1. Noțiuni teoretice (Firewall)

Un firewall este o aplicaţie sau un echipament hardware care monitorizează şi filtrează permanent transmiterea fluxurilor de date realizate între Calculatorul personal sau reţeaua locală şi Internet, în scopul implementării unei "politici" de filtrare.

Această politică poate însemna:

- ✓ protejarea resurselor reţelei de restul utilizatorilor din alte reţele similare
- ✓ Protejarea resurselor impotriva posibililor "musafiri" nepoftiţi, atacurile lor asupra calculatorului sau reţelei local
- ✓ Controlul resurselor pe care le vor accesa utilizatorii locali.

Un firewall, lucrează îndeaproape cu un program de routare, examinează fiecare pachet de date din reţea (fie cea locală sau cea exterioară) ce va trece prin serverul gateway pentru a determina dacă va fi trimis mai departe spre destinaţie. Un firewall include de asemenea sau lucrează împreună cu un server proxy care face cereri de pachete în numele staţiilor de lucru ale utilizatorilor. În cele mai întâlnite cazuri aceste programe de protecţie sunt instalate pe calculatoare ce îndeplinesc numai această funcţie şi sunt instalate în faţa routerelor.

Firewall-urile se împart în două mari categorii:

- prima este reprezentată de soluţiile profesionale hardware sau software dedicate protecţiei întregului trafic dintre reţeaua unei întreprinderi (instituţii şi internet)
- cea de a doua categorie este reprezentată de firewall-urile personale dedicate monitorizării traficului pe calculatorul personal. (Zone Alarm Free, Outpost Firewall Pro, Norton Personal Firewall)

Utilizând o aplicaţie din ce-a de a doua categorie veţi putea preîntâmpina atacurile colegilor “lipsiţi de fair-play” care încearcă să acceseze prin mijloace mai mult sau mai puţin ortodoxe resurse de pe PC-ul dumneavoastră. În situaţia în care dispuneţi pe calculatorul de acasă de o conexiune la Internet, un firewall personal vă va oferi un plus de siguranţă transmisiilor de date. Cum astăzi majoritatea utilizatorilor tind să schimbe clasica conexiune ISDN, xDSL cu modalităţi de conectare mai eficiente (cablu, FTTx, Wi-Fi sau telefon mobil), pericolul unor atacuri reuşite asupra sistemului dumneavoastră creşte. Astfel, mărirea lărgimii de bandă a conexiunii la Internet facilitează posibilitatea de "strecurare" a intruşilor nedoriţi.

Astfel, un firewall este folosit pentru două scopuri:

- pentru a păstra în afara reţelei utilizatorii rău intenţionati (viruşi, viermi cybernetici, hackeri, crackeri)
- pentru a păstra utilizatorii locali (angajaţii, clienţii) în reţea.

Politica Firewall-ului:

Înainte de a construi un firewall trebuie hotărâtă politica sa, pentru a şti care va fi funcţia sa şi în ce fel se va implementa această funcţie. Politica firewall-ului se poate alege urmând câţiva paşi simpli:

1. alege ce servicii va deservi firewall-ul
2. desemnează grupuri de utilizatori care vor fi protejaţi
3. defineşte ce fel de protecţie are nevoie fiecare grup de utilizatori
4. pentru serviciul fiecărui grup descrie cum acesta va fi protejat
5. scrie o declaraţie prin care oricare alte forme de access sunt o ilegalitate

Politica va deveni tot mai complicată cu timpul, dar deocamdată este bine să fie simplă şi la obiect.

Firewallurile pot fi clasificate după:

- Layerul (stratul<=>nivel) din stiva de reţea la care operează
- Modul de implementare

În funcţie de layerul din stiva TCP/IP (sau OSI) la care operează, firewall-urile pot fi:

- Layer 2 (MAC) şi 3 (datagram): packet filtering.
- Layer 4 (transport): tot packet filtering, dar se poate diferenţia între protocoalele de transport şi există opţiunea de "stateful firewall", în care sistemul ştie în orice moment care sunt principalele caracteristici ale următorului pachet aşteptat, evitând astfel o întreagă clasă de atacuri
- Layer 5 (application): application level firewall (există mai multe denumiri). În general se comportă ca un server proxy pentru diferite protocoale, analizând şi luând decizii pe baza cunoştinţelor despre aplicaţii şi a conţinutului conexiunilor. De exemplu, un server SMTP cu antivirus poate fi considerat application firewall pentru email.

Deşi nu este o distincţie prea corectă, firewallurile se pot împărţi în două mari categorii, în funcţie de modul de implementare:

- dedicate, în care dispozitivul care rulează software-ul de filtrare este dedicat acestei operaţiuni şi este practic "inserat" în reţea (de obicei chiar după router). Are avantajul unei securităţi sporite.
- combinate cu alte facilităţi de networking. De exemplu, routerul poate servi şi pe post de firewall, iar în cazul reţelelor mici acelaşi calculator poate juca în acelaţi timp rolul de firewall, router, file/print server, etc.

