (Network Service) માટે ફાયરવોલ Configuration વડે નિયમો (Rules) બનાવી શકાય છે.

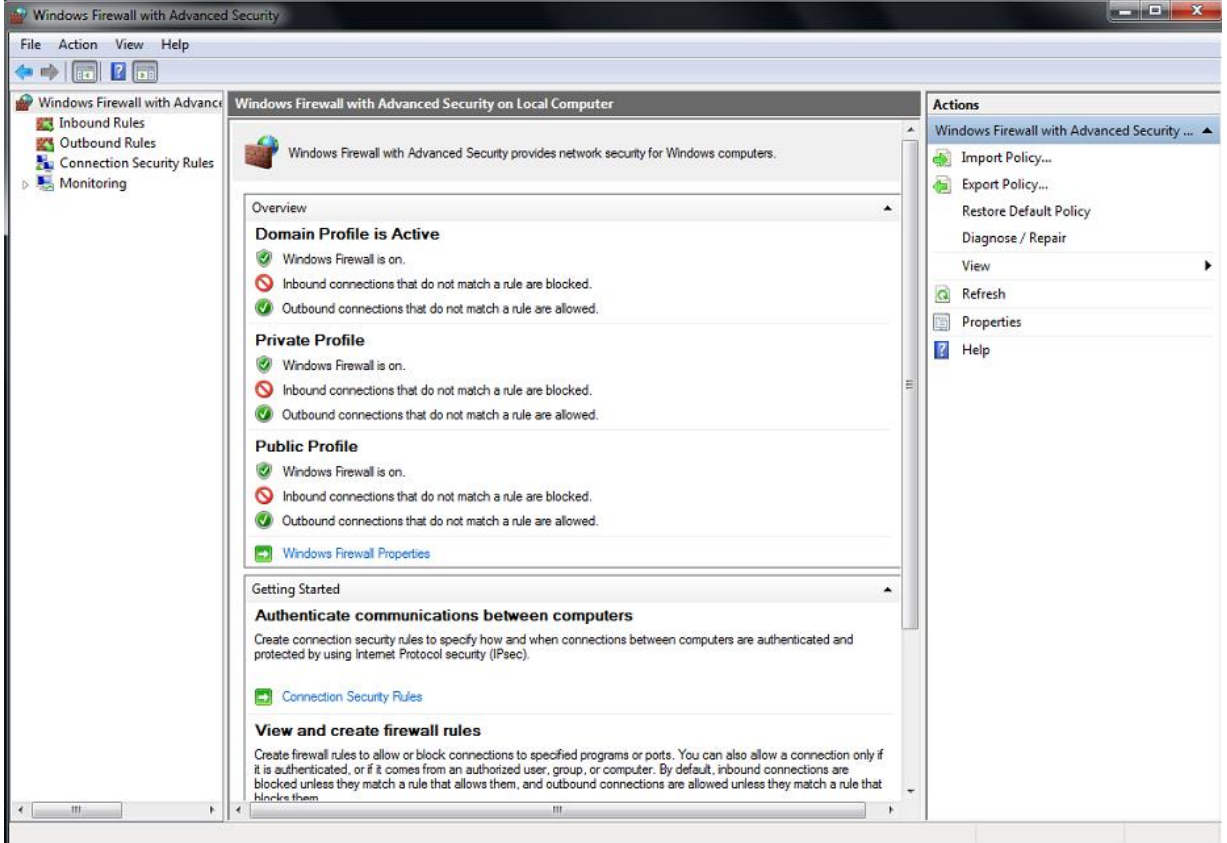


આકૃતિ 2.16 ફાયરવોલના વિસ્તૃત Configurations

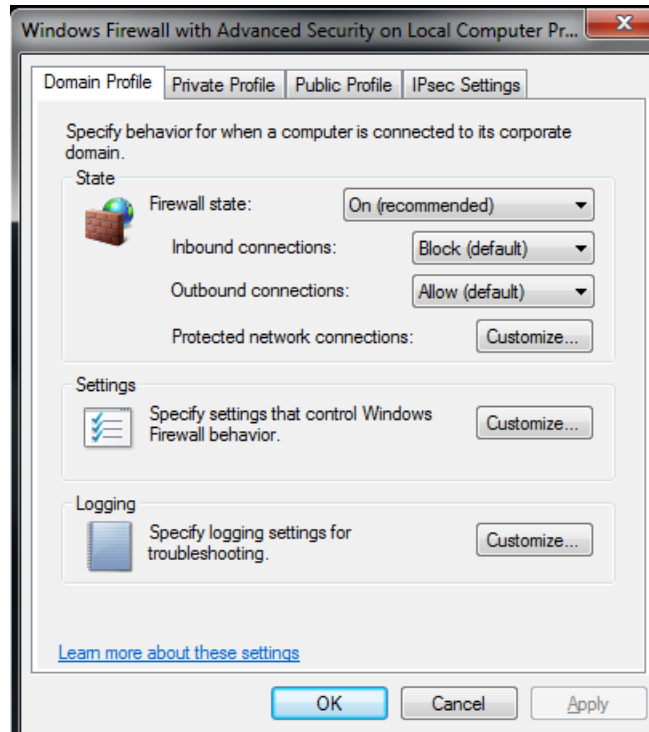
Firewall Configurationની Advanced Settings: માં જઈને વિવિધ પ્રકારના Inbound Rules તેમજ Outbound Rules બનાવી તેને કન્ફિગર (Configure) કરી શકાય છે.

જો કમ્પ્યુટર નેટવર્કમાં અનેક કમ્પ્યુટર હોય અને દરેક કમ્પ્યુટર પર સમાન નિયમો લાગુ કરવા હોય તો પ્રથમ કમ્પ્યુટર પર Rules બનાવી તેને અન્ય કમ્પ્યુટર પર કોપી કરી શકાય છે આ માટે Firewallની Advanced Settingsમાંથી Import Policy અથવા Export Policyનો ઉપયોગ કરી શકાય છે. (આકૃતિ 2.17)

