**ლექცია № 6 ინტერნეტში ჩართვა, ბრანდმაუერი**

ინტერნეტში ჩართვა შესაძლებელია რამდენიმე საშუალებით: დაწყებული ***კერძო მოდემური*** და დამთავრებული ***ზოგადი - კორპორატიული ქსელის საშუალებით*** ჩართვამდე.

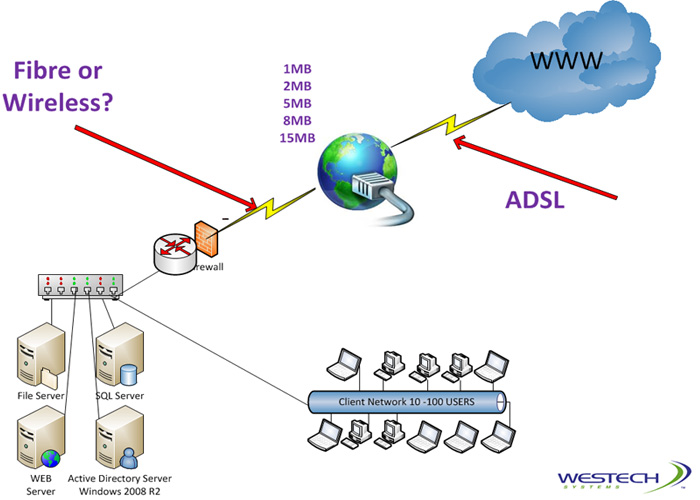
**ინტერნეტ მომსახურების მომწოდებელი - პროვაიდერი, (ISP)** არის ორგანიზაცია ან კომპანია, რომელიც უზრუნველყოფს ინტერნეტის წვდომას. პროვაიდერს აქვს მაღალსიჩქარული შეერთება ინტერნეტთან და როგორც წესი, მიაწოდებს თავის კლიენტებს ინტერნეტ შეერთებას უფრო ნაკლე სიჩქარით.

**ინტერნეტ ჩართვის ტიპები და მოწყობილებები**

* **მოდემური ჩართვა** ჩვეულებრივი სპილენძის სატელეფონო ხაზებით. სიჩქარე: ჩამოტვირთვის (Download speed) - 53,3 კილობიტი/წამში; ატვირთვის (Upload speed) – 33,6 კილობიტი/წამში. რეალური სიჩქარეები გაცილებით ნაკლებია. შესაძლებელია რამდენიმე მოდემის გაერთიანება მრავალარხიანი ტექნოლოგიების გამოყენებით.
* **ISDN არხი**,წარმოადგენსციფრულ სატელეფონოხაზს. როგორც წესი გამოიყენება ორი არხი (ერთი ასატვირთად, მეორე ჩამოსატვირთად) სიჩქარით - 64 კილობი­ტი/წამში. **ISDN** ჩაირთვება **ტერმინალურ ადაპტერში (TA)** ან ISDN მარშრუტიზატორში. TA ფაქტიურად არის ”ციფრული მოდემი” , თუმცა ტექნიკური აზრით იგი არ წარმოადგენს მოდემს, რადგანაც არ ხდება სიგნალის მოდულაცია და დემოდულაცია. TA არის როგორც შინაგანი, ასევე გარეგანი.
* **თანამგზავრული ჩართვა** - ან ცალმხრივი ( თანამგზავრის არხის გამოყენება მონაცემთა ჩამოსატვირთად და ასატვირთად კი სატელეფონო ხაზის), ან ორმხრივი; ჩართვა ხდება თანამგზავრული ანტენით -თეფშით; თანამგზავრული ჩართვის სიჩქარე ვარირებს ***400 კილობიტი/წამიდან 2 მეგაბიტი/წამამდე.***
* **DSL (Digital Subscriber Line- ციფრული სააბონენტო ხაზი)** არხი იძლევა საშუალებას სატელეფონო ხაზების გამტარიანობის გაზრდას. გამოიყენება DSL-ის სხვადასხვა ვარიანტები, მაგალიღად ასიმეტრიული DSL – ADSL, როცა გამტარიანობის დასაშვები შუალედი ასიმეტრიულადაა განაწილებული ჩამოტვირთულ და ასატვირთ ტრაფიკებს შორის. სიჩქარე: ჩამოტვირთვის- **384 *კილობიტი/წამიდან***  **6 *მეგაბიტი/წამამდე.*** და ასატვირთვი **128 *კილობიტი/წამიდან*** **2** ***მეგაბიტი/წამამდე*** .
* **საკაბელო ჩართვა** და კაბელური ”მოდემი” ან მარშრუტიზატორი, ანალოგიურის DSL-ის სიჩქარეების.
* **ოპტიკურ-ბოჭკოვანი არხი და ბარათი Ethernet**. ოპტიკურ-ბოჭკოვანი არხით დაკავშირებულ აბონენტებს შორის კავშირის სიჩქარე **100**  ***მეგაბიტი/წამამდე*** .
* **გამოყოფილი ციფრული სატელეფონო ხაზი,** მაგალითად **T1** (1,544 ***მეგაბიტი/წამი)*** და **T3 (44,736** ***მეგაბიტი/წამი)***

**ბრაუნდმაუერი**

ქსელური ჩართვის დასაცავად გამოიყენება პროგრამული ან აპარატული მოწყობილება სახელად ბრამდმაუერი. გერმანული სიტყვა ბრამდმაუერი ნიშნავს ცეცხლისგან დამცავ კედელს. მისი ინგლისური ექვივალენტია ფაიერვოლი - Firewall,

****

ნახატი 6.1. ბრანდმაუერისა და პროქსი-სერვერების მდებარეობა კომუნიკაციებში

ბრანდმაუერი წარმოადგენს დაცვას ქსელის (იხ. ნახატი 6.1.) საზღვარზე და ახდენს შემოწმებას მონაცემთა იმ პაკეტისა, რომლებიც ცდილობენ შიგა ქსელში შეღწევას, და ამ შემოწმების შემდეგ, ნებართვას იძლევა მონაცემთა იმ პაკეტის გატარებაზე, რომლებიც აკმაყოფილებენ ადმინისტრა­ტორის მიერ შემუშავებულ პოლიტიკას. მაგალითად ადმინისტრატორს შეუძლია ბრანდმაუერის ისეთი კონფიგურაციის შექმნა, როცა იგი გაატარებს ელექტრონული ფოსტის ტრაფიკს და დაბლოკავს ჩატს.

არსებობს ბრანდმაუერის მრავალი სახეობა, დაწყებული იმ პროგრამული მოწყობილებებიდან, რომლებიც ბინის ქსელების დაცვისთვისაა შექმნილი, დამთავრებული რთული და ძვირადღი­რებული აპარატული ქსელური ეკრანებით, რომლებიც ისეთი ხარისხის დაცვას იძლევიან, რომე­ლიც საკმარისია სამხედრო საქმეში გამოსაყენებლად. Windows XP -ს გააჩნია ჩაშენებული (შიგა) პროგრამული ბრანდმაუერი, გათვალისწინებული ცალკეული კომპიუტერებისა და მცირე ქსელების დასაცავად და რომელსაც ეწოდება **Windows Firewall** (ვინდოუს ფაიერვოლი), იგი წარ­მოადგენს ადრე არსებული უტილიტას - *ინტერნეტ შეერთების ფაიერვოლის* - **Internet Connection Firewall** (**ICF**) მოდიფიკაციას. მოდიფიკაციის აუცილებლობა გამოიწვია იმ კომპიუტერების მასობ­რივმა დაინფიცირებამ 2003-2004 წლებში ორი ”ჭიის” საშუალებით - *ბლასტერისა* (Blaster) და *სასერის* (Sasser) მიერ, რომლებშიც ქსელთაშორის ეკრანისთვის **Windows** -მა გამოიყენა **ICF**.