Posibilitatile unui Firewall

- ✓ să monitorizeze căile de pătrundere în reţeaua privată, permiţând în felul acesta o mai bună monitorizare a traficului şi deci o mai uşoară detectare a încercărilor de infiltrare.

- ✓ să blocheze la un moment dat traficul în şi dinspre Internet
- ✓ să selecteze accesul în spaţiul privat pe baza informaţiilor conţinute în pachete
- ✓ să permită sau interzică accesul la reţeaua publică, de pe anumite staţii specificate
- ✓ să şi nu în cele din urmă, poate izola spaţiul privat de cel public şi realiza interfaţa între cele două.

Un Firewall nu poate:

- ✓ interzice importul/exportul de informaţii dăunătoare vehiculate ca urmare a acţiunii răutăcioase a unor utilizatori aparţinând spaţiului privat (căsuţa poştală şi ataşamentele)
- ✓ interzice scurgerea de informaţii de pe alte căi care ocolesc firewall-ul (acces prin dial-up ce nu trece prin router)
- ✓ apăra reţeaua privată de utilizatorii ce folosesc sisteme fizice mobile de introducere a datelor în reţea (USB Stick, dischetă, CD, etc.)
- ✓ preveni manifestarea erorilor de proiectare ale aplicaţiilor ce realizează diverse servicii, precum şi punctele slabe ce decurg din exploatarea acestor greşeli.

Outpost Pro Firewall.

Instalarea si configurarea unui astfel de program pe sisteme Windows este relativ usoară.

Continuăm cu *Next* până cand instalarea va incepe in directorul de instalare default: C:\Program Files\Agnitum\Outpost Firewall Pro

Instalare, accesam **Simple Mode,** in timpul asta softul verifica calculatorul de anterioarele instala sau daca exista versiuni mai vechi pe PC, si reinoieste baza de date. Pasul urmator programul ne cere restartarea calculatorului!!!

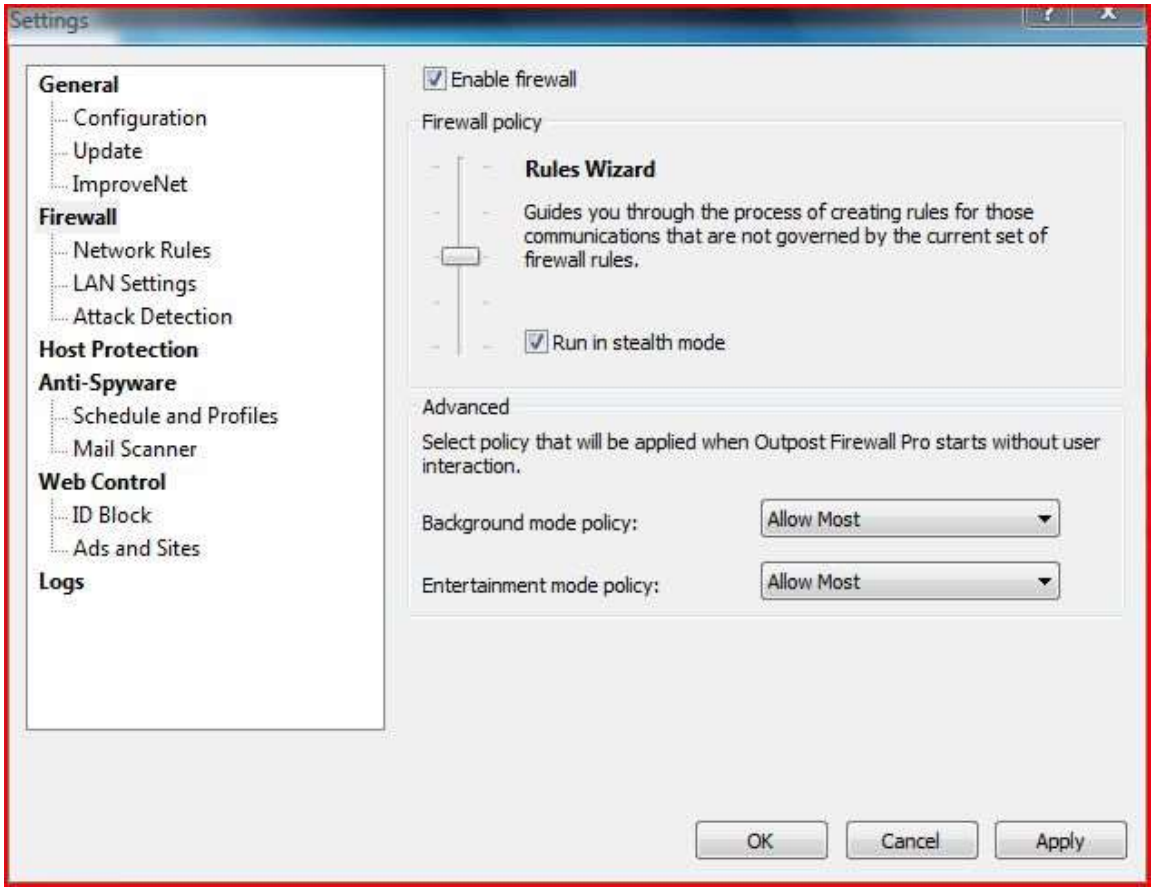
Configurare. Dupa finalizarea instalării programul vă va oferi o ferestra de configurare a

