Firewall sau zidul de protecție este un instrument foarte important atunci când este vorba de securitatea sistemului de operare. Microsoft a implementat propriul firewall în Windows 2000 și de atunci fiecare sistem de operare are acest instrument care, cu fiecare versiune, este mai avansat și mai bun.

Întregul trafic care are loc în rețea vine la unul dintre calculatoare trecând prin anumite porturi care trebuie să fie deschise pentru a primi traficul. Însă, atunci când porturile sunt deschise, pe lângă traficului normal şi legitim, prin ele mai poate trece şi traficul rău intenționat, al cărui scop este să provoace daune. Aici intervine firewall-ul care se ocupă cu controlul porturilor. Firewall-ul vă permite să închideţi porturile inutile și să le deschideți pe acelea de care aveți nevoie pentru comunicarea directă. În mod implicit, odată cu instalarea sistemului de operare, toate porturile de intrare sunt închise, ceea ce înseamnă că niciun pachet nu poate ajunge la calculatorul dvs. Acest lucru este excelent, deoarece sunteţi pe deplin protejat de pachetele malware care există pe Internet, dar, în același timp, este şi rău, fiindcă nici pachetele legitime nu vor ajunge la dvs., ceea ce înseamnă că nu veţi putea comunica cu nimeni.

Atunci când este vorba de setarea firewall,foarte mulți administratori recurg la dezactivarea totală a acestui instrument. Acest lucru este acceptabil doar în cazul în care există în reţea un firewall care va filtra traficul pentru toţi clienţii. În caz contrar, recomandarea este ca firewall-ul să fie activat și configurat corect.

Pentru configurarea firewall-ului, se utilizează instrumentul Windows Firewall din Control Panel. De aici, cu un clic pe Turn Windows Firewall On or Off puteţi dezactiva, respectiv activa firewall-ul. Pentru a accesa setările detaliate ale firewall-ului, daţi un clic pe linkul Advanced Settings din partea stângă a ferestrei.

