LABORATORIJSKA VEŽBA BR. 9

Mrežne barijere

- Upoznavanje sa zaštitom mrežnih okruženja primenom mrežnih barijera
- TCP/IP skup protokola
- IP adresiranje I uloga maske podmreža
- Principi rutiranja paketa i rada DNS
- Karakteristike Firewall-ova i filtriranje paketa

POTREBNA OPREMA

- Računar sa instaliranim Windows operativnim sistemom

TEORIJSKE OSNOVE

TCP/IP skup protokola

TCP/IP model čine sloj pristupa mreži, Internet sloj, transportni sloj I aplikacioni sloj. TCP/IP model ne specificira sloj veze podataka i fizički sloj, već na tom sloju koristi različite protokole i tehnologije – kao što je, na primer, *Ethernet*.

Internet sloj odgovara sloju mreže u OSI modelu. Na ovom sloju koriste se sledeći protokoli:
• **IP** (*Internet Protocol*) – adresiranje i rutiranje, tj rad sa fizičkim adresama i prenos informacija od računara do računara na osnovu logičkih adresa.
• **ICMP** (*Internet Control Message Protocol*) – IP protokolu obezbeđuje kontolne poruke, kao što je *Destination Unreachable*. Protokol ICMP najčešće se koristi za slanje ICMP ECHO paketa (ping) kojim se proverava da li je udaljeni računar dostupan,
• **ARP** (*Address Resolution Protocol*) – osim logičke adrese (IP), svaki mrežni uređaj karakteriše i fizička adresa (MAC) dužine 48 bitova. MAC adrese dodeljuju proizvođači mrežnih adaptera i one su, uslovno rečeno, nepromenljive. MAC adrese se koriste prilikom prenosa okvira podataka po fizički istoj mreži (kao što je Ethernet). Protokol ARP prevodi IP adrese u MAC adrese.

Transportni sloj preuzima podatke s višeg nivoa, po potrebi segmentira podatke u datagrame ili uspostavlja virtuelne veze i prenosi podatke do odredišta koristeći usluge Internet sloja. Na transportnom sloju koriste se:
• **TCP** (*Transmission Control Protocol*) – protokol koji obezbeđuje pouzdanu vezu između dva procesa, otkriva i ispravlja greške,
• **UDP** (*User Datagram Protocol*) – protokol koji ne uspostavlja virtuelne veze niti obezbeđuje mehanizam za detekciju grešaka.

Aplikacioni sloj omogućava aplikacijama, odnosno korisnicima da pristupe servisima Internet mreže. Primeri protokola aplikacionog sloja su:
• HTTP (*HyperText Transport Protocol*) – pristup Web stranicama,
• FTP (*File Transport Protocol*) – prenos datoteka,
• POP3 (*Post Office Protocol v3*) – dolazeća pošta,
• SMTP (*Simple Mail Transport Protocol*) – odlazeća pošta,
• DNS (*Domain Name System*) – prevođenje imena u IP adrese.

IP adresiranje

Svaki računar i ruter na Internetu ima svoju jedinstvenu IP adresu (ili više IP adresa). **IP adrese** su 32-bitne, sastoje se od 4 okteta i obično se predstavljaju u decimalnoj notaciji s tačkom (na primer: 192.198.3.1). Svaka IP adresa ima dva dela:
• deo koji predstavlja adresu IP mreže, isti za sve računare na jednoj IP mreži
• deo koji predstavlja adresu računara, jedinstven za svaki računar na istoj IP mreži.
Na osnovu broja okteta koji pripadaju adresi mreže, odnosno adresi računara, IP adrese se dele u klase A, B, C, D i E (za sada zanemarite klase D i E).
• **IP adrese klase A** počinju binarno sa 0. Prvi oktet predstavlja adresu mreže, a sledeća tri okteta adresu računara. Kako su adrese 0.x.y.z i 127.x.y.z rezervisane, IP adrese klase A nalaze se u opsegu od 1.0.0.0 do 126.255.255.255,
• **IP adrese klase B** počinju sa 10. Prva dva okteta pretstavljaju adresu mreže, a sledeća dva adresu računara. IP adrese klase B nalaze se u opsegu od 128.0.0.0 do 191.255.255.255,
• **IP adrese klase C** počinju sa 110. Prva tri okteta predstavljaju adresu mreže, a poslednji adresu računara. IP adrese klase C nalaze se u opsegu od 192.0.0.0 do 223.255.255.255.
U posebne slučajeve IP adresa spadaju:
• x.0.0.0 (adresa mreže u klasi A), x.y.0.0 (adresa mreže u klasi B), x.y.z.0 (adresa mreže u klasi C),
• 127.0.0.1 (adresa lokalne petlje, engl. *local loopback address*),
• x.y.255.255 (*broadcast* adresa mreže x.y.0.0 koja pripada klasi B).