**პროქსი-სერვერი**

პროქსი-სერვერი წარმოადგენს პროგრამულ ან აპარატულ მოწყობილობას, რომელიც განთავ­სებულია კომპიუტერთა ქსელსა და ინტერნეტთან შეერთებას შორის (იხ. ნახატი 6.1.). ქსელური კომპიუტერებიდან მოთხოვნები ინტერნეტის მიმართ, მოწმდება პროქსი-სერვერში, რათა გამორიცხულ იქნეს ის მოთხოვნები, რომლებიც მიმართულია აკრძალული საიტებისკენ. (მაგალითად, ზოგიერ­თი კომპანიები ბლოკავენ სპორტულ, აზარტულ, პორნოგრაფიულ და სხვა საიტებს). პროქსი-სერვერი ასევე ინახავს ხშირად მოთხოვნილ საიტებს მათი სწრაფი ჩამოტვირთ­ვისთვის, რაც გამორიცხავს ერთი და იგივე ვებ-გვერდის ხელახლა მიღებას სერვერიდან ყოველი მომხმარებლისთვის ცალ-ცალკე.

**ქსელური შეერთებების უსაფრთხოების უზრუნველყოფა**

მრავალი უსიამოვნების თავიდან აცილებაა შესაძლებელია, თუ კი გამოვიყენებთ ქსელ­თაშორის ეკრანს, სწორედშერჩეული პარამეტრებით. ამასთან კომბინაცია აპარატული და პროგრამული ბრანდმაუერებისა იძლევა სასურველ ეფექტს კომპიუტერის თავდაცვისა ჰაკერული შეტევისგან, ვირუსებისგან, ”ჭიებისგან” და ა.შ. როგორც ვიცით, ინტერნეტში გადასაცემი დიდი მონაცემები დაიყოფა უფრო მვირე მონაცემებად - პაკეტებად და ხდება ამ პაკეტების გადაცემა ერთი წყაროდან მეორეში. ქსელ­თაშორისი ეკრანი აკონტროლებს და თუ საჭიროა არ უშვებს მიმღებ წყარომდე იმ პაკეტებს, რომლებიც არ შეესაბამებუან იმ კრიტერიუმებს, რომლითაც ხდება სანქცირებული ჩართვა - დაკავშირება.

**პაკეტების ფილტრაცია**

უმეტესი ბრანდმაუერებისა ახდენენ პაკეტების ფილტრაციას - ანუ ისინი ან ბლოკავენ ან იძლევიან უფლებას ამათუ იმ პაკეტის გადაცემისა. და ეს დამოკიდებულია პაკეტის შიგთავსზე.

ქსელ­თაშორისო ეკრანის მიერ პაკეტების ფილტრაციის წესები შეიძლება მიმართულ იქნეს გარკვეული IP-მისამართიდან ან IP-მისამართისკენ გზავნილის ან გატარებისკენ ან დაბლოკვისკენ. პაკეტების ფილტრი ამოწმებს ყოველი პაკეტის გარკვეულ ატრიბუტებს და ამის შემდეგ ამ გაატარებს მათ მარშრუტის თანახმად, ანუ მიაწვდის კომპიუტერს ან დაბლოკავს მას. მოწმდება შემდეგი ატრიბუტები:

* **საწყისი მისამართი**. იმ კომპიუტერის IP-მისამართი სადაც მოხდა პაკეტის გენერირება.
* **დანიშნულების მისამართი**. იმ კომპიუტერის IP-მისამართი რომლისთვისაც განკუთვნილია პაკეტი.
* **ქსელური პროტოკოლი.** ტრაფიკის სახე, მაგალითად, IP (ინტერნეტ პროტოკოლი).
* **სატრანსპორტო პროტოკოლი.** ზედა დონის პროტოკოლი, ისეთი როგორცაა TCP – Transmission Control Protocol (გადაცემის მართვის პროტოკოლი) ან UDP – User Datagram Protoco ( მომხმარებლის დეიტეგრამის პროტოკოლი).
* **საწყისი პორტი და დანიშნულების პორტი.** რიცხვი, რომელიც გამოიყენება კომუ­ნიკაციების განმახორციებლელი კომპიუტერების მიერ საკომუნიკაციო არხის დასა­წყისისა და დასასრულის იდენტიფიკაციისთვის.

**პაკეტების ფილტრაცია მდგომარეობის შემოწმებით**

განვიხილოთ თუ როგორ ხდება ბრანდმაუერის კონტროლის მექანიზმის ჩართვა ვებ-ბრაუზერის მაგალითზე:

1. ბრაუზერის სამისამართი სტრიქონში ვკრიფავთ რომელიმე საიტის URL -მისამარ­თს და ვაჭერთ კლავიშს - Enter.
2. ბრაუზერი გადააგზავნის ერთ ან რამდენიმე მონაცემთა პაკეტს ვებ-სერვერის მი­მართულებით. HTTP -ს ინსტრუქციები ჩართულია თავად მოთხოვნაში. დანიშნუ­ლების პორტი - 80, ეს არის HTTP -ს პორტი ვებ-სერვერისთვის, დანიშნულების პორტი შეიძლება იყოს რიცხვი 1024-ზე ნაკლები. საწყისი პორტი - ნებისმიერი რიცხვი 1024-დან 65535-მდე, რომელიც გამოიყენება მიმდინარე ჩარ­თვაზე მოთხოვნის განსაზღვრისათვის. საწყის მოთხოვნაში დაყენებულია SYM-ალამი.
3. ქსელთაშორისი ეკრანი თავის მდგომარეობათა ცხრილში ინახავს ინფორმაციას დაკავშირების შესახებ, რომელსაც იგი შემდეგ გამოიყენებს შემავალი ტრაფიკის სისწორის შემოწმებისთვის.
4. მას მერე რაც ვებ-სერვერი და მომხმარებლის კომპიუტერი დაასრულებენ კვიტირებას - ინფორმაციის სტრუქტურული ერთეულის გადაცემა-მიღების დადასტურებას, აუცილებელს TCP- შეერთებისთვის ვებ-სერვერი აგზავნის პასუხს (მოთხოვნილი ვებ-გვერდის შინაარს) კომპიუტერის IP-მისამართზე და გამომავალ პორტზე.
5. ქსელთაშორისი ეკრანი მიიღებს შემომავალ ტრაფიკს, შეადარებს საწყის-გამომავალ მისამართს საბოლოო-დანიშნულების მისამართთან, ასევე პორტის ნომერს იმ ინფორმაციასთან რომელიც ინახება მდგომარეობათა ცხრილში. თუ კი ინფორმაციები თანხვედრა ხდება ( და შემავალ პაკეტში დაყენებულია SYM და ACK ალმები), მაშინ ბრანდმაუერი იძლევა უფლებას ბრაუზერმა მიიღოს პასუხი. თუ კი ინფორმაციები სრულად არ ემთხვევა, მაშინ პაკეტი უარყოფილი იქნება.
6. ბრაუზერი მიღებულ მონაცემებს გამოიტანს მონიტორზე.

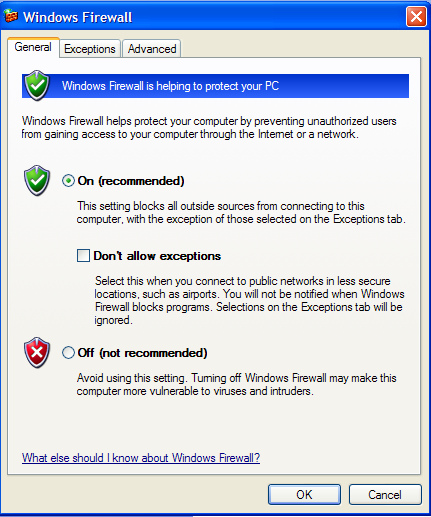
**ბრანდმაუერის ჩართვა და გამორთვა**

ბრანდმაუერ ვინდოუსის უტილიტა შეიძლება გავხსნათ რამდენიმე გზით:

* Start » Control Panel » (თუ კი Control Panel-ს აქვს კატეგორიების სახე) » Network and Internet Connections » Windows Firewall.
* Start » Control Panel » (თუ კი Control Panel-ს აქვს კატეგორიების სახე) » Security Center » Windows Firewall.
* Start » Control Panel » Network Connections » Network task (ქსელური ამოცანები) სექციაში დააჭირეთ Change Windows Firewall Settings (ვინდოუს ბრანდმაუერის პარამეტრების შეცვლა).
* Start » Control Panel » Network Connections » გაამუქეთ აქტიური ინტერნეტ კავშირის ლოგო» მაუსის მარჯვენა ღილაკით გამოიძახეთ კონტექსტური მენიუ» Properties » Advanced » Windows Firewall-ია სექციაში აირჩიეთ Settings.
* ბრძანების სტრიქონში აკრიფეთ firewall.cpl და დააჭირეთ ok.

