LABORATORIJSKA VEŽBA BR. 10

Mrežne barijere

- Programski paket Comodo Personal Firewall

POTREBNA OPREMA

- Računar sa instaliranim Windows operativnim sistemom
- Instalirani programski paket Comodo Personal Firewall

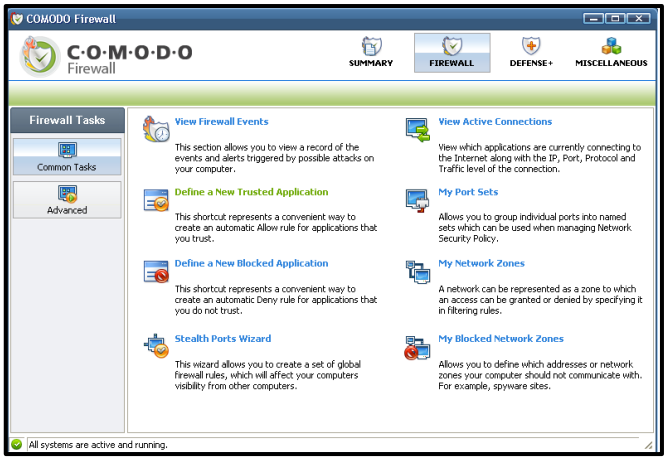
TEORIJSKE OSNOVE

Comodo Personal Firewall

Comodo Internet Security Kombinuje tehnike Antivirusne zaštite i naprednih tehnika filtriranja paketa i HIP sistem (engl.: *Host Intrusion Prevention*) kako bi zaštitio računar od internih i eksternih pretnji. Comodo u svom paketu sadrži Antivirusnu proaktivnu zaštitu, Mrežnu barijeru koja neprekidno pruža zaštitu filtriranjem paketa, Defence + koji sadrži napredne tehnike postavljanja pravila baziranim na IPS-u, (engl.: *Intrusion Prevention System*), koja pružaju zaštitu sistemskih datoteka od malicioznih (zlonamernih) procesa i blokira nepoznati malware pre nego što dobije priliku da se instalira na sistem. Sadrži još dva paketa koji su dostupni u **Profesional** verzijama, što znači da se ova dva paketa dodatno naplaćuju. To su **Live PC Support** što podrazumeva sve tipove online zaštite I **Secure Wireless Internet Conectivity** paket koji pruža bezbedno konektovanje na internet preko bilo koje javne bežične mreže (lokacije).

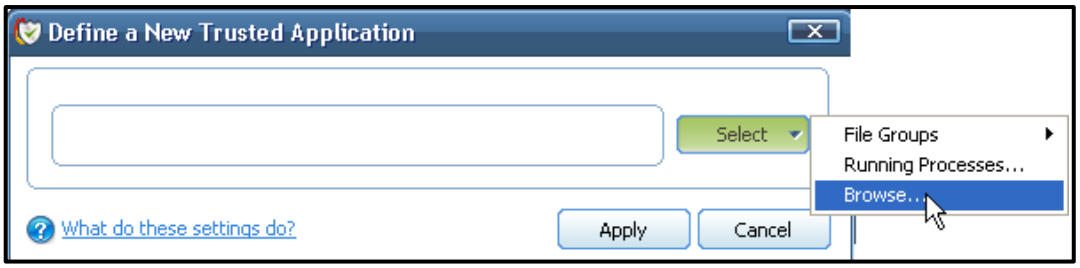
Demonstracija na Virtual Box-u
Sada ćete pokrenuti Comodo čija se startup ikonica nalazi na Desktopu. Na prvom prozoru imate listu svih dešavanja u saobraćaju (Sumary), Imate **Network Defence** i **Defence +**. Nas će danas interesovati samo Network Defence i način na koji ćete postaviti određena pravila za filtriranje paketa, restrikciju pristupa nekim programima kao i dozvolu pokretanja.