Privatne i javne IP adrese
IP adrese se dalje mogu podeliti na javne i privatne.
• **Javne adrese** dodeljuje se mogu se koristiti na Internetu.
• **Privatne adrese** su namenjene mrežama koje nisu direktno povezane na Internet i ne mogu se koristiti na Internetu. U privatne adrese spadaju:
• 10.0.0.0 – 10.255.255.255,
• 172.16.0.0 – 172.31.255.255,
• 192.168.0.0 – 192.168.255.255.

Maska podmreže
Maska podmreže (engl. *subnet mask*) je 32-bitni broj koji se formira tako što se umesto bitova koji u IP adresi predstavljaju adresu mreže i podmreže stavi 1, a umesto bitova koji predstavljaju adresu računara stavi 0. Podrazumevane maske podmreže
• za mreže u klasi A: 255.0.0.0
• za mreže u klasi B: 255.255.0.0
• za mreže u klasi C: 255.255.255.0.
Adresa mreže se uvek navodi s maskom podmreže. Na primer, adresa mreže 192.168.10.0 u klasi C zapisuje se kao 192.168.10.0 255.255.255.0 ili 192.168.10.0/16 (broj 16 ukazuje na broj bitova koji pripadaju adresi mreže).

Podmreže

Podmreže su segmenti iste IP mreže koji komuniciraju preko rutera. Podmrežavanjem se smanjuje broj računara po segmentu IP mreža s velikim brojem računara. Svaka podmreža ima svoju jedinstvenu adresu, koja se formira tako što se određen broj bitova pozajmi iz dela IP adrese koji predstavlja adresu računara. Podmrežavanje se može jednostavno objasniti na primeru IP mreže u klasi C. U ovom slučaju, pozajmićemo tri bita iz četvrtog okteta. Ukoliko je adresa IP mreže 192.168.10.0, adrese podmreža će redom biti: 192.168.10.32/28, 192.168.10.64/28, 192.168.10.92/28, itd. Na ovaj način je napravljeno 8 segmenata, tj. osam podmreža čija je maska podmreže 255.255.255.248. U zavisnosti od toga da li protokol za rutiranje na ruteru koji spaja podmreže podržava VLSM (*variable length subnet masking*) ili ne, upotrebljivo je 6, odnosno 8 podmreža. Svaki segment sadrži 25=32 adrese. Prva adresa u svakom segmentu (na primer, 192.168.10.32) jeste adresa podmreže, a poslednja (192.168.10.63) – *broadcast* adresa za tu podmrežu. To znači da se na svakom segmentu može naći najviše 30 računara.

Rutiranje

Da bi se paket poslao računaru koji se nalazi na drugoj mreži, u mreži mora da postoji uređaj koji zna kako i gde isporučiti paket. Ovaj oblik isporuke paketa poznat je kao rutiranje. Ruter posmatra mrežu u celini i na osnovu toga donosi odluke o najboljoj putanji za slanje paketa. Izbor putanje se svodi na izbor sledećeg skoka u mreži. Postoji nekoliko tipova rutiranja: standardno rutiranje (svi paketi koji nisu namenjeni mreži šalju se na podrazumevani mrežni prolaz – engl. *default gateway*), statičko rutiranje (administrator specificira statičke rute u tabeli rutiranja) i dinamičko rutiranje.