ફાયરવોલ દ્વારા ફક્ત ઇનબાઉન્ડ કનેક્શન અથવા ફક્ત આઉટબાઉન્ડ કનેક્શન ને પરવાનગી પણ આપી શકાય છે. ફાયરવોલ દ્વારા Log ફાઈલ પણ બનાવી શકાય છે જેથી કરીને કોઈપણ પ્રકારની અનિચ્છનીય ઘટનાને Log ફાઈલમાં નોંધ (Record) કરી શકાય. જ્યારે પણ આપણા બનાવેલ નિયમોનું ઉલ્લંઘન કરવાના પ્રયત્નો થાય ત્યારે તેની વિગત log ફાઈલમાં સંગ્રહ થઈ શકે છે. (આકૃતિ 2.18)



આકૃતિ 2.17 ફાયરવોલ ના એડવાન્સ Configurations



આકૃતિ 2.18 ફાયરવોલ inbound/outbound તેમજ log file ની configuration દર્શાવતી dialog box

તમારી પ્રગતિ ચકાસો

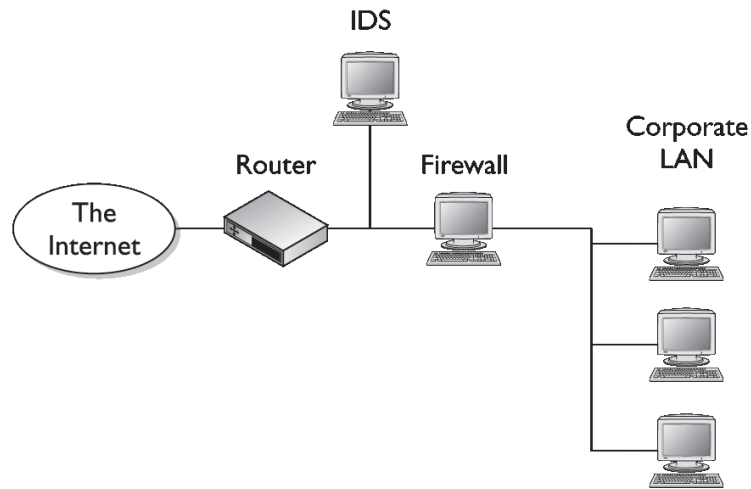
1. તમારા કમ્પ્યુટરમાં ફાયરવોલ સક્રિય છે કે નહિ તે ચેક કરો. જો ફાયરવોલ નિષ્ક્રિય (off) હોય તો તેને સક્રિય (On) કરો.