Firewall – ului prin 2 metode.

a) Modul *Normal*: este recomandat majorității utilizatorilor întrucât nu cere cunostințe foarte avansate de configurare.
b) Modul *Advanced*:

Dupa restartarea sistemuui n-i se va cere o cheie de inregistrare. Introducem cheia de inregistrare a produsului sau faceti ca in cazul meu apasati doar "**continue**" deoarece testez o varianta trial.

Odată ce produsul a fost inregistrat, deschidem "Settings" si vedem cu ce optiuni de configurare avansată avem.



In partea stangă observăm sub modul firewall 3 module de reţea pe care firewall – ul, prin reguli specifice le controlează astfel:

Firewall policy (general vorbind reprezintă o regulă de comportare a firewall-ului cu privire la diferite componente externe care interacţioneaza cu internetul)

- ✓ Block All (blochează toate conexiunile atât inbound cat si outbound)
- ✓ Block Most (blochează toate conexiunile atât inbound cat si outbound cu excepţia celor care sunt configurate manual de către utilizator sau automat printr-o asa numita "white list" de către program)
- ✓ Rules Wizard (atunci când aceasta opţiune este activa firewall-ul este în asa numita stare de "learning mode" ceea ce inseamna ca orice program care nu este filtrat automat de către el şi va cere "sa comunice" cu internetul, de regulă o mica fereastră va apărea şi va "intreba" utilizatorul daca, componenta respectivă se poate sau nu conecta la internet.
- ✓ Allow Most (permite toate comunicaţiile care nu sunt explicit blocate)
- ✓ Disable (dezactivează firewall – ul permițând tuturor conexiunilor sa aiba loc)

De asemenea observăm o opţiune: "Run in stealth mode" (rulează în modul invizibil)

Această opţiune este bifită în mod automat (calculatorul nu va răspunde la asa numitele "port scans" acest lucru facându-l invizibil persoanelor rău intenționate) .

Network rules (reguli de rețea) – în dreptul acestui tab în dreapta avem afișate o serie de programe si servicii windows (cu extensia .exe) care sunt încadrate sub 3 subcategorii:

- ✓ Blocked (process sau programe blocate)– aici vom gasi de regula executabilele unor programe pe care le-am adaugat explicit la aceasta subcategorie sau pe care firewall-ul le-a blocat din motive de securitate.
- ✓ Custom access (Reguli stabilite în mod manual de către utilizator) – de regulă în această subcategorie intră toate modulele programelor adăugate şi configurate manual de către utilizator prin intermediul Modulului Rules Wizard (Learning Mode).
- ✓ Trusted (Sigure) – procese adaugate manual ale caror module de conectare sunt implicit permise.

Eventual o serie de procese si programe care aparţin sistemului de operare sunt de asemenea încadrate la aceasta ultimă subcategorie.

LAN Settings (Setări privind Rețeaua locală) – acest tab va arăta în modul urmator:

(evident cu excepţia ip-ului care este unic si diferit de ceea ce se vede mai jos)

Opțiunile NetBIOS, Trusted si NAT Zone ne permit sa asignăm retelei tipul din care face parte.Daca nu esti sigur din ce categorie face parte o rețeaua ta e bine sa sa fie lasat asa cum este.

Atack Detection (Detectia unui atack) – prezinta 3 nivele

I. Maximal (Protectie maximă) – este raportat fiecare scanare a retelei; sunt detectate toate atacurile externe retelei Ethernet.

II. Optimal (Protectie optimă) – raportează un atac daca mai multe porturi sunt scanate sau daca un anumit port este scanat de mai mult ori si care este stiut ca este folosit cel mai des în atacuri. Mai detectează fenomenul de IP flood şi adrese duplicate ale IP-urilor.

III. Custom Settings (Setări Manuale) – mod presetat de firewall daca utilizatorul crează sau modifică orice regulă.

Actiuni atunci cand este detectat un atac:

- ✓ Block intruder IP adress for: x minutes (blochează adresa ip a "atacatorului" timp de un număr (în minute) stabilit de utilizator sau prestabilit de către firewall)
- ✓ Apariţia unor semnale audio sau vizuale cu referire la atac.

Se mai găseşte şi o Listă de Excludere pe baza careia se poate adăuga o anumita adresă IP,domeniu si porturi definite de utilizator care sa fie excluse de filtrare în acest mod permitându-se accesul nerestrictionat la acele resurse.

Host Protection (Protectia gazdei) – Unele aplicatii pot fi identificate ca făcând parte din programe legitime si pot sa-si desfăsoare activitatea din partea acesteia. Spre exemplu unii troieni pot fi injectați într-un computer ca făcând parte dintr-un modul al unei aplicaţii legitime (ex – un navigator) şi în acest mod câștigând privilegiile necesare persoanei care a creat acest troian.