Portovi

Osim IP adrese protokoli koriste i broj porta, to jest 16-bitnu vrednost koja dozvoljava više istovremenih veza ka jednom računaru. Ukupno ima 216 portova (0-65535). Servisi pokrenuti na nekom računaru osluškuju zahteve na određenim portovima, najčešće na rezervisanim portovima (0-1023). Procesi ostvaruju TCP i UDP komunkaciju pomoću takozvnih *socket*-a, koje se sastoje od IP adrese računara i broja porta i predstavljaju krajnje tačke komunikacije na transportnom sloju. Svaka veza se odnosi na određeni port, koji se dodeljuje određenom mrežnom servisu na korišćenje. Administratori mogu otvoriti ili zatvoriti određeni port, čime se omogućava, odnosno onemogućava uspostavljanje veze ka nekom tipu servisa.

Značajniji portovi su:
- 20, 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 – DNS
- 80 – HTTP
- 110 – POP3
- 119 – NNTP
- 143 – IMAP
- 443 – HTTPS

DNS

Korisnici se svakom računaru mogu obratiti putem IP adrese. To znači da korisnici koji koriste usluge 150 računara moraju znati 150 IP adresa. Da bi se komunikacija pojednostavila, koristi se sistem dodele logičkih imena IP adresama. Na primer, korisnici se mogu obratiti računaru čija je IP adresa 166.60.10.15 imenom mojserver, ukoliko je ime mojserver dodeljeno toj IP adresi. Imena računara pretvaraju se u IP adrese na osnovu upita koji klijenti šalju onom DNS serveru koji održava bazu podatka o imenima računara i mreža I odgovarajućim IP adresama.

Firewall

Mrežne barijere najčešće obavljaju sledeće funkcije:
- **Filtriranje paketa**. Zaglavlje paketa (izvorišna i odredišna adresa, broj porta) analizira se i upoređuje sa pravilima mrežne barijere. Zavisno od toga da li paket zadovoljava pravila, dozvoljava se prolaz paketa ili se paket odbacuje.
- **Prevođenje mrežnih adresa** (*engl. network adress translation*, NAT). Prevodi adrese računara u privatnoj mreži u jednu ili više javnih IP adresa i na taj način skriva identitet računara u lokalnoj mreži.
- **Proksi servisi** (engl. *proxy*). U najširem smislu, proksi (posrednički) server je sloj između lokalne i spoljašnje mreže koji omogućava većem broju računara da dele jednu vezu ka Internetu i skladišti, tj. kešira podatke kako bi se ubrzao pristup tim podacima sa lokalne mreže.

Mrežna barijera može biti hardver (na primer, Cisco PIX) ili softver (na primer, iptables ili Comodo Firewall).

Filtriranje paketa

Mrežne barijere analiziraju pakete i upoređuju ih s prethodno definisanim skupom pravila. Filtriranje je moguće na osnovu bilo kog dela zaglavlja paketa (slika 5.3), a većina filtara donosi odluku na osnovu:
- tipa protokola – na primer, mrežna barijera odbacuje sve ICMP ili IGMP pakete, a propušta sve TCP ili UDP pakete,
- IP adrese – prihvatanje ili odbijanje paketa na osnovu IP adrese najjači je oblik zaštite koji se može postići prostim filtriranjem paketa,