3.10 આધારરૂપ- માળખાકીય સુરક્ષા (Infrastructure Security)

આજકાલ મોટાભાગની સંસ્થાઓ પાસે પોતાના કમ્પ્યુટર નેટવર્ક પ્રસ્થાપિત થયેલ હોય છે. તેમની કમ્પ્યુટર વ્યવસ્થા તથા બધા ઉપકરણોને એક માળખા તરીકે જોવામાં આવે છે. કોઈપણ માળખા માટેની સુરક્ષા વ્યવસ્થાને આપણે બે ભાગમાં વહેંચી શકીએ :

- (a) ભૌતિક સુરક્ષા (Physical Security)
- (b) ડેટાની સુરક્ષા (Logical Security)

ભૌતિક સુરક્ષા (Physical Security): સંસ્થાના કમ્પ્યુટર તેમજ અન્ય ઉપકરણોને કુદરતી આપત્તિઓ જેવી કે ધરતીકંપ, વાવાઝોડું, વરસાદ વિગેરેથી સુરક્ષિત રાખવા જોઈએ. તેમજ આગથી, રમખાણ દરમ્યાન તેને નુકસાન ન પહોંચે તેની કાળજી લેવી જોઈએ. આ ઉપરાંત સંસ્થામાં કર્મચારી દ્વારા ઉપકરણોને હાનિ ન પહોંચે કે તેની ચોરી ન થઈ જાય તે તકેદારી પણ રાખવી પડતી હોય છે. ભૌતિક સુરક્ષાનો અન્ય આયામ તે પણ છે કે કોઈ પદ્ધતિવાળા તેમના મેનેજરનાં કમ્પ્યુટર કે પ્રિન્ટર તેમની જાણ બહાર ન વાપરે.



આકૃતિ 2.19 આધારરૂપ માળખાકીય સુરક્ષા

ડેટાની સુરક્ષા (Logical Security): જેમ કમ્પ્યુટર હાર્ડવેરને સુરક્ષિત રાખવા જોઈ તેવીજ રીતે ડેટા અને માહિતીની સુરક્ષા વ્યવસ્થા જરૂરી બને છે. સંસ્થાના ખાનગી ડેટા બહારના લોકોને મળે તેમજ ડેટાને વાયરસથી નુકસાન ન

પહોંચે તેની કાળજી રાખવી જરૂરી બને છે. ડેટાની સુરક્ષા હેતુ વિવિધ પ્રકારના સંશોધનો થઈ રહ્યા છે. જેથી કરીને ડેટા સલામત તેમજ સુરક્ષિત રહે તે માટે પ્રમાણીકરણ (Authentication) અને અધિકૃતિકરણ (Authorization) જેવી પદ્ધતિ ઉપયોગમાં લેવાય છે. આ પદ્ધતિઓનો આધાર સંકેતલિપિ (Cryptography) જેવી તકનીકો પર હોય છે.

Authentication: આ પ્રક્રિયા વપરાશકર્તા ની ઓળખની ખાતરી કરે છે જેથી તે ક્યાં સાધન વપરાશ કરી શકે છે તે નક્કી થઈ શકે છે. પ્રમાણીકરણ અસરકારક સુરક્ષા માટે જરૂરી છે.

Authorization: આ પ્રક્રિયા વપરાશકર્તાની ઓળખ દ્વારા તેને વિવિધ સ્ત્રોતો (Resource) વાપરવા માટે પરવાનગી આપે છે અથવા મનાઈ ફરમાવે છે.

Cryptography: સંકેતલિપિ એ માહિતીની સુરક્ષા માટે લખાણને વાંચી ન શકાય તેવી રીતે રૂપાંતરિત (એનક્રિપ્ટ) કરે છે. જેને માત્ર એક ગુપ્ત કી દ્વારા સાદા લખાણમાં (અથવા ડિક્રિપ્ટ) ફેરવી શકાય છે. આધુનિક સંકેતલિપિ યુક્તિઓ સુરક્ષિત હોવા છતાં એનક્રિપ્ટ થયેલ સંદેશાઓ ક્યારેક સંકેતલિપિ વિશ્લેષણ દ્વારા તોડી શકાય છે.

કામગીરીની વ્યવસ્થાની સુરક્ષા (Operations Security): કોઈપણ સંસ્થાની દૈનિક કામગીરી સુરક્ષિત રીત અને વિક્ષેપ રહિત ચાલ્યા કરે તે માટે જે-તે સંસ્થાએ નીચે મુજબના મુદ્દાઓ ધ્યાન પર લેવા જરૂરી છે:

- (1) કમ્પ્યુટર તેમજ તેના ઉપયોગો માટે નીતિ (Policy) તૈયાર કરવી. તથા તેનો અમલ થાય તેવી તકેદારી રાખવી.
- (2) ડેટાના ઉપયોગ કોણે કેવી રીતે કરવા તેવા ધોરણો (Standard) નક્કી કરવા તેમજ નીતિના અમલીકરણ માટેના ધોરણો તૈયાર કરવા
- (3) દરેક કાર્ય માટે, વિવિધ સુચનાઓ ક્રમશઃ તૈયાર હોવી જોઈએ અને તેની પ્રક્રિયાઓ (Procedures) સારી રીતે વ્યાખ્યાતિ હોવી જોઈએ.
- (4) નીતિ વિષયક માર્ગદર્શિકા (guidelines) તૈયાર હોવી જોઈએ.