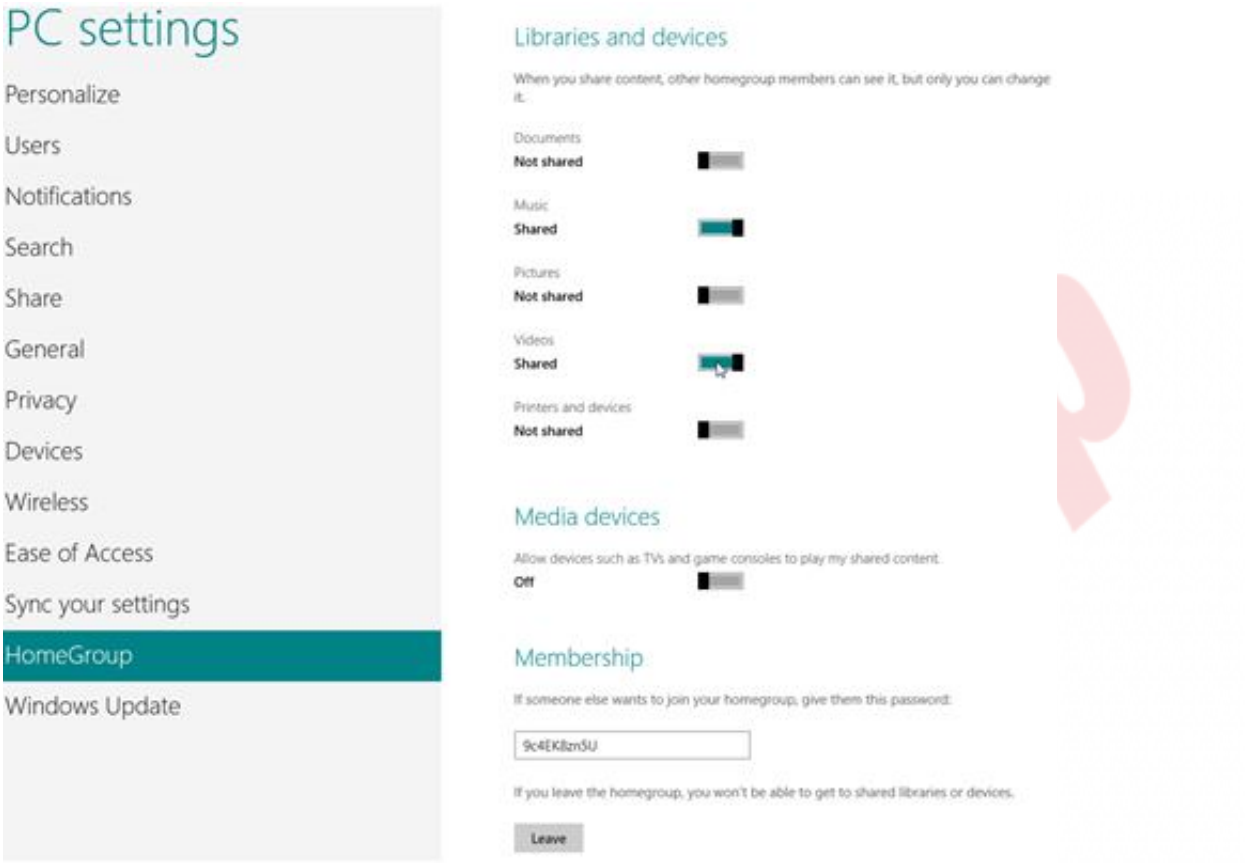

Figura 13.1 Setarea Windows Firewall

În cadrul setărilor avansate ale firewall-ului, veţi putea face configurații speciale pentru fiecare tip de rețea (private, public, domain), puteți seta reguli de securitate individuale sau reguli de partajare. De exemplu, puteţi activa File and Print Sharing numai în rețeaua companiei (domain) şi astfel veţi proteja datele de utilizator sensibile, atunci când utilizatorul se conectează la o rețea publică.

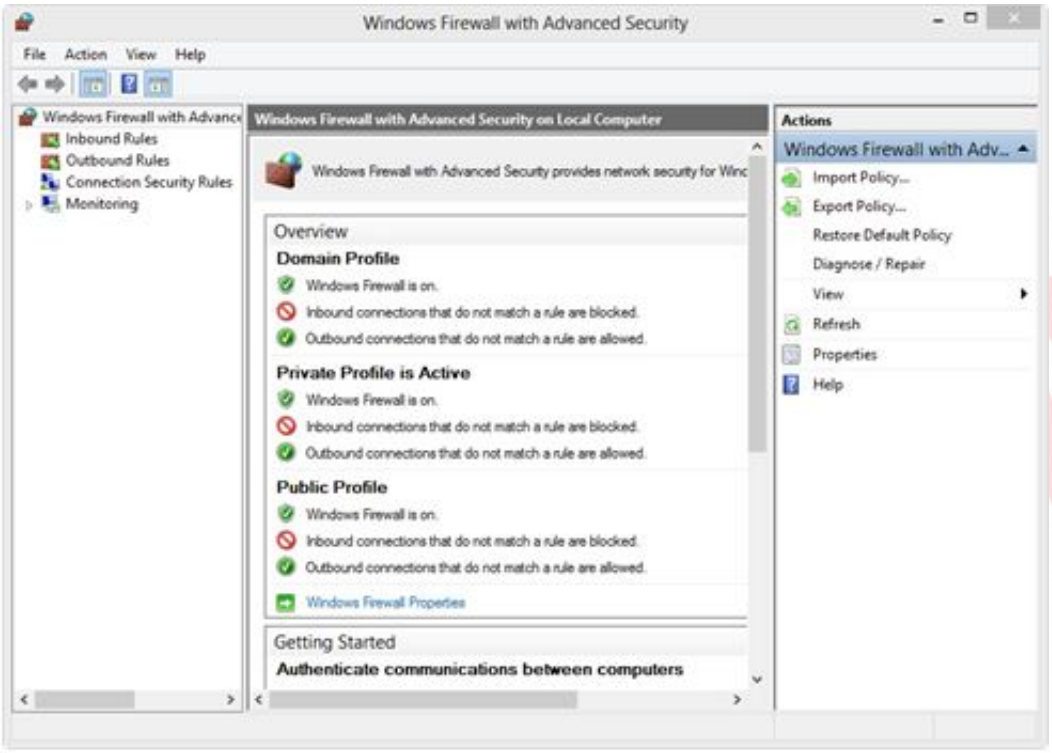

Figura 13.2 Windows Firewall - setări avansate

Pentru fiecare rețea separat, puteți configura:

- Firewall State – dacă firewall-ul este activat sau dezactivat.
- Inbound Connections -blocarea anumitor conexiuni pe baza anumitor reguli. Aceasta poate include blocarea unui anumit port, aplicație sau serviciu.
- Outbound Connections– aceeași situație, dar în direcția opusă. Deci, regulile care se referă la traficul de ieșire.
- Settings – setarea alertelor, a regulilor locale etc.
- Logging – dacă, cum și cât de mult se va ține o evidență a înregistrărilor despre evenimente legate de firewall (logs).

În panoul din stânga, se află opțiunea Monitoring pe care o puteți utiliza pentru a urmări regulile create prin default, dar şi regulile pe care le-ați creat singuri și, pe baza aceasta, să creaţi rapoarte legate

de comportament. Aceasta include informații despre statusul actual în care se află.

Toate regulile firewall le puteţi exporta dând clic dreapta pe regulă în fereastra principală a firewall-ului și selectând Export Policy. Aceste reguli le puteţi importa ulterior pe alte calculatoare pentru a reduce timpul necesar setării firewall-ului.

Când creați o nouă regulă de intrare (inbound) sau de ieşire (outbound), aveţi posibilitatea de a seta permisiuni și interdicții în funcţie de:

- Program rules – comportamentul firewall-ului atunci când vine în contact cu o anumită aplicație. Pentru a face acest lucru cu succes, este suficient doar să specificaţi fişierul executabil .exe al aplicaţiei căreia îi permiteţi sau interziceţi ceva.
- Port rules – interzicerea traficului TCP sau UDP pe un anumit port. Prin închiderea unui port, nicio aplicaţie nu va fi capabilă să primească, respectiv să trimită pachete prin el.
- Predefined rules – reguli predefinite. Se foloseşte Windows experience şi puteţi specifica unul dintre protocoalele enumerate sau programele cărora doriţi să le permiteţi sau să le interziceţi trecerea.
- Custom Rules – acoperă tot ceea ce v-aţi dori să faceți cu firewall-ul și nu este inclus în opțiunile precedente, dar şi o combinație a opțiunilor anterioare.

Pe lângă regulile de reglementare a traficului de intrare și de ieșire, puteți seta şi regulile Connection Security pentru securizarea conexiunii. Aceste reguli securizează traficul folosind IPSec şi vor fi folosite pentru a determina când și cum trebuie să se utilizeze autentificarea între două calculatoare.

- Regulile de izolare sunt folosite pentru dezactivarea conexiunilor pe baza criteriilor de autentificare, cum ar fi aderarea la domeniu, starea de sănătate a calculatorului (cea mai recentă versiune a

programului antivirus și baza lui de date etc.)

- Excepţia de la regulile de autentificare (Authentication Examption Rules). Se utilizează pentru a determina care tipuri de conexiuni pot fi excluse din regulile de autentificare. Aceste reguli se pot folosi pentru a permite accesul la un calculator sau comunicarea între două calculatoare sau subrețele şi fără o autentificare de succes.
- Regulile Server-To-Server poate proteja conexiunile dintre calculatoarele individuale.
- Regulile pentru tunneling pot oferi o comunicare securizată între două calculatoare prin crearea de tuneluri care sunt protejate de IPSec.

Porturile prin care trece traficul sunt în intervalul de la 0 la 65535. Unele dintre porturile cele mai întâlnite și traficul care trece prin ele sunt prezentate în tabelul de mai jos.

Port	Protocol	Se utilizează pentru...
21	TCP	File Transfer Protocol (FTP)
23	TCP	Telnet – conectarea la host-uri de la distanţă prin linia de comandă
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP	Domain Name System (DNS)
53	TCP	DNS
80	TCP	Hypertext Transfer Protocol (HTTP) – pentru navigarea pe Internet
110	TCP	Post Office Protocol (POP3) - pentru trimiterea mail-urilor

143	TCP	Internet Message Access Protocol (IMAP) – pentru sincronizarea mail-urilor
161	UDP	Simple Network Message Protocol (SNMP)
389	TCP	Lightweight Directory Access Protocol (LDAP)
443	TCP	Hypertext Transfer Protocol Security (HTTPS)
3389	TCP	Remote Desktop Protocol (RDP) – pentru preluarea controlului asupra unui calculator de la distanţă

Tabel 13.1 Porturi

Verificarea porturilor deschise și disponibile o puteţi face folosind instrumentul de comandă netstat.