შევნიშნოთ, რომ Network Connections -ში თუ კი View (სახე, ფორმა) -ში ავირჩევთ Thumpnails (ფურცელთა ესკიზი), Tiles (ფილები) და Icons (ნიშნები) მაშინ ბოქლომის ნიშანი მომქმედ შეერთებების თავზე მიუთითებს იმას, რომ ეს შეერთებები არიან ბრანდმაუერის კონტროლის ქვეშ.

რა გზითაც არ უნდა შევიდეთ Windows Firewall-ში მივიღებთ შემდეგ ფანჯარას, ნაჩვენებს ნახატი 6.2 -ზე



ნახატი 6.2. Windows Firewall-ს ფანჯარა

ბრანდმაუერის ჩასართავად მონიშნეთ **On** (ჩართვა). რომ გამორთოდ ბრანდმაუერი მონიშნეთ **Off** (გამორთვა). ბრანდმაუერის გამორთვა მაშინაა დასაშვები, თუ კი არსებობს, მეორე - სხვა, გარე ბრანდმაუერი - ქსელთაშორისი ეკრანი.

**მთელი შემავალი ტრაფიკის გამორთვა**

Windows Firewall-ის ფანჯარაში ჩანართში General (ზოგადი, საერთო), არსებული ოფცია **Don’t Allow Exceptions** ( არაა დაშვებული გამონაკლისები) წარმოადგენს უსაფრთხოების დამატებით ზომას, ხარისხს. თუ კი იგი არის მონიშნული, მაშინ ის ტრაფიკები (მარშრუ­ტები - გზები), რომლებიც ჩვეულებრივ რეჟიმში მოქმედებისას იყვნენ დაშვებული გამო­ნაკლისის სახით, ამჟამად იქნება სრულიად აკრძალული - შეუძლებელი. ამ რეჟიმის ჩარ­თვა რეკომენდებულია მაშინ როცა საჭიროა გარედან მომავალი შეტევებისგან დამატებითი თავდაცვა, მაგალითად, როცა თქვენ სარგებლობთ საერთო უსადენო ქსელით ან როცა თქვენ იცით, რომ თქვენი კომპიუტერი იმყოფოფება ჰაკერული შეტევის ობიექტი.

შევნიშნოთ, რომ Don’t Allow Exceptions ოფციის მონიშვნა არ ნიშნავს ინტერნეტიდან გამორ­თვას, რადგანაც Windows Firewall არ ბლოკავს კომპიუტერიდან გამომავალ ტრაფიკს, ამ­დენად ყველა გამომავალი ჩართვა, მათ შორის ნებადართული თუ ჯაშუშური, შესაძლე­ბელია და აკძალვას არ ექვემდებარება.

**Windows Firewall გამორთვა ცალკეული ჩართვებისათვის (შეერთებებისათვის)**

როგორც წესი, Windows Firewall-ის კონტროლის ქვეშაა ყველა ქსელური შეერთებები (ჩარ­თვები) რათა გამოირიცხოს არასასურველი ტრაფიკები. მაგრამ ზოგიერთ შემთხვევაში შე­იძლება დადგეს საჭიროება გამორთულ იქნეს ეს დაცულობა, მხოლოდ ერთი ან რამდენიმე შეერთებისათვის, ხოლო დანარჩენებისთვის კი იქნეს შენარჩუნებული. ამ მიზნის მისაღ­წევი ალგორითმია:

1. Windows Firewall-ის ფანჯარაში გადადით ჩანართ Advanced (დამატებით).
2. Network Connections Settings სექციაში მოხსენით მონიშვნა იმ შეერთების გასწვრივ, რომლისათვისაც აღარ გსურთ ბრანდმაუერის კონტროლი.

**ქსელთაშორისი ეკრანის პატამეტრების შერჩევა**

Windows Firewall მოგცემთ საშუალებას თქვენთან კონტაქტი დაამყაროს მხოლოდ იმ საიტებმა და მომხმარებლებმა ვისაც თქვენ გაუგზავნეთ მოთხოვნა. მაგრამ ზოგჯერ საჭიროა ნება დაერთოს სასარგებლო საიტებს თქვენთან კავშირის თავისუფალი დამყარებისა. ეს შესაძლებელი თუ კი Windows Firewall -ის პარამეტრებს შესაბამისად შევარჩევთ.

**შემავალი კავშირის დამყარების ნების დართვა Windows ბრაუნდმაუერით.**

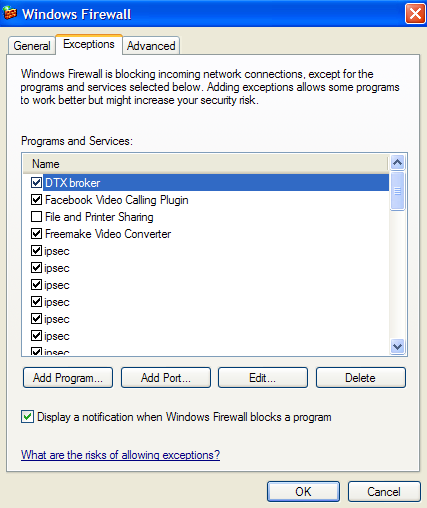
იმისათვის, რომ ჩავრთოთ, ნება მივცეთ, შემავალ კავშირებს კონტაქტის დამყარებისა, საჭიროა ერთ-ერთი გზა ავირჩიოთ:

* დავჭიროთ ღილაკს Unblock (განბლოკება), როცა Windows Firewall პირველად აღმო­აჩენს, რომ გარე წყარო ცდილობს დაამყაროს კავშირი თქვენს კომპიუტერში არსე­ბულ პროგრამას­თან. ჩუმათობის პრინციპით, უმეტესი პროგრამები იბლოკება. რო­ცა ვაჭერთ ღილაკს Unblock, მაშინ Windows დაამატებს ამ პროგრამას გამონაკლისთა გლობალურ სიას და მისცემს უფლებას მიიღოს მონაცემები გარე წყაროდან ნების­მიერი პორტის საშუალებით.
* შესაძლებელია ხელითაც დაამატოთ პროგრამა გამონაკლისთა გლობალურ სიაში. როცა ამას გავაკეთებთ, მაშინ Windows მოგვცემს უფლებას მიიღოს შემომავალი ტრაფიკი გარე წყაროდან ნების­მიერი პორტის საშუალებით.
* შესაძლებელია ხელითაც დაამატოთ გლობალურ სიაში გამონაკლისი პორტი. ეს დამა­ტება ნებას დართავს ბრანდმაუერს მიიღოს შემომავალი ტრაფიკი გარკვეულ პორტში, მიუხედავად იმისა, თუ რა შეერთება-კავშირი იქნა გამოყენებული.
* შესაძლებელია გახსნათ პორტი კონკრეტულ ქსელურ შეერთებაში. ამით შესაძლებელია ავირჩიოთ ნებისმიერი ვარიანტი წინასწარ განსაზღვრული სამსახურების სიიდან, ცნობილ პორტებზე (მაგ, ვებ-სერვერი) ანაც მომხმარებლის აღწერილობა იმ სამსახურებისთვის, რომლებიც მიითებენ ტრაფიკს მხოლოდ გარკვეული შეერთებისათვის.