સંસ્થાકીય સુરક્ષા (Organizational Security): પ્રતિદિન સુરક્ષા વ્યવસ્થાને વધુ ને વધુ મજબૂત કરવાની જરૂરિયાત ઉભી થતી રહે છે. કોઈપણ સંસ્થાના કમ્પ્યુટર નેટવર્કને અનેક પ્રકારના હાર્ડવેર તેમજ સોફ્ટવેર દ્વારા સુરક્ષિત રાખી શકાય છે. સુરક્ષા માટે ઉપયોગમાં લેવામાં આવતા મુખ્ય સોફ્ટવેર નીચે મુજબ છે.

(a) ફાયરવોલ (Firewall)

(b) Intrusion Detection System (IDS): જે અનાધિકૃત વ્યક્તિ કે પ્રોગ્રામને કમ્પ્યુટર નેટવર્કમાં પ્રવેશ થતા ઓળખી જાય છે.

(c) Intrusion Prevention System (IPS): જે અનાધિકૃત વ્યક્તિ કે પ્રોગ્રામને કમ્પ્યુટર નેટવર્કમાં પ્રવેશ થતા અટકાવે છે.

(d) એન્ટીવાયરસ અને એન્ટી માલવેર (Anti-Virus અને Anti-Malware)

સંસ્થામાં હાર્ડવેર આધારિત સુરક્ષા માટે બાયોમેટ્રિક (Biometric) ઉપકરણોનો મોટા ભાગે ઉપયોગ થતો જોવા મળે છે, તે ઉપરાંત Smart Card, RFID વિગેરે જેવી તકનીકો પણ ઉપયોગમાં લેવાય છે.

સંચાર સુરક્ષા **Communication Security**: જ્યારે ડેટાનું પ્રત્યાયન થઈ રહ્યું હોય ત્યારે પણ વિવિધ સુરક્ષા પદ્ધતિઓ ધ્યાનમાં લેવી જોઈએ જ્યારે ડેટાનું પ્રત્યાયન થઈ રહ્યું હોય ત્યારે નીચે મુજબની સુરક્ષા વ્યવસ્થા હોવી જોઈએ.

- (1) ડેટા ખાનગી રહે અને અન્ય કોઈ વ્યક્તિ તે જોઈ શકે નહિ. (**Confidentiality**)
- (2) ડેટા બદલાઈ ન જાય (**Integrity**)

પ્રત્યાયન થયેલા ડેટા નીચે મુજબના માપદંડ સંતોષે તેની ખાસ કાળજી રાખવી જોઈએ.

- (1) ડેટા હંમેશા ઉપબલ્ધ હોવા જોઈએ (**Availability**)
- (2) ડેટા હંમેશા ભૂલરહિત હોવા જોઈએ (**Accuracy**)
- (3) ઉપયોગમાં લેવાયેલ ડેટા પ્રમાણિત સ્ત્રોત પાસેથી મેળવેલ હોવા જોઈએ (**Authentication**)

નોંધ:- **https** પ્રોટોકોલ **http** પ્રોટોકોલની જગ્યાએ વધુ સુરક્ષા પ્રદાન કરે છે.

3.11 નેટવર્ક ટ્રબલશૂટિંગ (Network Troubleshooting)

નેટવર્ક ટ્રબલશૂટિંગ માટે સામાન્ય રીતે ઉદ્ભવતી સમસ્યા અને તેનું નિરાકરણ નીચે આપેલ છે.

પ્રશ્ન: **Cable Unplugged** નો મેસેજ આવે છે.....

ઉત્તર: મુખ્ય બે કારણથી **Cable Unplugged**નો મેસેજ આવી શકે

- (a) નેટવર્ક કાર્ડ સાથે જોડાયેલ કેબલનું કનેક્શન બરાબર ન હોય તો અથવા કેબલ ક્ષતિગ્રસ્ત થયેલ હોય તો. આ માટે આપણે કેબલ કાઢીને ફરીથી જોડી જોવો
- (b) હબ અથવા સ્વીચ ઉપકરણ બંધ હોય તો પણ આ પ્રકારનો મેસેજ આવી શકે છે.