Acest modul încearcă să asigure o cât mai bună protecție împotriva acestor genuri de atacuri.

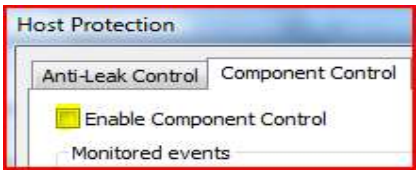
Este structurat pe 3 nivele:

- ✓ Maximum (Protecție maximă) – Controlul de tip Anti – Leak monitorizează toate activitățile sistemului.
  - o toate cererile de accesare a rețelei din partea unor componente noi sau modificate de la ultima accesare sunt monitorizate.
  - o lansarea executabilelor noi sau a celor modificate este monitorizată.
- ✓ Advanced (Protecție avasantă) – vezi toate opţiunile de mai sus
- ✓ Optimal (Protecție optimă) – marea majoritate a aplicaţiilor periculoase sunt monitorizate.
  - o cererile executabilelor care s-au modificat de la ultima verificare, la rețea sunt monitorizate.
- ✓ Low (Protecție scazută) – Controlul Anti-Leak este dezactivat.
  - o cererile executabilelor care s-au modificat de la ultima verificare, la rețea sunt monitorizate.

Toate aceste modificări ale executabilelor și alte operațiuni care se aplica anumitor componente ale diferitelor aplicatii sunt intr-o continua modificare datorită interactiunii unor module ale acestora cu sistemul de operare.

Aceste "schimbări" sunt monitorizate de o asa numita "Component Control" (prezenta la majoritatea firewall-urilor personale) ea fiind resposabilă de detectarea acestor schimbări. Datorită acestor modificări continue a unor programe recomand dezactivarea acestei presetări din simplul motiv de a scapă de o "bombardare" aproape constantă cu mesaje de avertizare.

Apasăm ***Customize…***



Trecem peste prezentarea modului anti-spyware cu mentiunea că daca nu avem cunoștințe minime despre termenul de spyware este bine sa lăsăm active opţiunile "by default".

Modulul "***Mail Scanner***" - (filtrează e-mail-urile primite si trimise au ajutorul unor reguli prestabilite sau stabilite de către utilizator prin intermediul unui filtru de atașamente e – mail).

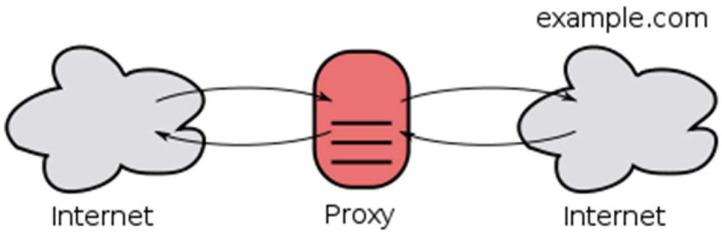
Web Control (Controlul în timpul navigării pe Web) – Ne lasă să creeăm reguli specifice privind accesul la anumite site – uri sau/și mesaje e – mail. Practic filtrul acestui modul blochează conținut activ care este considerat malițios. (scripturi, reclame (ads), elemente active potențial periculoase ș.a)

Logging Level (aici se stochează toate informațiile cu privire la activitățile inregistrate de către modulele programului asupra activitații sistemului)

Astfel aşa numitele log'uri sunt clasificate şi ele funcție de fiecare categorie a programului prezentate mai sus. In acest mod am încercat să prezint în linii mari cum să configurăm "Outpost Firewall" O prezentare foarte complexă a tuturor setărilor şi opţiunilor de configurare poate fi gasită pe site-ul oficial. Ceea ce ferm putem afrima ca aceste solutii in cazul nostru avem prezentata una foarte eficienta si care utilizeaza niste algoritmi foarte bine pregatiti ceea ce ne asigura o securitate maxima si in acelasi timp o filtrare a traficului si solutii pentru "vindecarea" sau neutralizarea anumitor viermi sau atacuri nebinevenite.

2. Noțiuni teoretice (Proxy server)

Un server proxy este un computer care funcționează ca intermediar între un browser Web (cum ar fi Internet Explorer) și Internet. Serverele proxy ajută la îmbunătățirea performanței Web, stocând câte o copie a paginilor Web utilizate frecvent. Atunci când un browser solicită o pagină Web stocată în colecția (cache) serverului proxy, pagina este furnizată de serverul proxy, mai rapid decât deplasarea pe Web. De asemenea, serverele proxy ajută la îmbunătățirea securității, filtrând unele tipuri de conținut Web și software-urile rău intenționate.



Pentru a elimina unele dintre dezavantajele filtrarii de pachete, firewall-ul trebuie sa foloseasca aplicatii software pentru intermedierea accesului la unele servicii: Telnet si FTP. O astfel de aplicatie se numeste serviciu proxy, iar sistemul gazda pe care ruleaza - server proxy.

