Proiect Reţele de Calculatoare

Configurarea unui firewall

Agnitum Outpost Firewall Pro 2008

Student: Hudescu Marius Gabriel

Anul 3 – Facultatea de Inginerie Electrică şi Știința Calculatoarelor

Anul Universitar 2007 – 2008

Rezumatul Proiectului

- Noţiuni despre firewall si configurarea unui firewall personal

Notiuni generale despre un firewall:

Firewall - "Zid de foc" sau "Paravan de protecţie"

Generalităţi/Definiţii:

Un paravan de protecţie poate ţine la distanţă traficul Internet cu intenţii rele, de exemplu hackerii, viermii şi anumite tipuri de viruşi, înainte ca aceştia să pună probleme sistemului. În plus, un paravan de protecţie poate evita participarea computerului la un atac împotriva altora, fără cunoştinţa dvs. Utilizarea unui paravan de protecţie este importantă în special dacă sunteţi conectat în permanenţă la Internet.

Un firewall este o aplicaţie sau un echipament hardware care monitorizează şi filtrează permanent transmisiile de date realizate între PC 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 – Internetul -> sunt identificaţi posibilii "musafiri" nepoftiţi, atacurile lor asupra PC-ului sau reţelei locale putând fi oprite.
- Controlul resurselor pe care le vor accesa utilizatorii locali.

Cum funcţionează?

De fapt, 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.

Soluţiile firewall se împart în două mari categorii: prima este reprezentată de soluţiile profesionale hardware sau software dedicate protecţiei întregului trafic dintre reţeaua unei întreprinderi (instituţii -> ex.: Universitatea "Stefan cel Mare", Suceava) şi Internet; iar cea de a doua categorie este reprezentată de firewall-urile personale dedicate monitorizării traficului pe calculatorul personal. (ex // Zone Alarm Free,Outpost Firewall Pro,Norton Personal Firewall ș.a)

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 dial-up cu modalităţi de conectare mai eficiente (cablu, ISDN, xDSL 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:

- alege ce servicii va deservi firewall-ul
- desemnează grupuri de utilizatori care vor fi protejaţi
- defineşte ce fel de protecţie are nevoie fiecare grup de utilizatori
- pentru serviciul fiecărui grup descrie cum acesta va fi protejat
- 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.

Clasificări:

Firewallurile pot fi clasificate după:

- Layerul (stratul) 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.

Ce "poate" şi ce "nu poate" să facă un firewall?

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

De asemeni, o aplicaţie firewall nu poate:
- interzice importul/exportul de informaţii dăunătoare vehiculate ca urmare a acţiunii răutăcioase a unor utilizatori aparţinând spaţiului privat (ex: 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.

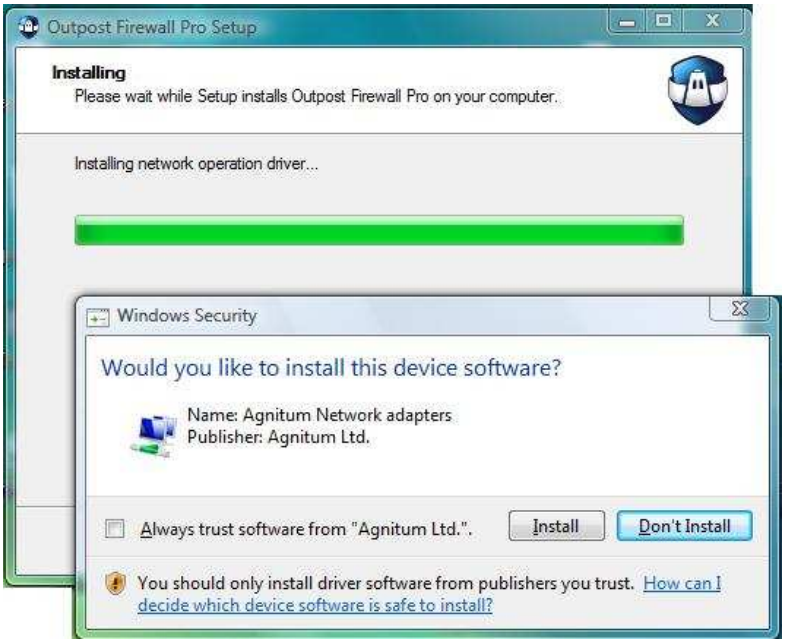
Pentru acest proiect am ales ca soluţie software “Outpost Firewall Pro 2008”