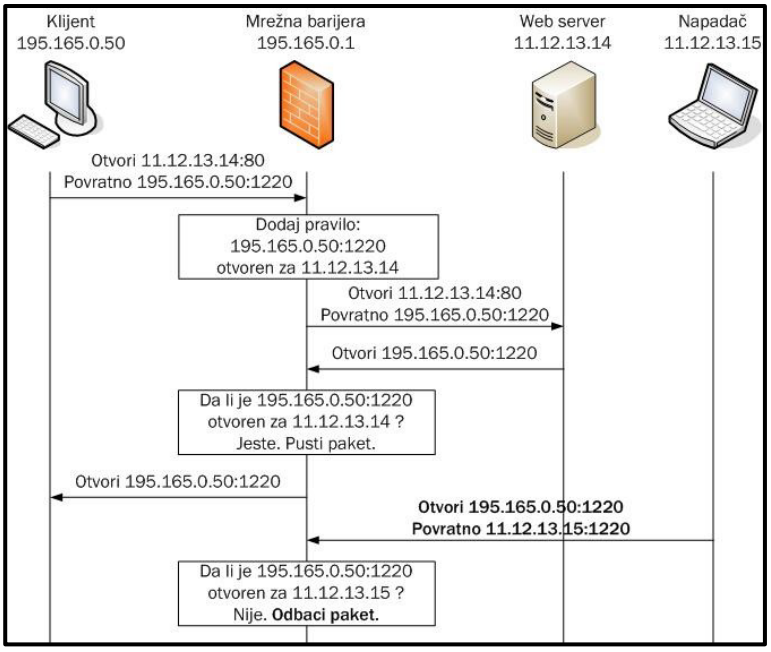
• TCP/UDP porta – na primer, svim računarima se može dozvoliti da pristupe TCP portu 80 (HTTP), dok je pristup TCP portu 22 (ssh) ograničen računarima koji pripadaju određenom opsegu IP adresa.
Na osnovu definisanih pravila i zaglavlja konkretnog IP paketa, filter paketa može da odluči da:
• prihvati paket,
• odbaci paket,
• odbaci paket i obavesti pošiljaoca da njegov paket nije prihvaćen.
Navodimo neke preporuke za konfigurisanje filtra paketa:
• eksplicitno zabranite sve osim onog što treba da bude dozvoljeno,
• napravite demilitarizovanu zonu za servere koji treba da budu dostupni računarima sa Interneta,
• zabranite sve ulazne veze, tj. pokušaje povezivanja spolja na računare u lokalnoj mreži (time se sprečava mogućnost povezivanja spolja na prethodno instalirane trojanske konje na računarima u lokalnoj mreži),
• zabranite računarima iz lokalne mreže da na Internet šalju pakete koji nisu zahtevi namenjeni Internet servisima (na primer, lokalni računar ne treba da šalje NetBIOS paket na Internet).
• zabranite odgovore na ICMP echo ili ICMP redirect pakete.

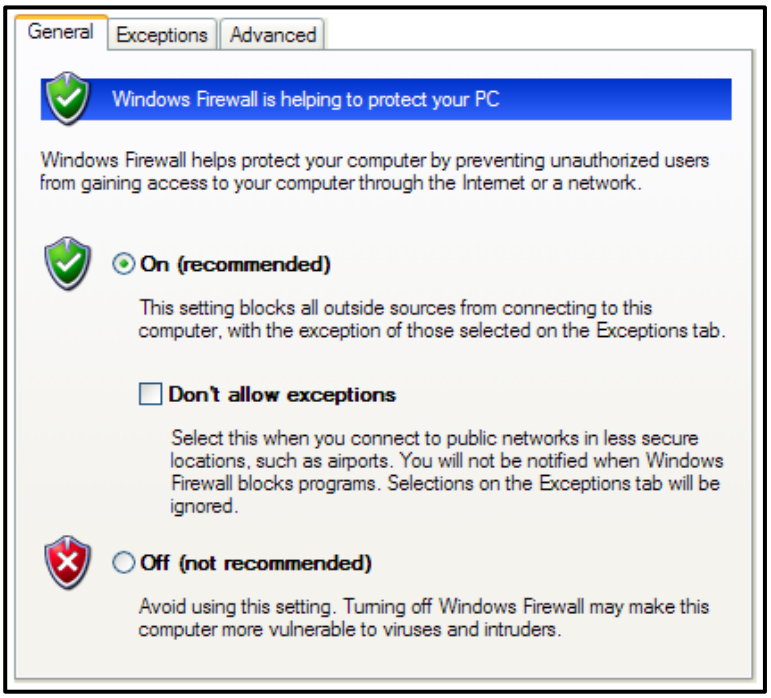
Stateless i statefull filteri

Postoje dve vrste filtera paketa: mrežne barijere bez uspostavljanja stanja (engl. *stateless firewall*) i mrežne barijere sa uspostavljanjem stanja (engl. *statefull firewall*).