În timpul unui dialog între un client si un server destinatie, serverul proxy actioneaza ca si server pentru clientul respectiv si devine la randul sau client pentru serverul destinatie. Comunicatia se desfasoara în urmatorii pasi :

1. Clientul trimite cererea catre serverul destinatie, dar ea este interceptata de serverul proxy.
2. Serverul proxy analizeaza cererea si, daca aceasta respecta politica de securitate a organizatiei, este trimisa serverului destinatie.
3. Serverul destinatie raspunde cererii, iar raspunsul se întoarce la serverul proxy.
4. Serverul proxy analizeaza raspunsul si daca acesta respecta politica de securitate a organizatiei, este trimis clientului.
5. Serverul proxy înregistreaza conexiunea într-un fisier jurnal.

Serverul proxy e capabil sa monitorizeze si sa filtreze anumite informatii sau comenzi. El este un server dedicat aplicatiilor care ruleaza pe un calculator care face legatura între reteaua locala si restul retelelor.
Pentru un client, accesul la serverul proxy se poate face numai prin autentificarea acestuia (protectie suplimentara).

Mai jos vor fi enumerate citeva din avantajele si dezamvantaje utilizarii unui server proxy :

Avantaje :

- permit autentificarea utilizatorilor (interni sau externi)
- creeaza fisiere tip log cu activitatea utilizatorilor din retea sau pot monitoriza autentificarile

Dezavantaje: - f. scumpe

- trebuie creat un proxy pentru fiecare serviciu de retea (FTP, TELNET, HTTP..)

Un **server proxy** are două scopuri importante:

- păstrează anonimatul mașinilor client.
- Crește viteza de acces la resurse prin salvarea lor în memoria tampon

Este cunoscut faptul ca atunci cind acceseaza un site**,** adresa IP a PC-ului poate fi vazuta de administratorul site-ulu vizitat. Adresa de IP poate furniza date despre providerul de Internet (ISP), tara de origine, orasul, si uneori chiar adresa utilizatorului. Pentru a ascunde adresa de IP si a naviga in anonimat, este nevoie de folosit web proxy sau ori care alta aplicatie care va ascunde adresa IP .

In cele ce urmeaza ma voi axa pe 2 aplicatii care vor servi drept protectie pentru cei care navigheaza pe internet si totodata vor satisface cele 2 scopuri mentionate mai sus pe care si le propune un proxy server:

1. Prima aplicatie se refera la ascunderea IP atunci cind dorim sa vizitam un site si nu dorim ca sa fie cunoscuta adresa noastra IP.
2. Al doua aplicatie se refera la blocarea site-urilor care poate fi utilizata atit in intr-o retea locala cit la domiciliu.

1. **HideMyIp**

Hidemyip este o aplicatie simpla prin intermediul careia este ascunsa adresa noastra IP, utilizta atunci cind dorim sa vizitam un site insa cu o alta adresa de pe un alt host, din o alta tara, etc. Astfel este una din solutiile de top atunci cand vine vorba de navigarea anonima.

Principala functie a hidemyip este de a permite navigarea anonima prin schimbarea dresei IP. Pe langa aceasta exista si alte functii cum ar fi:

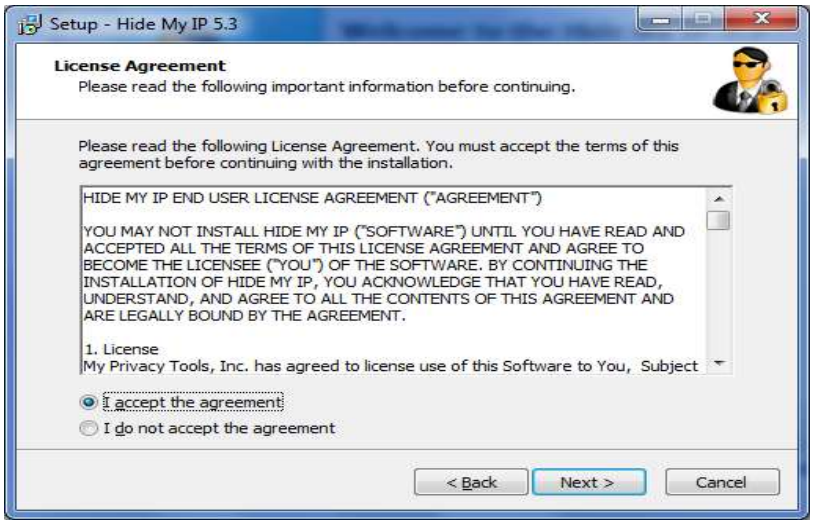
- Ascunde identitatea in timpul folosirii e-mail-ului, chat-ului, jocurilor etc.
- Protejeaza identitatea de hackeri – care iti pot folosi adresa IP pentru a-ti accesa calculatorul instaland keyloggeri, troieni sau alte instrumente care pot folosi scopurilor lor. Poti opri aceste abuzuri de la sursa prin ascunderea IP-ului.
- Poti trimite mailuri anonime prin ascunderea adresei IP din headerul mailului..
- Ofera o configurare automata a browserului – functionand cu majoritatea browserelor.