પ્રશ્ન: કમ્પ્યુટર નેટવર્કમાં પ્રસ્થાપિત થતું ન હોય તો.....

ઉત્તર: કમ્પ્યુટરમાં IP address આપેલ ન હોય અથવા **DHCP Server** બંધ હોય તો આપણું કમ્પ્યુટર કેબલ જોડેલું હોવા છતાં નેટવર્કમાં કાર્ય કરશે નહિ. આ માટે:

- (a) યોગ્ય IP Address અને Subnet Mask Configure કરવા જરૂરી છે.
- (b) જો આપની સંસ્થામાં **DHCP Server**નો ઉપયોગ થતા હોય તો “Obtain an IP address Automatically” પસંદ કરો.

પ્રશ્ન:- કમ્પ્યુટર નેટવર્કમાં પ્રસ્થાપિત થયેલ છે પણ ઈન્ટરનેટ સેવાઓ બંધ છે.

ઉત્તર:- ઈન્ટરનેટ બંધ હોવાના અનેક કારણો હોય શકે. નીચે મુજબના કારણો તપાસના તેમજ તેનું નિરાકરણ લાવવા પ્રયત્ન કરવા

- (a) IP Address આપેલ છે પણ Gateway અથવા DNS Server Configure કરેલ નથી.
- (b) ફાયરવોલ માંથી ઈન્ટરનેટ સેવાઓ બંધ કરી હોય

- (c) વાયરસ અથવા માલવેર કમ્પ્યુટરમાં આવેલ હોય
- (d) જો આપ મોડેમ અથવા USB Dongleનો ઉપયોગ કરતા હોય, તો તેમના Configuration તપાસવા
- (e) ISP ની સેવાઓ સ્થગિત થયેલ હોય (Internet Account Expire) થઈ ગયું હોય.

3.12 સ્વાધ્યાય





Q1. યોગ્ય વિકલ્પ વડે ખાલીજગ્યા પુરો (Fill in the blanks)

- 1 _____ એ સર્ચ એન્જીન નથી. (બિંગ, આઉટલુક, ગુગલ)
- 2 આઉટલુક _____ દ્વારા પુરું પાડવામાં આવે છે. (ગુગલ, એપલ, માઇક્રોસોફ્ટ)
- 3 ઇન્ટરનેટનું જોડાણ _____ દ્વારા સ્થાપિત થઈ શકતું નથી. (વાઈ-ફાઈ, હોટસ્પોટ, હબ)
- 4 ઇન્ટરનેટ _____ દ્વારા એક્સેસ થઈ શકતું નથી. (પીડીએ, મોબાઈલ, સ્ટેન્ડઅલોન કમ્પ્યુટર)
- 5 ઇન્ટરનેટ પર ચાલતા સોફ્ટવેર _____ એપ્લિકેશન તરીકે ઓળખાય છે. (ડેસ્કટોપ, વેબ, મોબાઇલ)

Q2. નીચેના વિધાનો ખરાં છે કે ખોટાં તે જણાવો (True or false)

- 1 બધા મોબાઇલમાં ઇન્ટરનેટ કનેક્શન હોય છે.
- 2 જુના ઇ-મેઇલ આઉટલુકમાં ઇન્ટરનેટ કનેક્શન વગર પણ જોઈ શકાય છે.
- 3 નેટસ્કેપ એ બ્રાઉઝર છે.
- 4 કોઈપણ ધંધાકીય એપ્લિકેશન પર ઇન્ટરનેટ ફરજિયાત ચાલવું જોઈએ.
- 5 આઇ.પી. એડ્રેસની લંબાઈમાં ૧૨ આંકડા હોવા ફરજિયાત છે.

Q3. યોગ્ય જોડકા જોડો (Match the pair)

- | A | B |
|---------------------------------------------------------------------------------------|--------------------------------------------|
| 1  | a. ફાયરફોક્સ મોજિલા (Firefox Mozilla) |
| 2  | b. ઇન્ટરનેટ એક્સપ્લોરર (Internet explorer) |
| 3  | c. સફારી (Safari) |
| 4  | d. ક્રોમ (chrome) |

જવાબો

- Q1. 1. આઉટલુક 2. માઇક્રોસોફ્ટ 3. હબ 4. સ્ટેન્ડઅલોન કમ્પ્યુટર 5. વેબ એપ્લિકેશન
 Q2. 1. ખોટું 2. ખરું 3. ખરું 4. ખોટું 5. ખરું
 Q3. 1-b, 2-a, 3-d, 4-c.