• Stateless firewall odbacuje paket ukoliko nema dovoljno informacija šta bi s njim trebalo da uradi. Većina mrežnih barijera ovog tipa ostavlja portove veće od 1024 otvorene, kako bi omogućila slanje odgovora računaru koji je poslao zahtev. Trojanski konji mogu da iskoriste ove portove i to predstavlja ozbiljan sigurnosni propust.

• Statefull firewall prati stanje na mrežnom sloju (pamte zahteve za uspostavljanjem veze) i to koriste prilikom donošenja odluka. Karakteriše ih postojanje tabele stanja, tj. tabele u kojoj mrežna barijera vodi evidenciju o trenutnim stanjima veza. Barijere ovog tipa dozvoljavaju slanje odgovora ka računarima koji su uspostavili vezu, a potencijalne rupe ostaju otvorene samo onoliko dugo koliko je potrebno.
Rad mrežne barijere sa uspostavljanjem stanja ilustrovaćemo primerom (vidi sliku). Između klijenta koji pripada unutrašnjoj mreži (195.165.0.50) i servera koji pripada spoljašnjoj mreži (11.12.13.14) nalazi se mrežna barijera sa uspostavljanjem stanja, konfigurisana tako da propušta sav odlazeći saobraćaj.





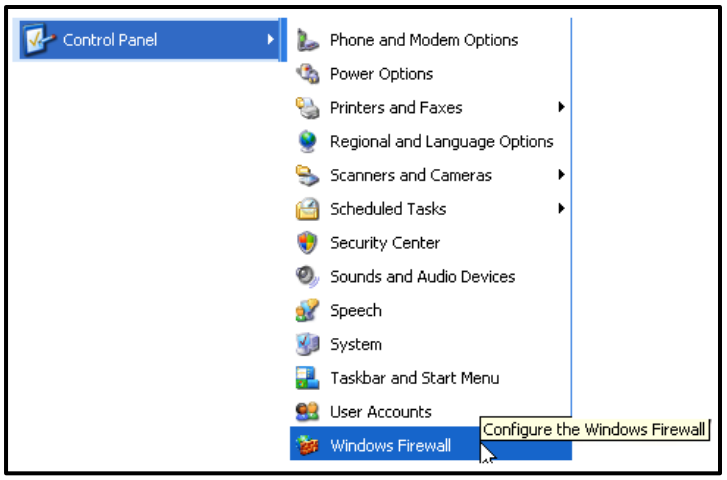
Firewall-ovi za Windows

Počev od Service Pack 2, Windows XP se isporučuje sa integrisanom mrežnom barijerom. Windows Firewall se pokreće pomoću odgovarajuće ikonice u Control Panelu; nakon pokretanja otvoriće se dijalog sa slike 5.8.