Instalare

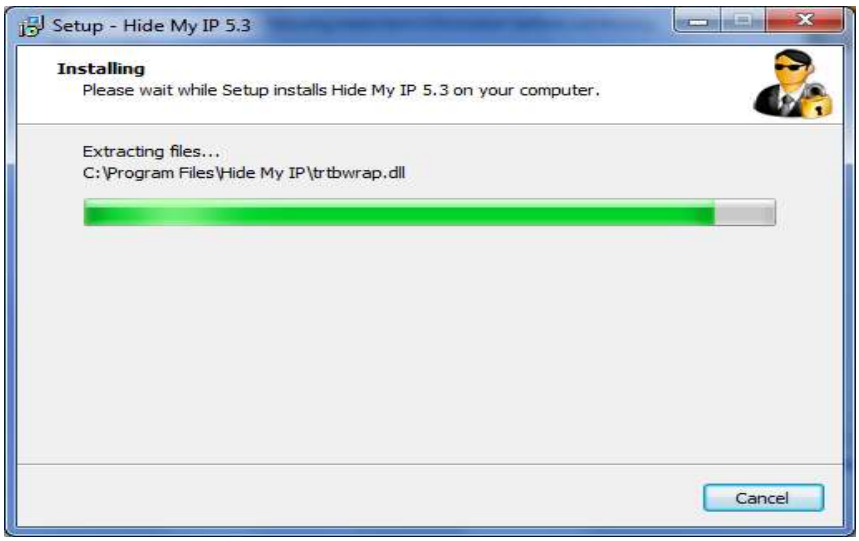
Hidemyip este o aplicatie simpla care respectiv necesita si o instalare simpla, mai jos sunt demosntrati principalii pasi in instalare acestuia:

Este lansata instalare aplicatiei

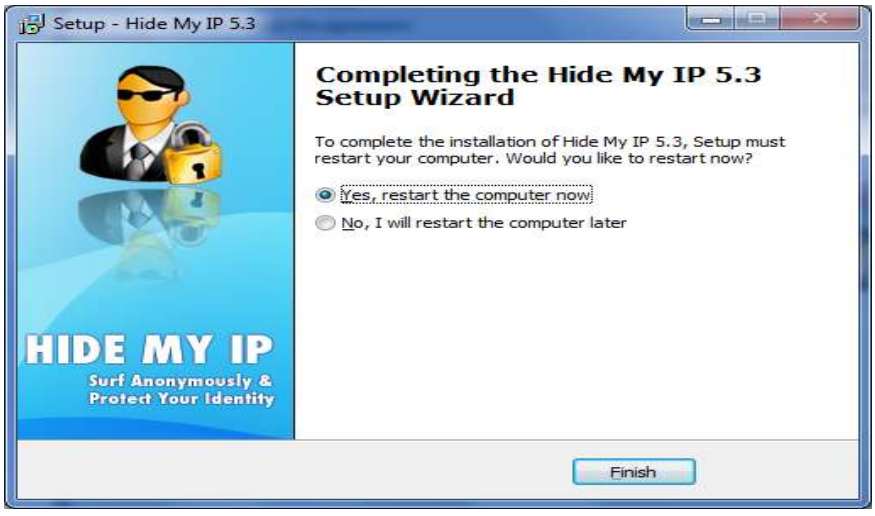
Dupa care acceptam termenii de acord



Dupa care are loc instalarea propriu-zisa



Dupa ce are loc instalarea completa ni se va cere o repornire a calculatorului



Configurare

Dupa lansarea HideMyIP vedem o interfata destul de simpla

de unde se pot face urmatoarele:

- de ascuns IP-ul facand click pe butonul **Hide My IP**
- de schimbat IP-ul la fiecare X minute
- de sters cooky-urile de fiecare data cand se schimba IP-ul
- de cerut un IP din State sau din oricare alta parte.

Pentru mai multe optiune putem accesa Advanced Settings

unde avem aceleasi posibilitati descrise mai sus precum si posibilitatea de a alege browsere-le pt care va functiona programul nostru

Astfel vedem ca programul dat este destul de simplu nu necesita o configurare complicate insa este destul de practic

Exemplu de utilizare:

In cele ce urmeaza voi arat un exemplu de utilizare a HideMyIP, asa cum la lansarea lui ne este aratat adresa noastra de IP reala

La alegerea optiunii Hide My IP, programul nostru ne va genera o noua adresa IP cu care vom naviga ca anonimat pe internet si asta va fi de ex :