იმისათვის, რომ ვნახოთ ამ დროისთვის როგორ გამოიყურება გამორჩეულთა სია, ვიმოქმედოთ შემდეგნაირად:

Start » Control Panel » Windows Firewall » Exception.

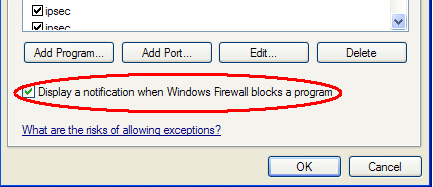
იხილეთ ნახატი 6.3.



ნახატი 6.3. გამონაკლისთა სია

***გამონაკლისი პროგრამებისთვის***

თუ კი **Windows Firewall**-ის ფანჯარის გამონაკლისთა ჩანართში მონიშნულია **Display a notifications when Windows Firewall blocks a program**, მაშინ ყოველი მცდელობა რაიმე



**ნახატი 6.4. ”უცხო” პროგრამების ბლოკირების მონიტორზე გამოტანის ჩართვა**

პროგრამის მოთხოვნა სისტემაში შეღწევისა, კონკრეტულად კი იმ პროგრამების მოთხოვნები, რომლებიც არ არიან გამონაკლისთა სიაში შეტანილნი, ბლოკირდება ბრანდმაუერის მიერ და გამოვა შეტყობი­ნება მონიტორზე შემდეგი სახით - Windows Security Alert

.

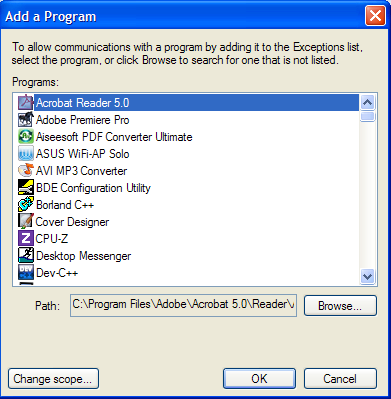
**ნახატი 6.5. ბლოკირებული პროგრამის შეტყობინება**

ნახ. 6.5 მოცემულ შეტყობინებას შეიძლება მოყვეს სამი ქმედება:

1. თუ კი დააჭერთ ღილაკს Keep Blocking (Блокировать) – ბლოკირება, მაშინ Windows Firewall არ შექმნის ახალ გამონაკლისს. ანუ, პროგრამა ვერ მიიღებს შემომავალ კავშირებს და შესაძლებელია მან არაკორექტულად დაიწყოს მუშაობა.
2. თუ კი დააჭერთ ღილაკს Unblock (Разлокировать) – განბლოკირება, მაშინ Windows Firewall შექმნის ახალ გამონაკლისს ამ პროგრამისთვის. ამის შემდეგ გაიღება პროგრამის მოლოდინის პორტი შემავალი კავშირისთვის.
3. თუ კი დააჭერთ ღილაკს Ask Me Later (Отложить) – მოგვიანებით, მაშინ Windows Firewall შექმნის ახალ გამონაკლისს ამ პროგრამისთვის თუმცა კი არ ჩართავს ამ რეჟიმს, ანუ ამ პროგრამის სახელი შეტანილი იქნება გამონაკლისთა სიაში, მაგრამ იგი არ იქნება მონიშნული

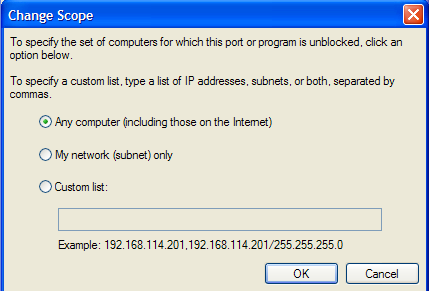
შესაძლებელია გამონაკლისთა სიაში პროგრამის შეყვანა წინასწარ, Windows Security Alert შეტყობინების გარეშეც. ამისთვის საჭიროა Windows Firewall-ის ფანჯარის Exception ჩანართში:

1. დავაჭიროთ ღილაკს Add Program (დაამატე პროგრამა). გაიხსნება დიალოგური ფანჯარა Add A Program (პროგრამის დამატება) იხ. ნახ. 6.6.



**ნახატი 6.6. პროგრამის დამატება**

1. ამოირჩიეთ პროგრამა (ანუ გაამუქეთ) მოცემული სიიან, მაგრამ თუ კი სასურველი პროგრამა Programs სიაში არ არის მაშინ ღილაკი Browse (მიმოხილვა) -ს დაჭერით ვიპოვოთ იგი კომპიუტერში.
2. დააჭირეთ ღილაკს Change Scope (შეცვალეთ არე) რათა გამოვიყვანოთ დიალოგური ფანჯარა, ნახატ 6.7 -ზე.



**ნახატი 6.7 არის შეცვლა**

IV. ამოვირჩიოთ კომპიუტერების ის დიაპაზონი, რომელთათვისაც გსურთ ნება დართოთ ეს გამონაკლისი - ანუ ნება დართოთ შემომავალ კავშირებს

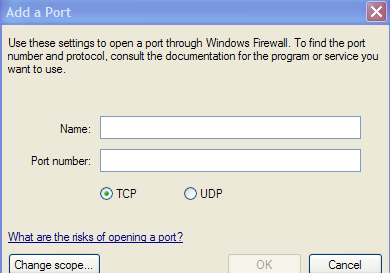
* **Any Computer** (ნებისმიერი კომპიუტერი) ნიშნავს, რომ ნებისმიერი კომპიუტერი თქვენი ლოკალური ქსელიდან თუ ინტერნეტიდან
* **My Network (Subnet) Only** (მხოლოდ ლოკალური ქსელიდან [ქვექსელიდან]) ნებას რთავს შემომავალ კავშირებს მხოლოდ იმ კომპიუტერებიდან, რომლებიც ლოკალურ ქსელშია.
* **Custom List** (განსაკუთრებული სია) - იძლევა საშუალებას მივუთითოთ ერთი ან რამდენიმე კომპიუტერი მათი IP-მისამართებით

V. დააჭირეთ OK.

ცხადია, რომ თუ კი გსურთ გამონაკლისთა სიიდან ამოიღოთ რომელიმე პროგრამა, საჭიროა მისი გამუქება - გამოყოფა და შემდეგ Delete -ს დაჭერა, ან Cancel ღილაკის დაჭერა გამონაკლისთა ჩანართში.

**როგორ გავხსნათ პორტი**

არის კიდევ ერთი საშუალება შემავალი კავშირებისთვის გამონაკლისის შეჰმნისა - ესაა პორტის გახსნა. თუ კი თქვენთვის საინტერესო პროგრამის ინსტრუქციაში არის მითითებული, თუ რო­მელი პორტი უნდა იყოს გამოყენებული მისთვის, მაშინ შესაძლებელია ამ პორტის გასახსნელად მოვიქცეთ შემდეგნაირად.

1. Windows Firewall-ის ფანჯარაში გადავიდეთ Exception ჩანართში.
2. დააჭირე ღილაკს Add Port (დაამატე პორტი). გაიხსნება დიალოგური ფანჯარა Add A Port (პორტის დამატება). იხ. ნახ. 6.7 პორტის დამატების დიალოგური ფანჯარა 

**ნახატი 6.7 პორტის დამატების დიალოგური ფანჯარა**

III**.** ამ დიალოგურფანჯარა ავირჩიოთ ჩანაწერები

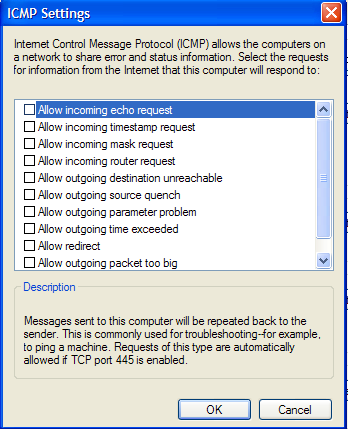
* Name (სახელი) ველში ჩაწერეთ აღმწერი სახელი პროგრამის ან სამსახურისთვის.
* Port Number (პორტის ნომერში0 ჩაწერეთ პორტის ნომერი, რომელიც მოითხოვება ამ პროგრამის ან სამსახურისთვის.
* ამოარჩიეთ TCP ან UDP პროტოკოლები ( ეს ის პროტოკოლებია რომელსაც პროგრამა ან სამსახური იყენებს.