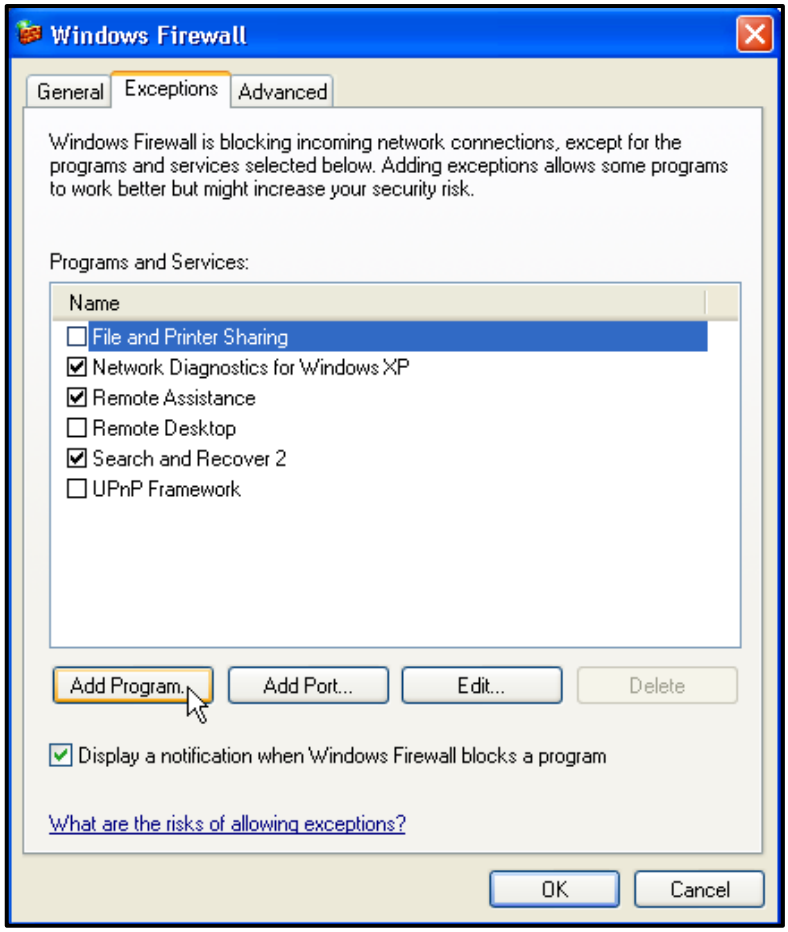
Windows Firewall obavlja sledeće funkcije:
• blokira dolazni saobraćaj, tj. otvaranje veza sa udaljenog računara (osim ka specificiranim portovima),
• sprečava programe sa vašeg računara da se ponašaju kao mrežni servisi (osim onih programa kojima eksplicitno dodelite pravo da se ponašaju kao servisi na kartici Exceptions).
• nudi mogućnost da dozvolite prijem i slanje ICMP paketa,
Realno, Windows Firewall nije dovoljno dobro rešenje jer, ako zanemarite ICMP, filtrira samo dolazni saobraćaj. Na Windows XP Firewallu ne može se obaviti restrikcija odlazećih paketa koje lokalni računar generiše niti odrediti koje aplikacije mogu da pristupe Internetu, a koje ne mogu.

Demonstracija na Virtual Box-u

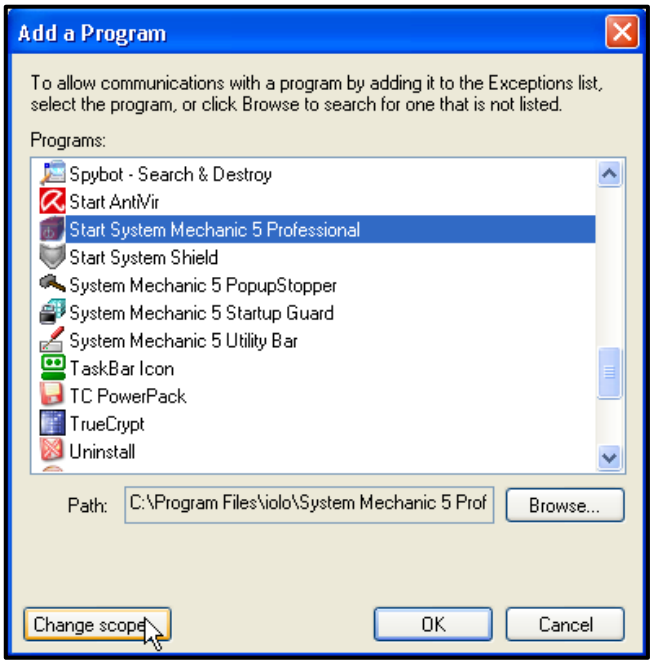
Klikom na **Start – Control Panel – Windows Firewall** pokrećete grafičko okruženje Windows Firewall-a:



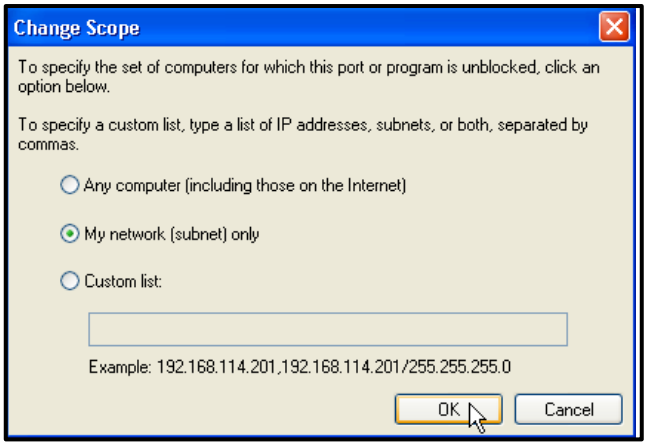
Pokreće se aplikacija koja vam omogućuje da editujete neke od opcija ove mrežne barijere. Kao što je već rečeno, Windows Firewall omogućuje filtriranje paketa samo u dolazećem saobraćaju tako da je dosta nesiguran za neke ozbiljnije potrebe. Kako god bilo, potrebno je znati način na koji ćete dodati novo pravilo koje podrazumeva dozvolu pristupa sa mreže ili interneta nekom od programa ili portova na vašem računaru. Dodaćete Pravilo tako što ćete klikon na dugme "**Exeptions**" otvoriti list na kom su vam izlistana sva trenutno aktivna pravila, klikom na "**Add Program**", dodajete program kome želite da računari iz vaše mreže pristupaju:



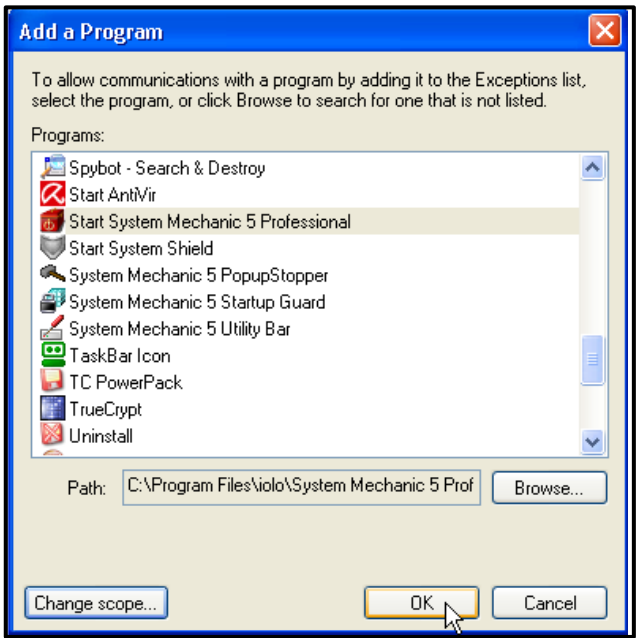
Klikom na dugme "**Add Program**", otvarate prozor za selektovanje odgovarajućeg programa i tu selektujete program System Mechanic 5 Profesional:



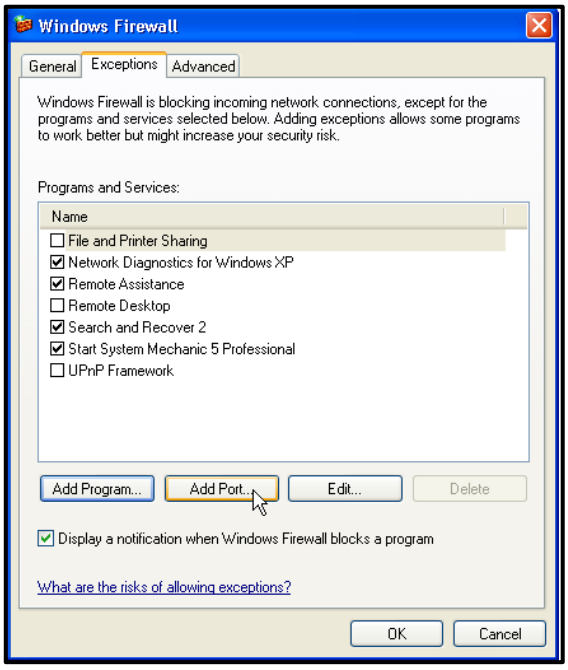
Sada ćete klikom na dugme "**Change Scope**", precizirati ko tačno može da pristupa ovom programu. Postavite na opciju "**My Network**" ili možete dodati I određenu IP adresu sa odgovarajućom Subnet maskom, klikom na opciju Custom list:



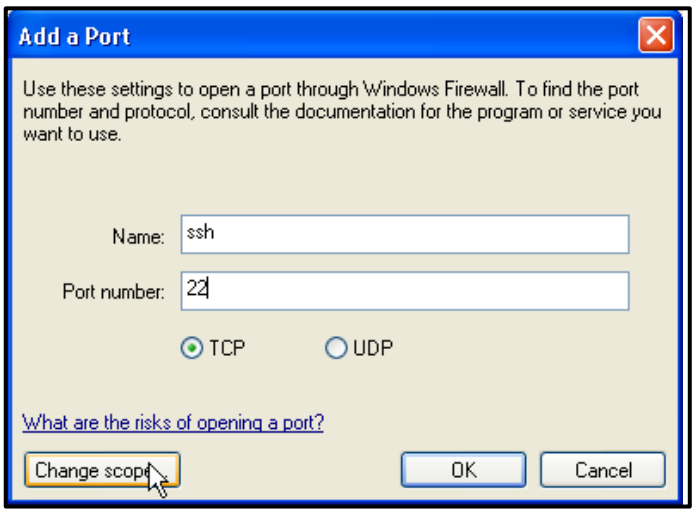
Kada ste dodali ovo pravilo, potvrdite izmene sa "**OK**" i u listi za izbor programa takođe "**OK**":



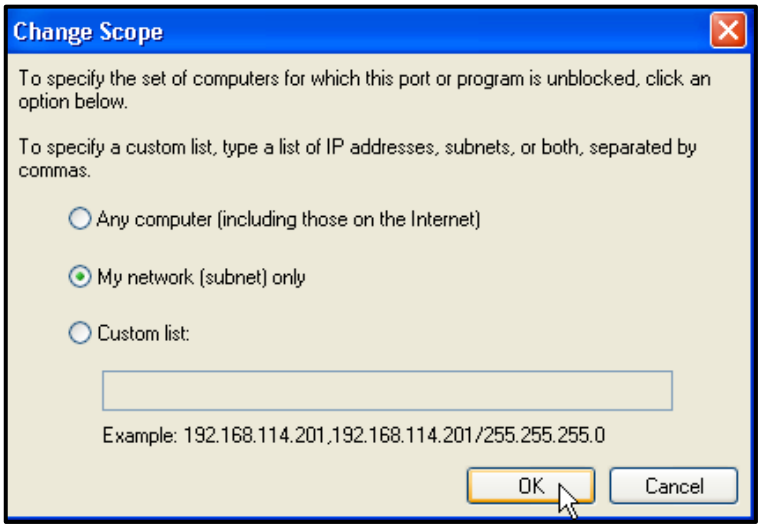
Sada ćete dodati, odnosno otvoriti port preko kog će računari u vašoj mreži moći da pristupe vašem računaru. Ovo ćete urediti klikom na dugme "**Add Port**":



Otvoriće se sledeći prozor u kom ćete dozvoliti pristup vašem računaru preko TCP porta SSH, odnosno Secure Shell-a koji radi na portu 22! Popunite polja u ovom prozoru na sledeći način:



Klikom na "**Change Scope**" dodajete precizniji pristup, odnosno, dozvoljavate pristup vašem računaru samo sa lokalne mreže ili možete dodati i određenu IP adresu sa odgovarajućom Subnet maskom, klikom na opciju Cusom list:



Sada možete videti sva pravlia koja trenutno važe i koja možete editovati klikom na dugme "**Edit**", u slučaju da nekada bude potrebe za izmenom nekog od pravila.