Netstat vă va afișa toate conexiunile active TCP şi UDP și toate porturile deschise.

Windows Defender

Windows 8 este prima versiune a sistemului de operare Windows care vine cu un program antivirus integrat. Windows Defenderaduce antivirusul Microsoft Security Essentials, care este pornit imediat după instalare, ceea ce înseamnă că acum nu veți fi niciun moment fără protecţie antivirus. Windows Defender nu trebuie confundat cu Windows Defender-ul de pe sistemul de operare Vista sau Windows 7. Acum, acesta conţine mult mai multe facilităţi decât înainte.

Windows Defender aduce o opțiune foarte bună, care îl diferenţează în mare măsură de celelalte soluții antivirus. Dacă lucrați pe calculator, el nu vă va sufoca cu scanări și verificări permanente și nu va utiliza o parte de resurse pentru el însuși, încetinindu-vă astfel munca. El va scana doar dispozitivele care se conectează la calculator (USB), iar pentru scanarea fişierelor va aştepta să mergeţi în pauza sau, pur și simplu, să lăsați calculatorul inactiv pentru un anumit timp.

Instrumentul pentru setarea Windows Defender-ului îl puteţi porni căutând în ecranul de start sau direct din Control Panel.

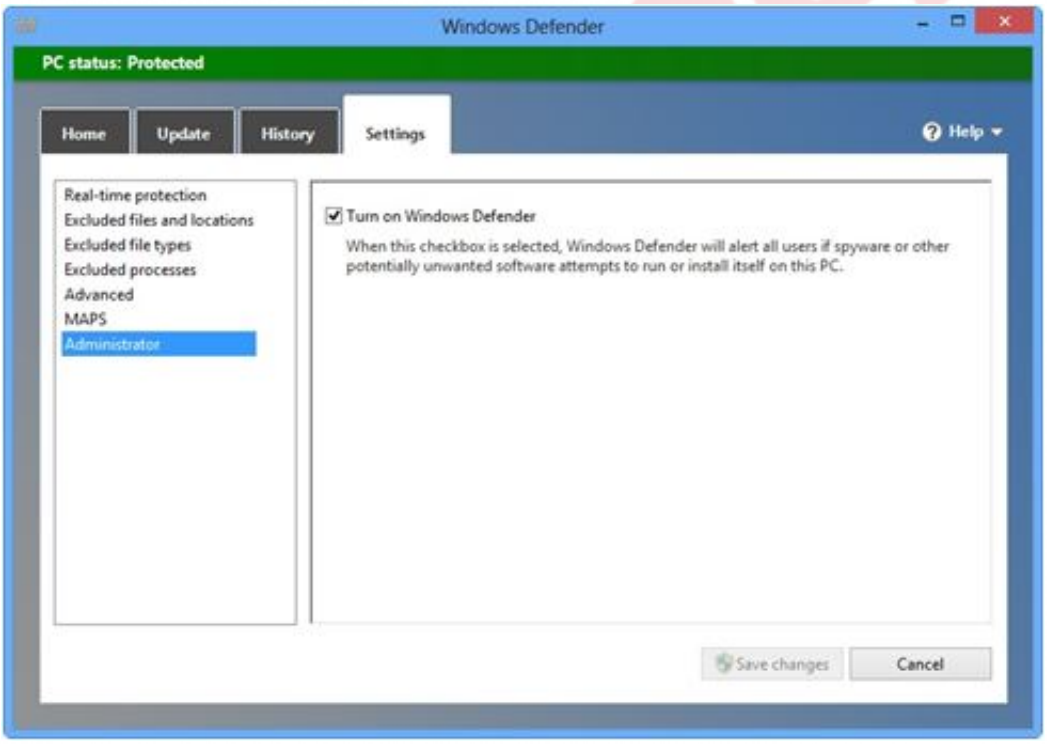

Figura 13.3 Setarea Windows Defender

În tab-ul Settings, puteţi seta:

- Real-Time Protection – vă permite să opriți scanarea continuă și constantă. Acest lucru cu siguranţă nu este recomandat.
- Excluded Files And Locations – vă permite să specificați folderele, partițiile și fișierele care nu ar trebui să fie scanate. Acest lucru se

referă în principal la părțile care pot provoca alerte false cu privire la conținut.