IV. დააჭირეთ ღილაკს Change Scope (შეცვალეთ არე) რათა გამოვიყვანოთ დიალოგური Change Scope, და ამოირჩიეთ იმ კომპიუტერების დიაპაზონი, რომლებისთვისაც გინდათ პორტის ან პორტების გახსნა. იხილე ნახატი 6.7.

**ICMP პარამეტრების მითითება**

TCP და UDP ინტერნეტში, მონაცემთა გაცვლის ყველაზე პოპულარული პროტოკოლებია. მაგრამ ბრძანების სტრიქონის ზოგიერთი ინსტრუმენტები და გამოყენებითი პროგრამები, იმ მონაცემების გადასაცემათ, რომლებიც შეეხებიან მდგომარეობას, მართვას და კომპიუტერთა შორის შეცდომებს, სარგებლობენ ICMP (Internet Control Message Protocol - ინტერნეტ შეტყობინებების მართვის პროტოკოლი) პროტოკოლით. ამასთან ხარვეზენის დაფიქსირებისა და გადაწყვეტის ისეთი უტილიტები, როგორებიცაა **Ping** და **Tracert** , ასევე ICMP პროტოკოლს გამოიყენებენ. რადგანაც ICMP-ს არ გადააქ მონაცემები ის არ შეიძლება გამოყენებულ იქნეს უშუალოდ კომპიუტერში შესაღწევად და ინფორმაციის მიტაცებაში, მაგრამ მიუხედავათ ამისა ხაკერები იყენებენ ICMP შეტყობინებებს ქსელების სკანირებისთვის, ტრაფიკის გადამისამართებისა და DoS-შეტევების განსახორციებლად.

ჩუმათობის პრინციპით ბრანდმაუერი - Windows Firewall ბლოკავს უმეტეს შემავალ და გამომავალ ICMP შეტყობინებებს. მაგრამ ბრანდმაუერში არის საშუალება ამა თუ იმ ICMP შეტყობინებების გატარების ნების დართვისა. ამისთვის შევიდეთ Windows Firewall -ის დიალოგურ ფანჯარაში და ამოვირჩიოთ ჩანართი Advanced (დამატებით), რომლის ICMP სექციაში ვაჭერთ ღილაკს ICMP Setting (ICMP პარამეტრები). გაიხსნება ICMP Setting ფანჯარა. იხილე ნახატი 6.8.



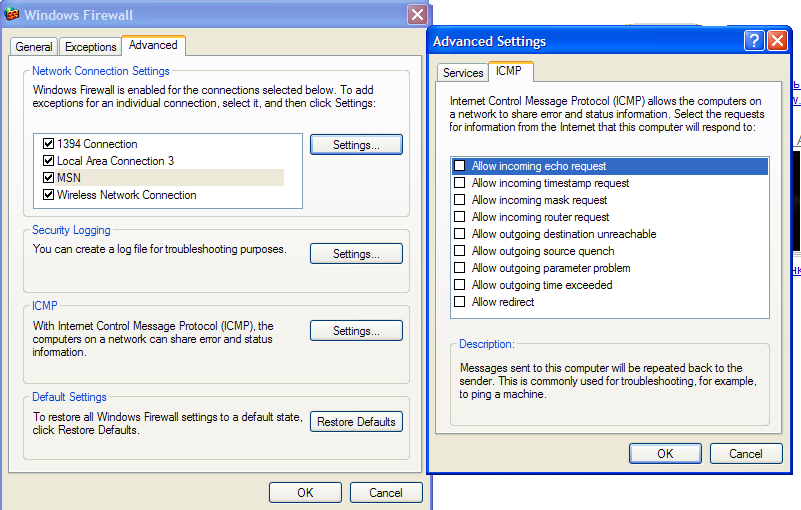
**ნახატი 6.8. ICMP პარამეტრების ფანჯარა**

ICMP Setting -ში შესაძლებელია იმ ოპციების მონიშვნა რომელთა დაშვებაც გსურთ - რათა ბრანდმაუერმა ისინი გაატაროს. ქვემოთ მოყვანილია ცხრილი რომელიც აღწერს ამ ოფციებს. ხარვეზისა მოძიებისა და მისი გამოსწორების ოფციის გარდა სხვა ოფციების ცართვა სერიოზული განსჯის საკითხი უნდა იყოს, რადგანაც ისინი კომპიუტერის უსაფრთხოებას ამცირებენ.

ცხრილი 6.1.

|  |  |
| --- | --- |
| ოფციები | აღწერა |
| Allow incoming echo request (შემავალი ექოს მოთხოვნის დაშვება) | თუ ჩავრთავთ ამ ოფციას, მაშინ კომპიუტერი უპასუხებს **Ping -**ს(ექო) მოთხოვნას. |
| Allow incoming timestamp request (დროის შტამპის შემავალი მოთხოვნის დაშვება) | თუ ჩავრთავთ ამ ოფციას, მაშინ კომპიუტერი ადასტურებს მითითებულ დროში მიღებული მოთხოვნას და ამის შესახებ იძლევა დამადასტურებელი შეტყობინებით |
| Allow incoming mask request (მასკის შემავალი მოთხოვნის დაშვება) | თუ ჩავრთავთ ამ ოფციას, მაშინ კომპიუტერი ელოდება და პასუხობს იმ მოთხოვნაზე, რომელიც შეეხება იმ ქსელს, რომელსაც იგი არის მიერთებული. |
| Allow incoming router request (მარშრუტუზატორის შემავალი მოთხოვნის დაშვება) | თუ ჩავრთავთ ამ ოფციას, მაშინ კომპიუტერი უპასუხებს იმ ინფორმაციის მოთხოვნაზე, რომელიც მისი მარშრუტუზაციის ცხრილს ეხება |
| Allow outgoing destination unreachable (”გამომავალი დანიშნულების მიუწვდომლობის” დაშვება) | თუ ჩავრთავთ ამ ოფციას, მაშინ კომპიუტერი უპასუხებს შეცდომის შემცველი შეტყობინებით იმის შესახებ, რომ კომპიუტერთან ან ქსელთა მოხდა წარუმატებელი შეერთების მცდელობა |
| Allow outgoing source quench (გამომავალი შეტყობინებების წყარის სიჩქარის შემცირების დაშვება) | თუ ჩავრთავთ ამ ოფციას, მაშინ კომპიუტერს ეძლევა უფლება გააგზავნოს შეტყობინება კომპიუტერი-წყაროს სიჩქარის შემცირებისა. შეტყობინება კომპიუტერი-წყაროს სიჩქარის შემცირებისა ეს არის მოთხოვნა იმისთვის, რომ კომპიუტერი-მიმღები ვერ ასწრებს მიღებული პაკეტების დამუშავებას. |
| Allow outgoing parameter problem ( ”გამომავალი პარამეტრის პრობლემის” დაშვება ) | თუ კი თქვენი კომპიუტერი იღებს მონაცემებს არაკორექტული სათაურით, იგი უარყოფს ამ მონაცემებს. ამ ოფციის ჩართვისას კი კომპიუტერი წყაროს გაუგზავნის შეტყობინებას არსებული შეცდომის შესახებ |
| Allow outgoing time exceeded ( გამომავალი დროის გადაჭარბების დაშვება) | ყველა პაკეტს აქვს ე.წ. ”სიცოცხლის დრო”, რომლის შემდეგ იგი აღარ აღიქმება. ამიტომ როცა მონავემთა მისაღებად უფრო მეტი დროა საჭირო ვიდრე დასაშვებია, კომპიუტერს აღარ შეუძლია ფრაგმენტირებული დეიტაგრამის აღდგენა და იგი ამ დეიტაგრამას უარყოფს. ამ ოფციის ჩართვისას კი კომპიუტერი წყაროს გაუგზავნის შეტყობინებას ”დრო ამოიწურა” |
| Allow redirect (გადამისამართების დაშვება) | თუ ოფცია ჩართულია, მაშინ კომპიუტერს შეუძლია გასცეს პასუხი მოთხოვნას - მონაცემთა გადამისამართებისა სხვა შლუზზე, |
| Allow outgoing packet too big (”გამომავალი პაკეტი ძალზე დიდია” დაშვება) | ეს ოფცია გამოიყენება მხოლოდ ქსელური ჩაღტვებისას, რომლებიc IPv6 პროტოკოლს (დამისამართებას) გამოიყენებენ. ამ ოფციის ჩართვისას ძალძე დიდი მონაცემების უარყოფის ინფორმაცია გაეგზავნება წყაროს. |