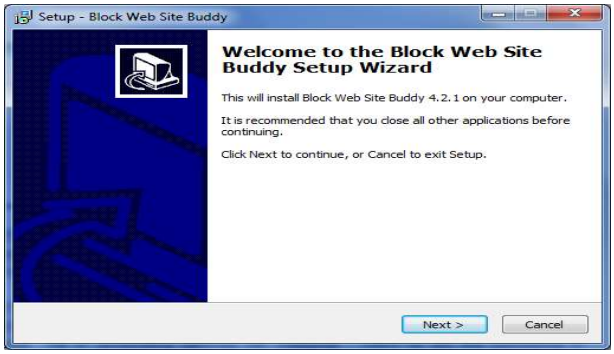
In cazul in care dorim sa revenim la adresa noastra IP reala atunci activam butonul Stop Hiding IP, si respectiv vom reveni la adresa noastra initiala. Pentru un exemplu concret in care sa vedem ca intradevarul programul nostru functioneaza vom experimenta urmatoarele, mai intii accesam un site care ne va arata adresa noastra reala precum si date despre IP-ul nostru, accesam adresa http://www.globushost.ro unde avem datele noastre

Dupa ce activam butonul Hiding My IP si vom accesa aceeasi adresa http://www.globushost.ro , datele nostre vor arata astfel atit la verifcarea lui pe site cit si la activare butonului in program:

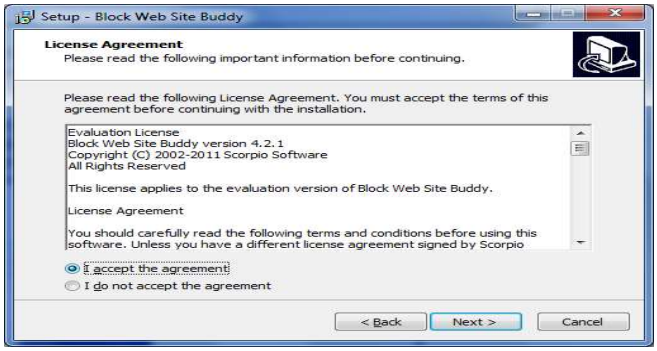
Observam astfel ca programul nostru lucreaza perfect si adresele IP corespund atit la generarea de catre program precum si la verificarea pe site. Acum putem naviga liber ca anonimat pe oricare site fara frica de a se afla datele noastre.

2. A doua aplicatie cu directia de proxy server se refera anume la restrictionarea site-urilor nedorite de a fi accesate, Block Web Site Buddy este la fel o aplicatie simpla cu o interfata destul de simpla care la fel nu necesita o configurare complicata.

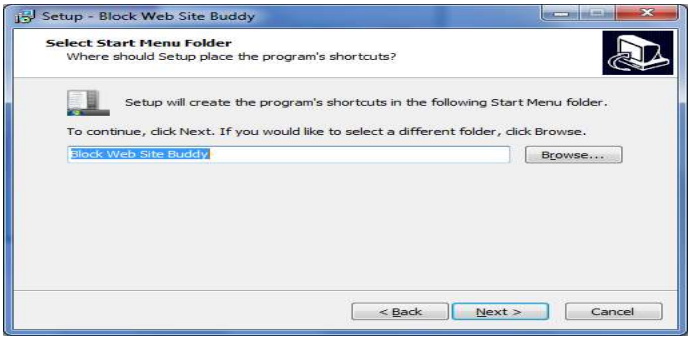
Instalare:



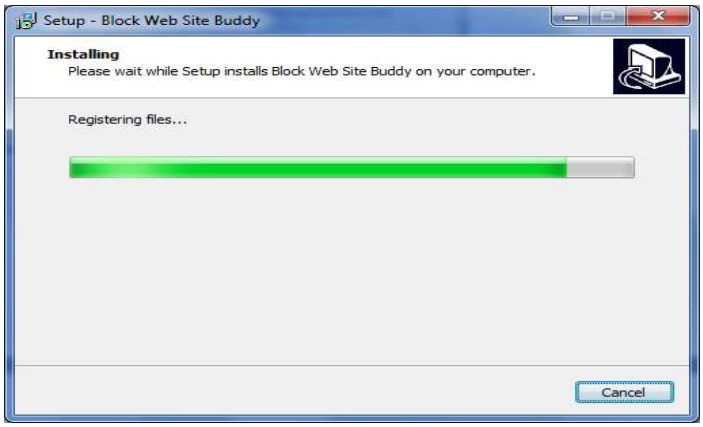
Acceptam conditiile:



Selectam directoriul

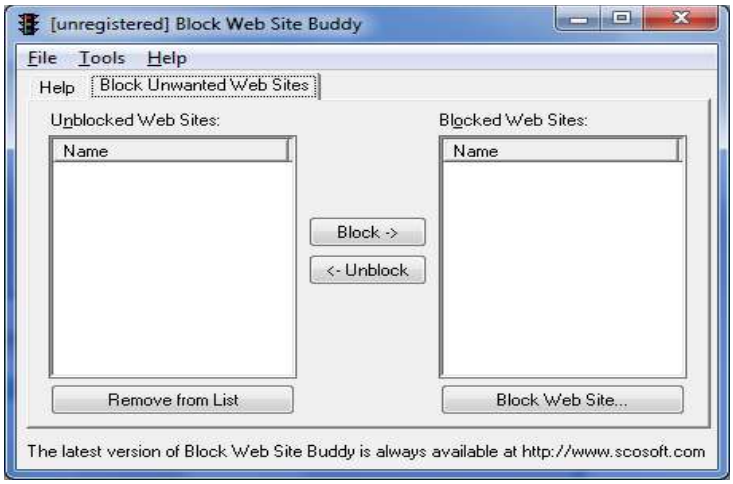


Instalare propriu-zisa

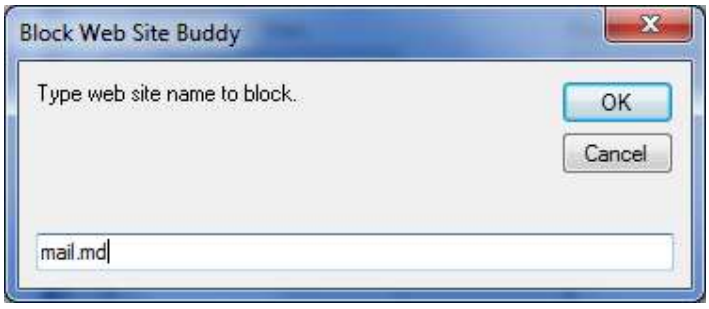


Confgurare si exemplu de utilizare:

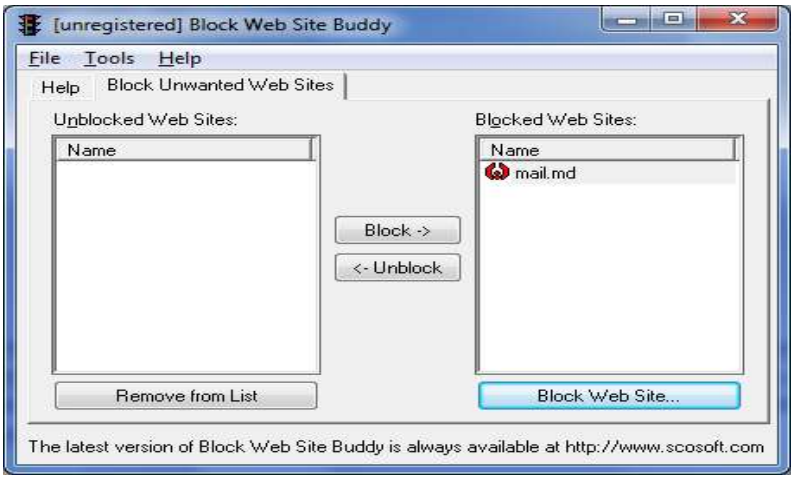
Programul este unul foarte simplu care nu necesita o configurare speciala asa ca dupa instalarea lui lansam programul unde ne apare urmatoare fereastra



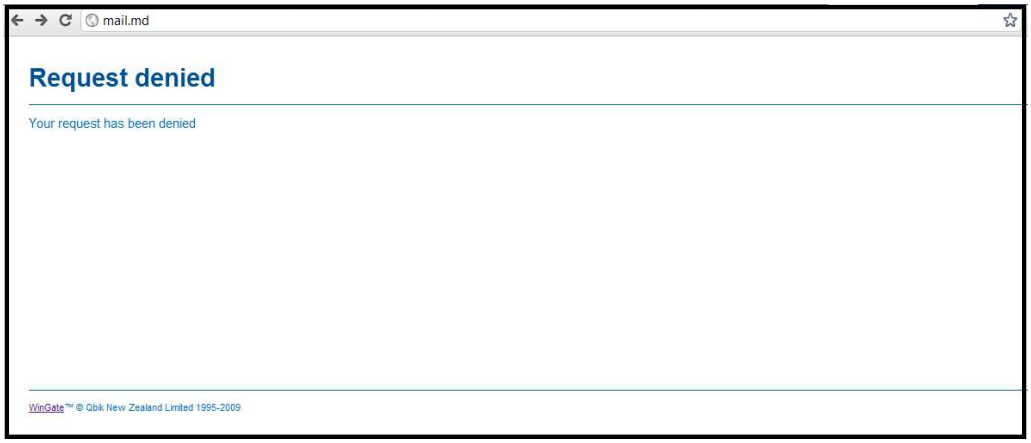
Asa cum se vede si in fereastra de mai sus avem 2 colonite in care in una din ele putem numerota lista site-urilor neblocate , iar in a 2-a colonita lista site-urile cu acces interzis. De ex. Pentru a bloca accesul unui site apasam butonul Block Web Site… in care vom scri denumirea site-ului care urmeaza a fi blocat:



Apasam OK si avem numele site-ului in lista a 2-a:



Acum la accesarea acestui site vom avea ca raspuns :



Block Web Site Buddy este o aplicatie foarte utila in blocarea site-urilor precum si a bannerele publicitare, fiind totodata compatibil cu toate tipurile de browsere.