1.1 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

In timpul instalării vor aparea 2 ferestre de genul urmator:



Bifaţi si instalați şi aceste componente adiționale, necesare soft-ului.

2. Configurare

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

Firewall – ului prin 2 metode.

1. Modul *Normal*: este recomandat majorității utilizatorilor întrucât nu cere cunostințe foarte avansate de configurare.

2. Modul *Advanced*:

Vor apărea cateva opțiuni de configurare pentru modulul anti-spyware al programului peste care vom trece:

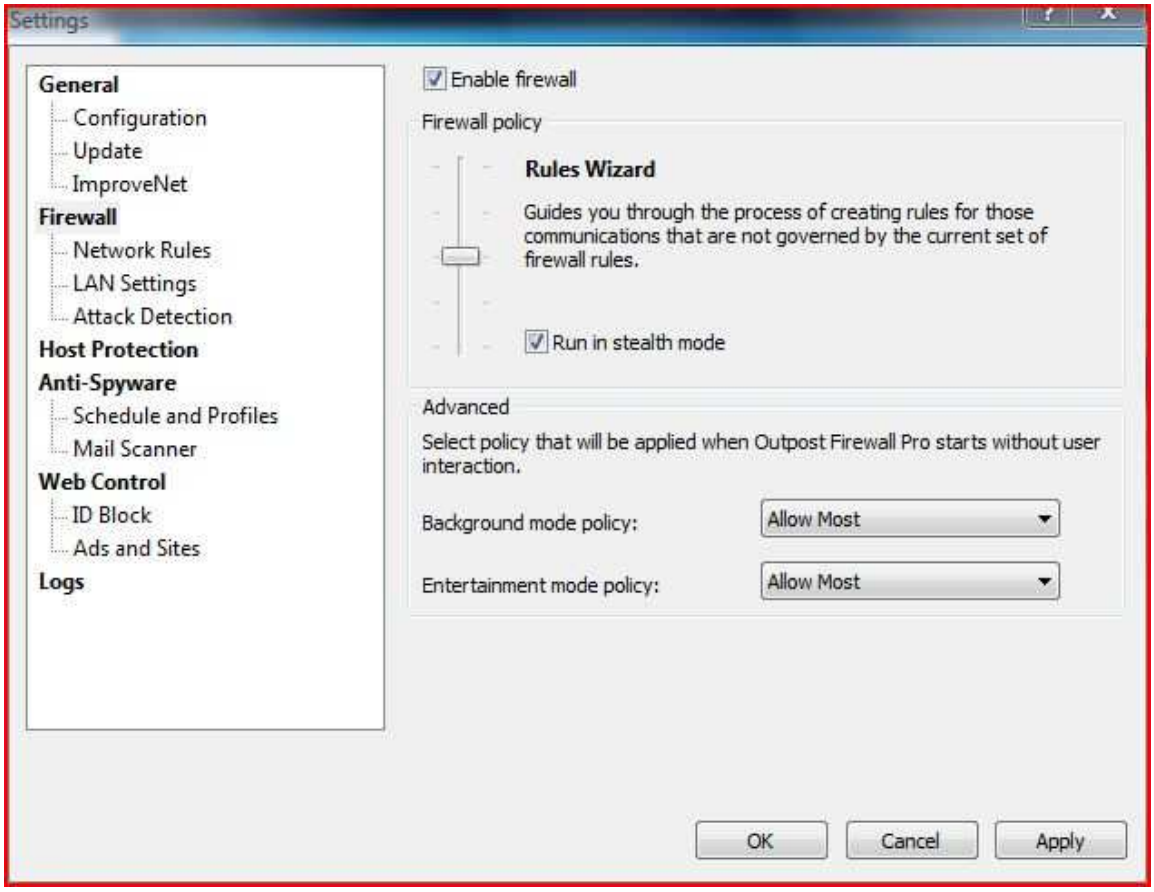
Clic pe *Next* si expertul de configurare a incheiat instalarea.