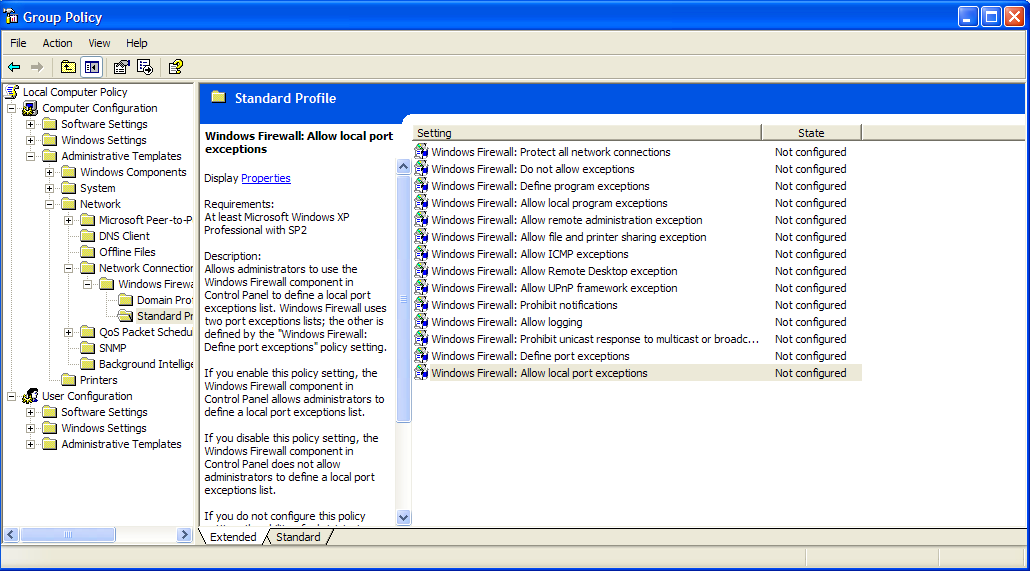
აღწერილი სქემა მუშაობს ყველა ქსელური ჩართვებისთვის. თუ კი თქვენ გსურთICMP შეტყობინებები გააქტიუროთ ცალკეული ქსელური კავშირებისთვის, მაშინ Windows Firewall -ის დიალოგურ ფანჯარაში ამოვირჩეულ ჩანართში - Advanced (დამატებით),სექციაში Network Connection Setting -ში ვირჩევთ (ვამუქებთ) ქსელურ კავშირს და ვაჭერთ ღილაკს Setting, გახსნილ Advanced Setting ფანჯარაში ვირჩევთ ჩანართს ICMP. იხილე ნახატი 6.9.

****

**ნახატი 6. 9. ცალკეული კავშირისთვის ICMP პარამეტრების ჩართვა**

***ბრანდმაუერის მართვა ჯგუფური პოლიტიკის საშუალებით***

Windows XP Professional -ში ჯგუფური პოლიტიკით შეიძლება ბრანდმაუერის მართვა. თანაც ჯგუფური პოლიტიკიდან შესაძლებელია ისეთი მოქმედებების შესრულება. რომელიც მიუწვდომელია Control Panel-დან. შევიდეთ ჯგუფურ პოლიტიკაში: ბრძანების სტრიქონში ავკრიფოთ gpedit.msc, შემდეგ Computer Configuration » Administrative templates » Network » Network Connections » Windows Firewall. გამოჩნდება ორი ფაილი: Domain Profile და Standard Profile. იხილეთ ნახატი 6.10. ეს ორი ფაილი იძლევა საშუალებას ცალ-ცალკე ავაწყოთ პარამეტრები, როცა თქვენი კომპიუტერი (როგორც წესი ლეპტოპი) ჩართულია კორპორატიულ ქსელში ან როცა ჩართულია ჩვეულებრივ ქსელში. თვითოელი ოფციის მნიშვნელობა აღწერილია გახსნილ ოფციაში.

****

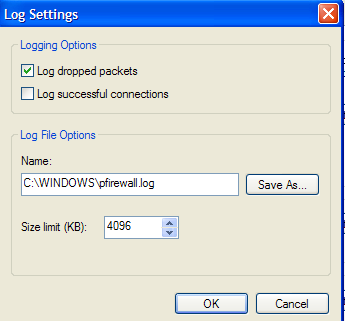
**ნახატი 6.11. ბრანდმაიერის მართვა ჯგუფური პოლიტიკიდან**

**ბრანდმაუერის ჟურნალის პარამეტრების შერჩევა.**

ბრანდმაუერს შეუძლია აწარმოოოს აღრიცხვა ინტერნეტთან წარმატებული თუ წარუმატე­ბელი კონტაქტების დამყარებისა. ეს მონაცემები შეიძლება ჩაიწეროს სპეციალურ ჟურ­ნალ­ში, თანაც აქ აღნიშნული იქნება შემომავალი კავშირების დამყარების მსურველ კომპი­უტერთა IP-მისამართები. ამ მისამართებით კი შეგვიძლია დავადგინოთ ის კომპიუტე­რები რომლებიდანაც ხდება ჰაკერული შეტევების ორგანიზება. ამ მისამართების გადაცემა შე­იძლება პროვაიდერისთვის, ხოლო მას კი ხელეწიფება ამ ჰაკერის ინტერნეტ მომსახურე­ბის შეჩერება, ანაც მისცეს ამ საქმეს ს/ს მსვლელობა.

იმისთვის რომ ვაწარმოოთ ბრანდმაუერის ჟურ­ნალი საჭიროა:

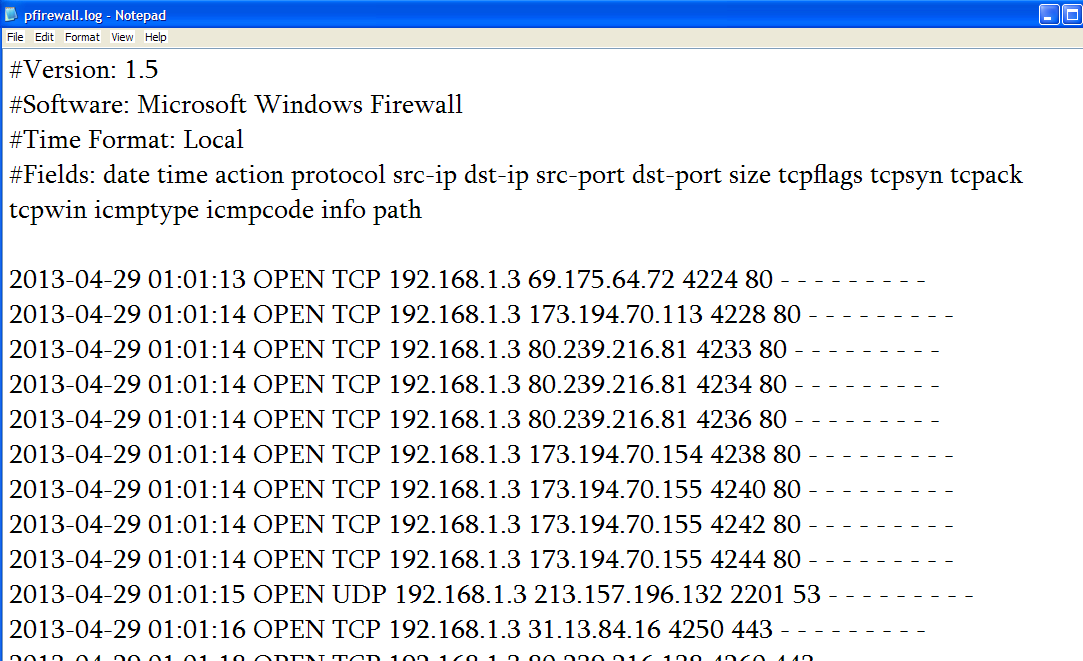
1. Control Panel-ში გავხსნათ Windows Firewall ფანჯარა.
2. დიალოგურ Windows Firewall ფანჯარაში გავხსნათ Advanced ჩანართი.
3. Security Logging (უსაფრთხოების ჟურნალის წარმოება) სექციაში დავაჭიროთ ღილაკს Settings (პარამეტრები).
4. აღნიშნეთ Log dropped packets ( ჩაწერეთ შეჩერებული პაკეტები). იხილე ნახატი 6.12.
5. ამოირჩიეთ საქაღალდესა და ფაილის სახელი. ჩუმათობით ბრანდმაუერ Windows-ის ჟურნალს ეწოდება Pfirewall.log და მოთავსებულია საქაღალდეში %SystemRoot% - ეს ციცტემური დისკია, მაგრამ სურვილის შემთხვევაში შეიძლება მივუთითოთ სხვა საქაღალდე და ფაილი (გამოიყენეთ Save as... ღილაკი).
6. ამოირჩიეთ ფაილის მაქსიმალური ზომა. ჩუმათობით ის 4096 კბაიტზე ნაკლებია.
7. შერჩეული პარამეტრების შესანახად დავჭიროთ ღილაკს ok.



**ნახატი 6.12. ბრანდმაუერის ჟურ­ნალის პარამეტრები**

**ბრანდმაუერის ჟურნალის შესწავლა**

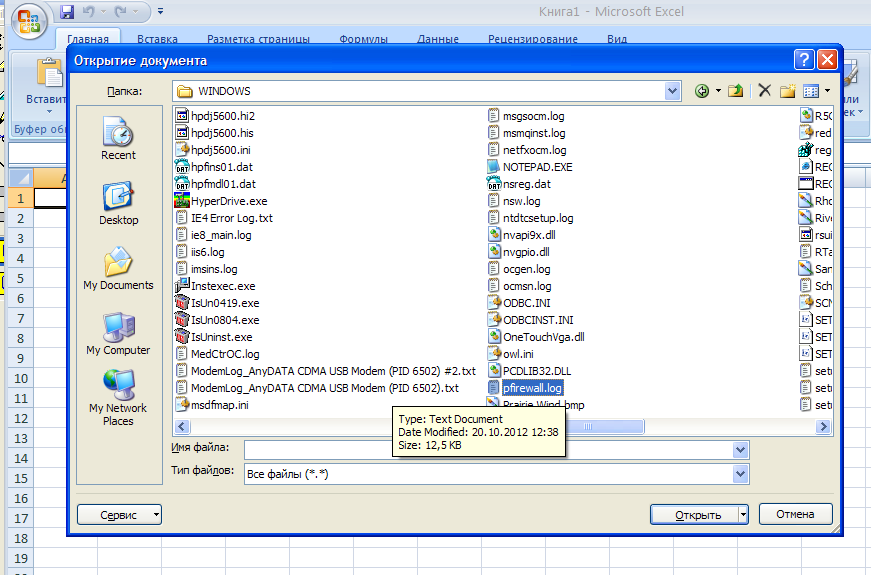
ბრანდმაუერის ჟურნალი ტექსტურ ფაილს წარმოადგენს (იხილე ნახატი 6.13), ამიტომ გაიხსნება ბლოკნოტის საშუალებით და მასში ყოველ სტრიქონში ჩაწერილია თითო მოვლენა, რომელიც ბრანდმაუერმა დაარეგისტრირა. მითითებულია დრო (date time), კონკრეტული პროტოკოლის აქტიურობა (action protocol); მიმღების ip მისამართი (src-ip); გამგზავნის ip მისამართი (dst-ip); მიმღების პორტი (src-port); გამგზავნის პორტი (dst-port); და კიდევ 9 პარამეტრი.

****

**ნახატი 6.13. ბრანდმაუერის ჟურნალი**

ბრანდმაუერის ჟურნალის შესწავლა გაჩილებით მოსახერხებელის, თუ კი მას ჩავწერთ Excel-ფაილში და მერე გამოვიყენებთ Excel -ში არსებულ საშუალებებს ჩანაწერების ანალიზისთვის. ბრანდმაუერის ჟურნალის Excel-ფაილში წარმოდგენისთვის ვიქცევით შემდეგნაირად:

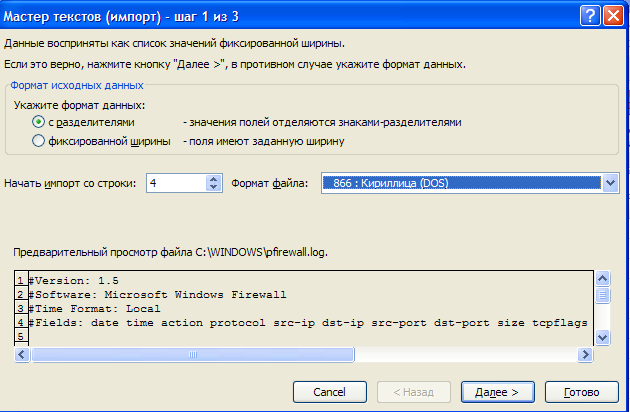
1. ჩავტვირთავთ Excel -ს და ვხსნით File » Open (ფაილი » გახსენი).
2. ფაილის ტიპის ველში (File Of Type) ავირჩევAll File Read Only, შემდეგ კი გადავალთ ბრანდმაუერის ჟურნალზე და მას გამოვყოფთ. იხილე ნახატი 6.14.



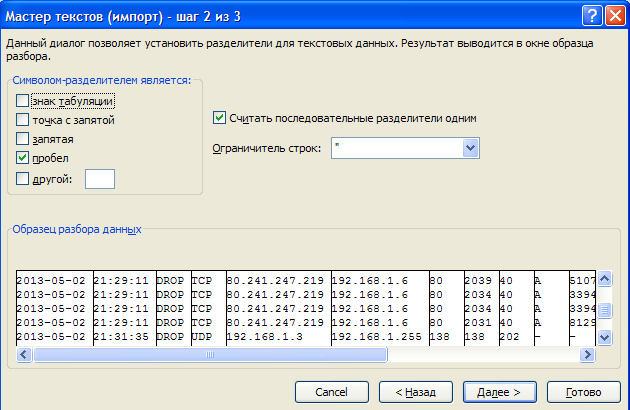
**ნახატი 6.14. ბრანდმაუერის ჟურნალის Excel-ფაილში გარდაქმნა**

თუ ბრანდმაუერი მუშაობს, და ეს როგორც წესი ასეა, Excel გამოიტანს შეტყობინ­ებას, რომ ფაილი ამ მომენტში გამოიყენაბა. ამიტომ, იმისთვის, რომ გავხსნათ ფა­ილი ვაჭერთ ღილაკს Read Only (მხოლოდ გავხსნათ). Exel გაუშვებს Tex Import Wizard-ს (ტექსტების იმპორტირების ოსტატს) რათა ტექსტური ფაილი გარდაიქნეს ელექტრონულ ცხრილში (Exel-ში).