- Excluded File Types – aici puteți specifica tipurile de fișiere care nu ar trebui să fie scanate. Acest lucru nu este recomandat, deoarece programul malware se poate atașa la orice tip de fișier.
- Excluded Processes – o opțiune bună în mediul de afaceri. Companiile folosesc adesea aplicații și instrumente care pot fi recunoscute ca malware.
- Advanced – vă permite să activați sau să dezactivați scanarea fișierelor arhivate, a drive-urilor USB etc.
- MAPS – permite Windows Defender-ului să utilizeze Microsoft Active Protection Service, care permite detectarea soft-urilor maliţioase şi verificarea automată.
- Administrator – vă permite să dezactivați Windows Defender dacă aveți de gând să folosiți o altă soluție antivirus.

WIN8_13 - Windows 8

1. Portul pe care trebuie să-l deschideţi în firewall pentru a asigura utilizatorilor o navigare neîntreruptă pe Internet este:

- a) 8080
- b) 80
- c) 90
- d) 143

2. În instrumentul Windows Defender este inclus un program antivirus. Care este acesta?

- a) AVG
- b) Avira
- c) Microsoft Security Essentials
- d) Trend Micro

3. Windows Defender scanează continuu traficul care are loc și controlează activitățile de pe calculator. Acest lucru îl puteţi opri prin dezactivarea opțiunii:

- a) Real-Time Protection
- b) Excluded Files And Locations
- c) Excluded File Types
- d) MAPS

4. Windows Defender scanează prin default toate fișierele și folderele de pe calculator. Pentru a opri acest lucru și pentru a stabili ce trebuie şi ce nu trebuie scanat, trebuie să setaţi opţiunea:

- a) Real-Time Protection
- b) Excluded Files And Locations
- c) Excluded File Types
- d) MAPS

5. Compania dvs. foloseşte serverul IMAP pentru sincronizarea mail-urilor pe calculatoarele client. Ce port trebuie să fie

deschis în Firewall-ul de pe calculatorul dvs. pentru ca acesta să funcţioneze?

- ◯ a) 8080
- ◯ b) 80
- ◯ c) 110
- ◯ d) 143

6. Pentru a bloca intrarea unui anumit tip de trafic pe calculatorul dvs., ce regulă trebuie să configuraţi în setările firewall?

- ◯ a) Inbound
- ◯ b) Outbound
- ◯ c) Logging
- ◯ d) State

7. Regulile Firewall le puteţi defini în funcţie de:

- ☐ a) porturi
- ☐ b) programe
- ☐ c) utilizatori

1. Portul pe care trebuie să-l deschideţi în firewall pentru a asigura utilizatorilor o navigare neîntreruptă pe Internet este:

b

2. În instrumentul Windows Defender este inclus un program antivirus. Care este acesta?

c

3. Windows Defender scanează continuu traficul care are loc și controlează activitățile de pe calculator. Acest lucru îl puteţi opri prin dezactivarea opțiunii:

a

4. Windows Defender scanează prin default toate fișierele și folderele de pe calculator. Pentru a opri acest lucru și pentru a stabili ce trebuie şi ce nu trebuie scanat, trebuie să setaţi opţiunea:

b

5. Compania dvs. foloseşte serverul IMAP pentru sincronizarea mail-urilor pe calculatoarele client. Ce port trebuie să fie deschis în Firewall-ul de pe calculatorul dvs. pentru ca acesta să funcţioneze?

d

6. Pentru a bloca intrarea unui anumit tip de trafic pe calculatorul dvs., ce regulă trebuie să configuraţi în setările firewall?

a

7. Regulile Firewall le puteţi defini în funcţie de:

a, b