Restartam sistemul.

Dupa restartarea sistemului n-i se va cere o cheie de inregistrare.

Introducem cheia de inregistrare a produsului.

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) .

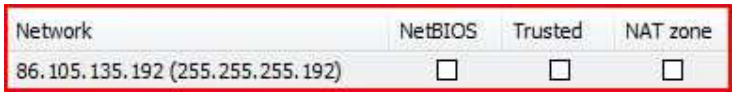
Network rules (reguli de rețea) – în dreptul acestui tab în dreapta avem afişate o serie de programe si servicii windows (cu extensia .exe) care sunt încadrate sub 3 subcategorii:

- 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

1) Maximal (Protectie maximă) – este raportat fiecare scanare a retelei; sunt detectate toate atacurile externe retelei Ethernet.
2) 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.
3) 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.

- toate cererile de accesare a rețelei din partea unor componente noi sau modificate de la ultima accesare sunt monitorizate.
- 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.

- cererile executabilelor care s-au modificat de la ultima verificare, la rețea sunt monitorizate.

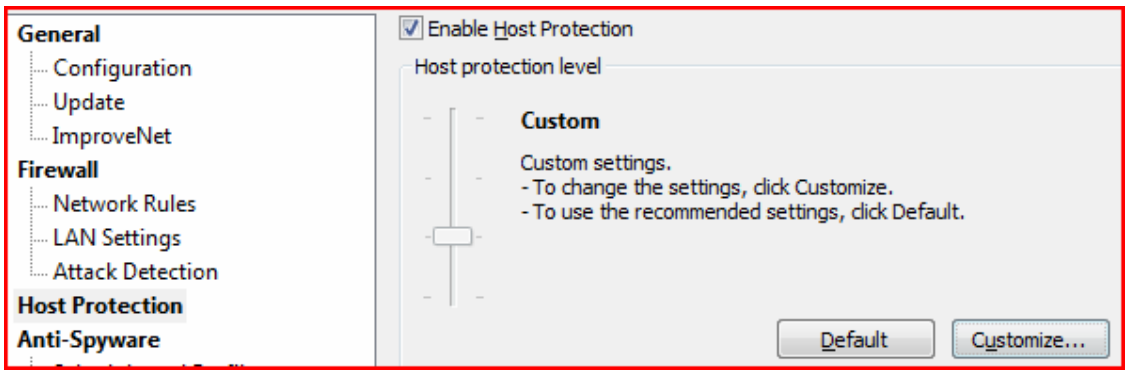
❖ Low (Protecție scazută) – Controlul Anti-Leak este dezactivat.

- cererile executabilelor care s-au modificat de la ultima verificare, la rețea sunt monitorizate.

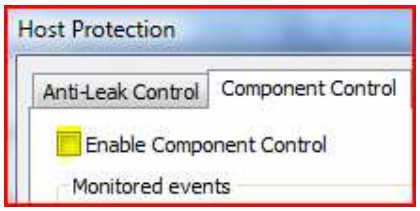
Obs: *Toate aceste modificări ale executabilelor și alte operațiuni care se aplica anumitor componente ale diferitelor aplicatii sunt intr-o continua modificare datorită interactiunii unor module ale acestora cu sistemul de operare.*

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 Pro 2008"

Sigur că erau mult mai multe de prezentat însă era pur și simplu prea mult … ☺

O prezentare foarte complexă a tuturor setărilor şi opţiunilor de configurare poate fi gasită pe site-ul oficial.

Bibliografie

- www.wikipedia.com
- www.auditmypc.com

Fisierele de help ale aplicatiei gasite la adresa www.agnitum.com