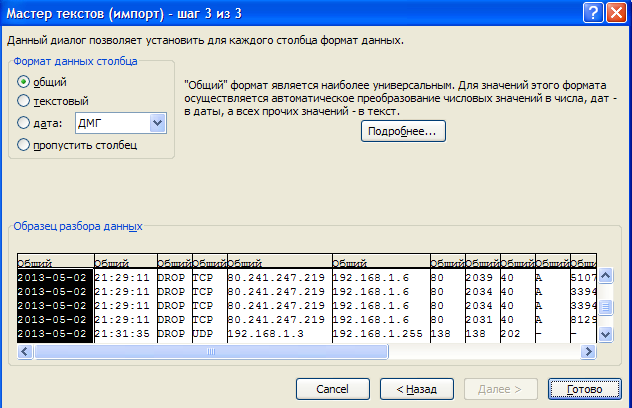
3. აირჩიეთ ვარიანტი Delimited (გამოყოფით - с разделением). დაიწყეთ იმპორტი მეოთხე სტრიქონიდან, რომელიც განსაზღვრავს ველთა სახელებს, ხოლო შემდეგ კი დააჭირეთ ღილაკს Next (შემდეგ - Далее).



4. Tex Import Wizard-ის (ტექსტების იმპორტირების ოსტატის) მეორე ნაბიჯია გამო­ყოფის სიმბოლოს არჩევა - ამიტომ ავირჩიოთ Space (ჰაერი -пробел) - ე.ი. მოვნიშ­ნოთ იგი და დავრწმუნდეთ, რომ მონიშნულია ასევე Treat Consecutive Delimiters As On ( ჩავთვალოთ მიმდებრობითი გამოყოფის სიმბოლოები ტოდორც ერთი). ცხრი­ლის სვეტები მიიღებს შემდეგ სახეს:



5. დავაჭიროთ ღილაკს Next (შემ­დეგ - Далее). ავაწყოთ ფაილის იმპორტის პროცესი, მაგრამ ეს პროცესი ჩუმათობის პრინციპითაც კარგად მიმდინარეობს რეჟიმ General (ზოგადი -Общий) -ში



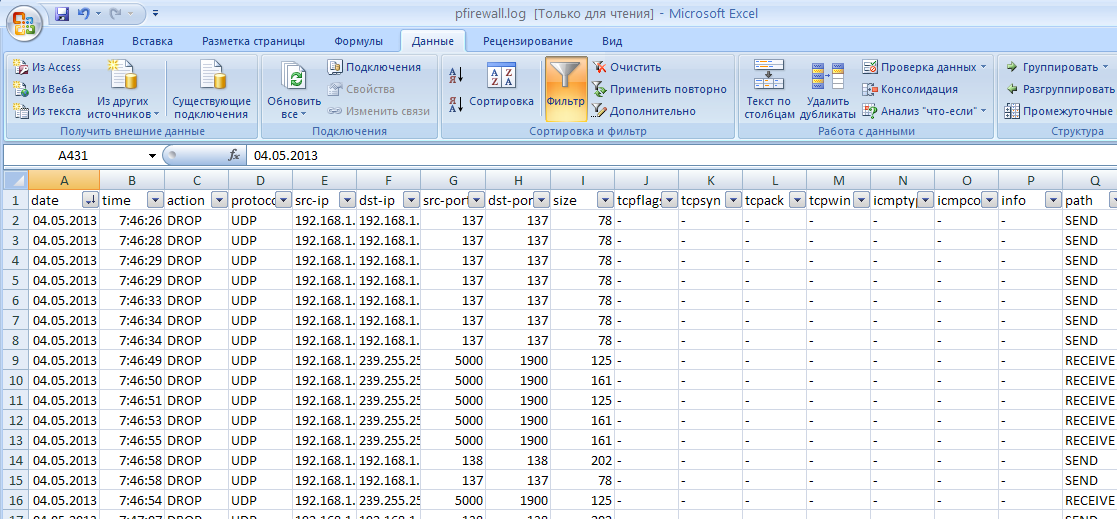
6. ვაჭერთ ღილაკს Finish (დაასრულეთ - Готово). იმპორტის დასრულების შემდეგ A1 უჯრაზე, რომელშიც უნდა იყოს სტრიქონი ”#Fields”, დააწკაპუნეთ მაუსის მარჯვენა ღილაკით, ამოირჩიეთ Delete (გააძევე - удалить), ხოლო შემდეგ Shift Cell Left (მარცხნივ ჩანაცვლებით - со сдвигом влево). დააჭირეთ Ok რათა სვეტების სათაურები სასურველ ველში აღმოჩნდეს. მაუსის მარჯვენა ღილაკით დააჭირეთ A2 უჯრაზე, ხოლო შემდეგ აირჩიეთ Entire Row (სტრიქონი -строку), რათა ამოვიღოთ ცარიელი სტრიქონი სათაურსა და მონაცემებს შორის. ნახატი 6.15

იმპორტირებული ფაილი შეიძლება შევინახოთ ახალ ფაილში ან გამოვიყენოთ Exel-ის სორტირებისა და ფილტრაციის შესაძლებლობა ფაილის ანალიზისთვის.

**რა დავუპირისპიროთ ჰაკერს**

ვთქვათ ბრანდმაუერის ჟურნალის ანალიზის შემდეგ აღმოვაჩინეთ რომ ჩვენი კომპიუტერზე ხდე­ბა ჰაკერული შეტევები და ჩვენ დავაფიქსირეთ დამრღვევი-შემტევის IP -მისამართი. ჩვენ შეგვიძ­ლია მივადევნოთ თვალი მის ქმედებებს და ამის შესახებ შევატყობინოთ მის პროვაიდერს. პროვა­იდერების მხოლოდ მცირე რაოდენობა რეაგირენს არგუმენტირებულ მიმართვებზე, და მზად არი­ან დამრღვევის ბლოკირებისთვის. უმეტესი პროვაიდერი ვერ ართმევს თავს დიდი რაოდენობის საჩივრებს ინდივიდუალური მომხმარებლებისგან და არ პასუხობს მათ.

მაგრამ თუ კი პროვაიდერებს მიმართავს ორგანიზაცია DShield (<http://www.dshield.org>), რომელიც ფინანსდება გავლენიანი ინსტიტუტის SANS -ის მიერ და ახდენს კომპიუტერში უნებართვო შეჭ­რების ანგარიშების ანალიზს, მაშინ პროვაიდერი ითვალისწინებს მათ აზრს. ამიტომაც თქვენს მი­ერ დაფიქსირებული უნებართვო შეჭრების ანგარიშები გააგზავნეთ DShield -ში. რა თქნა უნდა შე­საძლებელია მიმართოთ სამართალდაცავ ორგანოებს.



**ნახატი 6.15. ბრანდმაუერის ჟურნალი Exel - ფაილში**

როგორც წესი, შემოჭრის შესახებ მიღებული შეტყობინებისას, თქვენ უნდა მოიქცეთ შემდეგნაირ­ად:

* მოახდინეთ სწრაფი რეაგირება. ხშირად, შემოჭრის ფაქტების აღმოჩენა ძნელდება, თუ კი სამართალდამცავ ორგანოებისადმი მამართვამდე გადის დიდი დრო.
* თუ კი თქვენ არა ხართ დარწმუნებული, თუ რა ქმედებები უნდა განახორციელოთ, ნუ და­ასრულებთ სისიტემურ პროცესებს და ფაილებზე მანიპულაციებს. ამან შეიძლება წაშალოს შემოჭრის კვალი.
* სამართალდამცავებთან კავშირისთვის გამოიყენეთ ტელეფონი ან ის კომპიუტერი, რომე­ლიც არაა ჩართული კომპრომენტირებულ ქსელში. გაითვალისწინეთ, რომ ჰაკერი შეიძლე­ბა აკონტროლებდეს ელექტრონული ფოსტის ტრაფიკს.
* შექმენით იმ ფაილების კოპირები, რომელთა სეცვლა ან შემოგზავნა შეეძლო მომხდურს. ეს ხელს შეუწყობს იმის განსაზღვრას თუ საიდან და როგორ მოხდა შემოჭრა.
* ნუ შეხვალთ კონტაქტში სავარაუდო სამართალდამრღვევთან.