Kliknite na ikonicu **Firewall**, i otvoriće vam se područje Comodo-a gde ćete unositi pravila filtriranja:

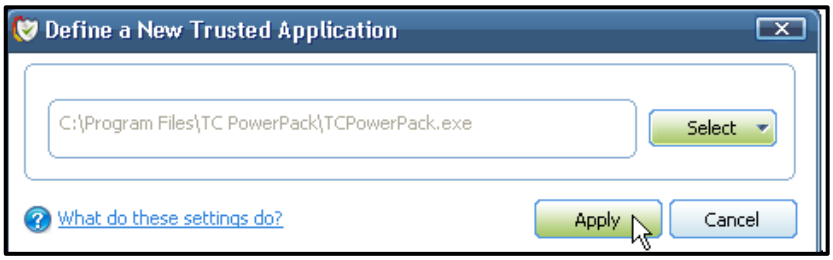


Klikom na **Define a New Trusted Application** otvarate prozor za definisanje polise na određenu aplikaciju. Tako u ovom slučaju definišete aplikaciju od poverenja na sledeći način:

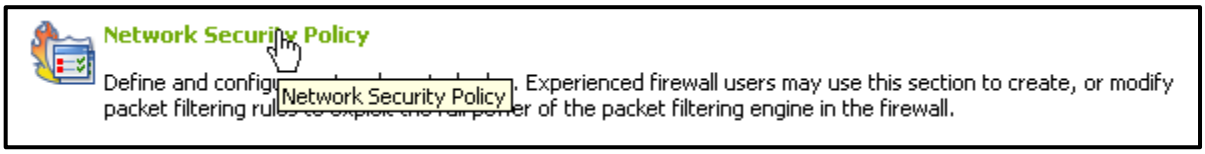
Otvara se prozor za definisanje aplikacije od poverenja i nju nalazite tako što ćete klikom na **Select** i **Browse** naći putanju do aplikacije kojoj želite da dozvolite pokretanje, (Za ovaj primer, ja sam uzeo TC PowerPack):

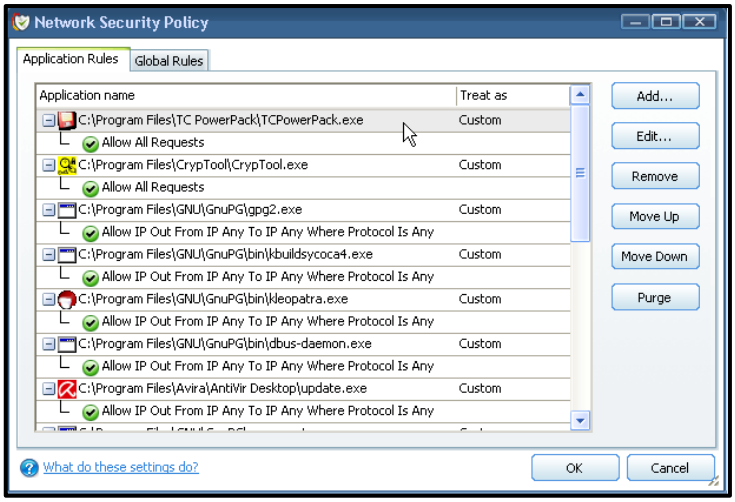


Potvrdite izbor aplikacije klikom **Apply**.

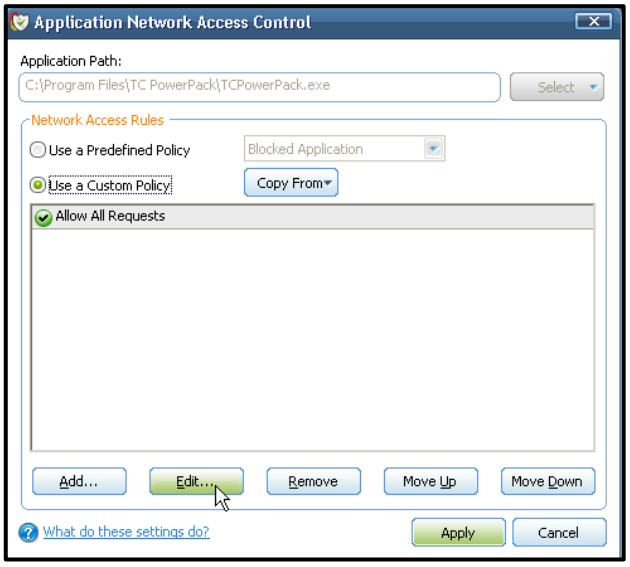


Sada klikom na Advanced dugme koje se nalazi na levoj strani aplikacije otvarate područje za napredno podešavanje polisa (pravila), zatim klik na **Network Security Policy** otvarate prozor za editovanje svih pravil koja su aktivna:

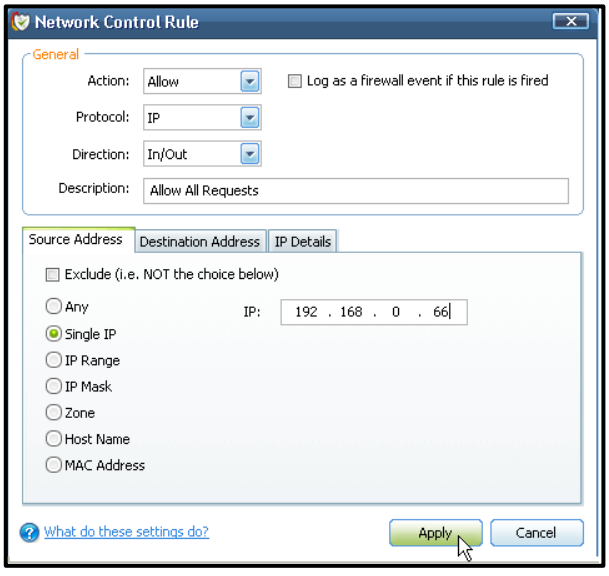


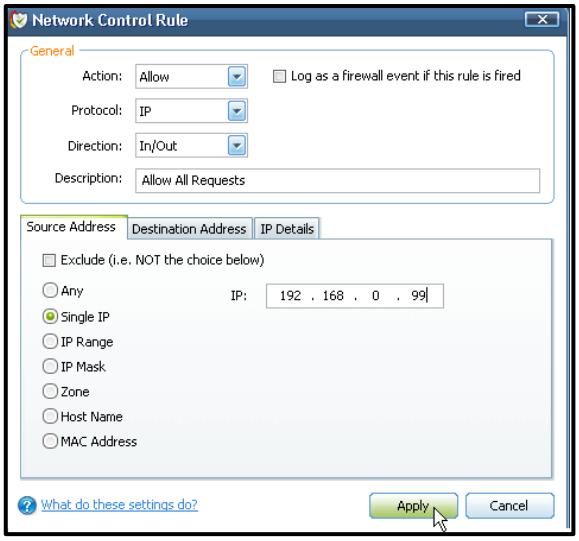


Sada klikom na **Edit** možete promeniti pravila po kojima se aplikacijama dozvoljava ili zabranjuje aktivnost u prozoru **Application Network Access Control**:

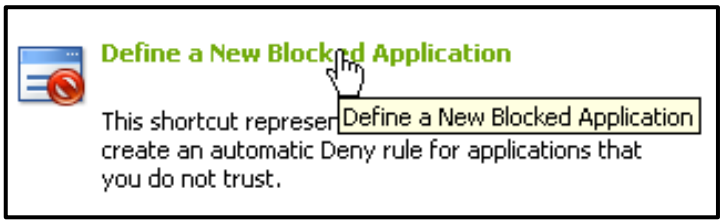


Klikom na dugme Edit menjate trenutno važeću polisu za ovu aplikaciju tako da Source Address postavite na određenu adresu: **192.168.0.66** a Destination Addresss postavite na **192.168.0.99**:

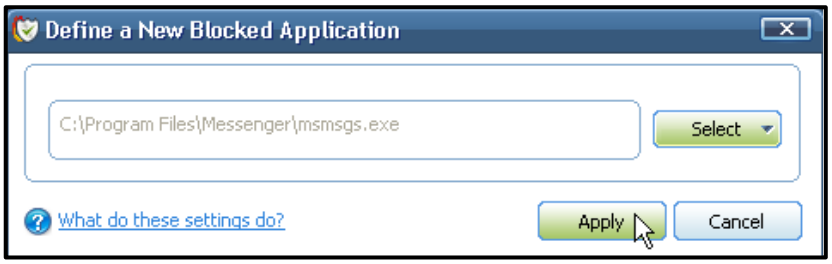




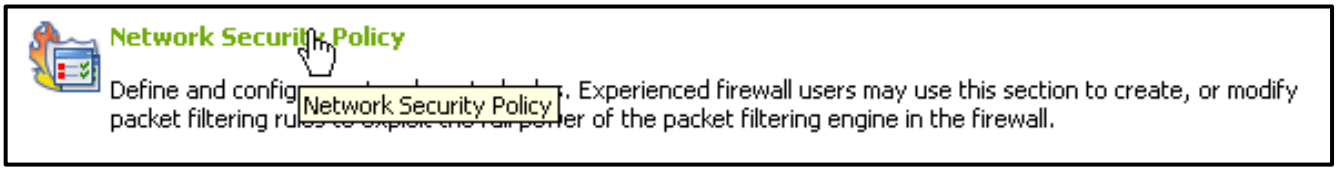
Sada ćete dodati aplikaciju u listu aplikacija kojima ne verujete. Klikom na **Define a New Blocked Application** otvarate prozor za definisanje te aplikacije:



Ja sam za ovaj primer izabrao da zabranim aktivnost Messenger-a:

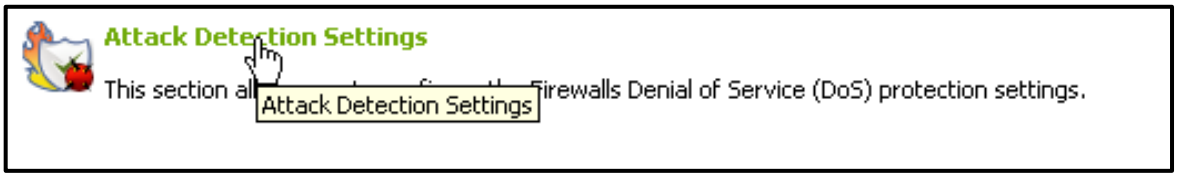


Klikom na **Network Security Policy** otvarate prozor za izmenu polisi:



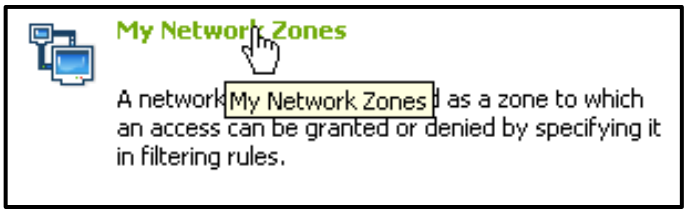
U zavisnosti od toga koliko ne verujete datoj aplikaciji, postavićete zabranu u toj težini. Možete ostaviti predefinisanu polisu za zabranu koja će zabraniti pokretanje ove aplikacije sa bilo koje adrese i praviće Log datoteke ua svaki pokušaj pokretanja.
Kako bi se zaštitili od napada brutal napada sa mreže koji izazivaju ICMP, TCP, UDP preplavljivanje, postavićete paranoična pravila koja kažu da je za sva tri protokola dozvoljen saobraćaj sa 10 paketa u

sekundi u trajanju od 10 sekundi. Vreme za koje će sumnjivi host (računar) biti blokiran nakon pokušaja skeniranja portova, postavite na 10 minuta a vreme za koje će Firewall biti u stanju pripravnosti dok je računar žrtva DoS (engl.: *Denial of Service*) napada, postavite na 5 minuta. Ovo ćete uraditi tako što ćete kliknuti na *Advanced* dugme koje se nalazi na levoj strani aplikacije a zatim na **Attack Detection Settings**:

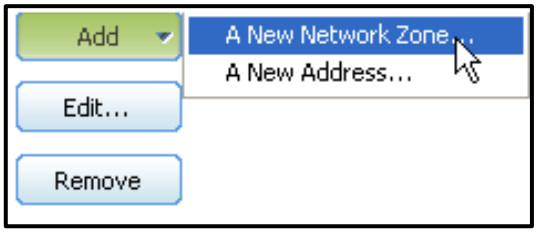


Zatim podesite parametre zaštite od gore navedenih napada sa odgovarajućim vrednostima:

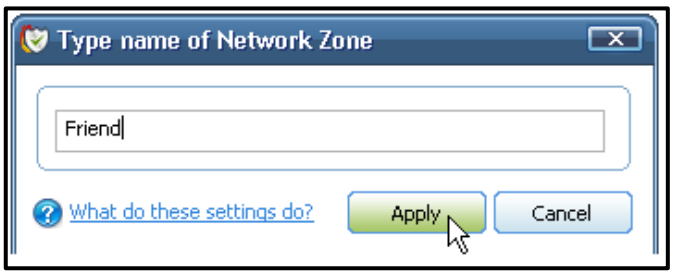
Sada ćete definisati novu zonu od poverenja i u nju ćete ubaciti IP adresom
192.168.0.33 kao host-a koji pripada toj zoni. Kreirate i zonu kojoj ne verujete
dodeljujući IP adresu računara koji pripada toj zoni a koja je 192.168.0.13.
Klikom na **My Network Zones** otvarate prozor za definisanje mrežnih zona
kojima verujete:



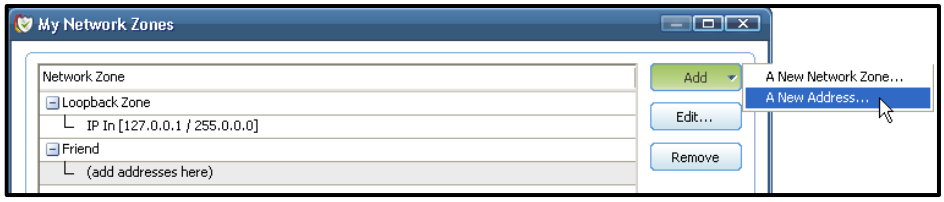
Zatim dodajete novu zonu klikom na dugme **Add – A New Ntework Zone**:



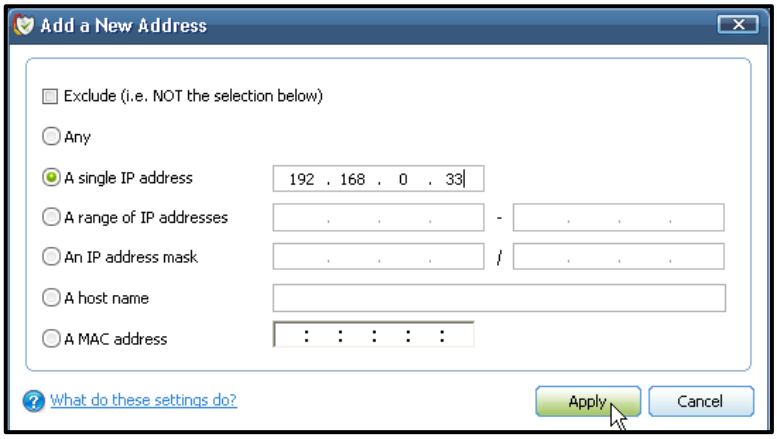
Sada dajete ime zoni, s obzirom da je to zona od poverenja, dajete joj simbolično ime, npr.: *Friend*:



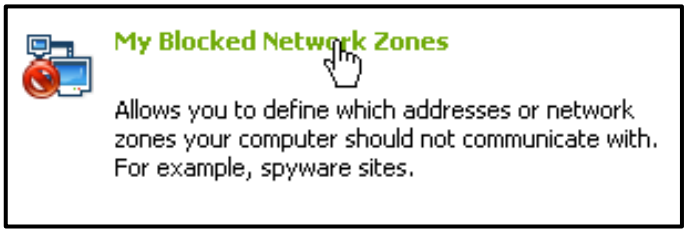
Sada dodajete novu IP adresu koja će pripadati ovoj zoni, odnosno IP adresu računara kome verujete. Klik na prazno polje za IP adresu ispod imena zone a zatim **Add – A New Address**:



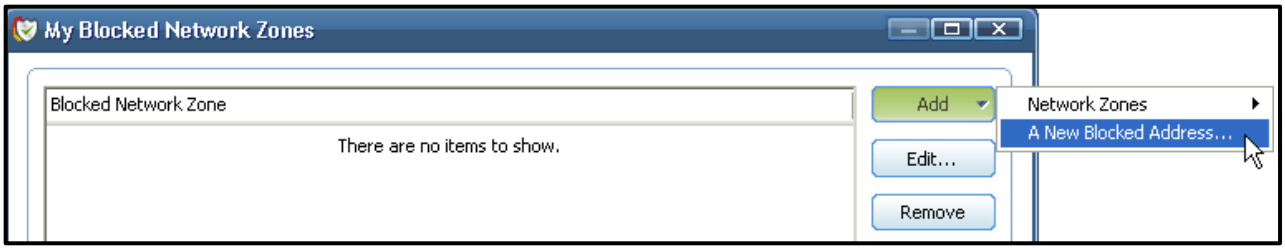
Prozor popunjavate shodno uslovima zadatka:



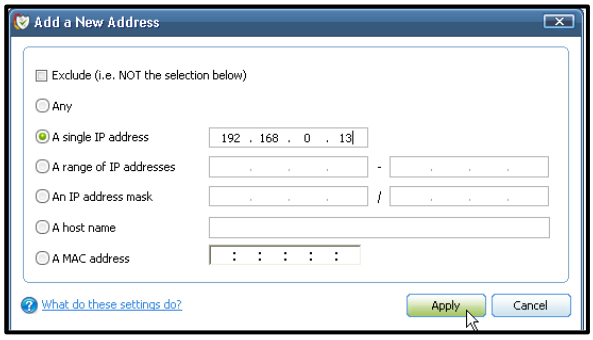
Potvrdite novonastale promene klikom na **Apply** a zatim kreirate i zonu kojoj ne verujete tako što ćete kliknuti na **My Blocked Network Zones**:



Sada dodajete IP adresu kojoj ne verujete:



Otvara vam se prozor za unos IP adrese i shodno uslovima zadatka popunjavate polja ovog prozora:



Klikom na **Apply** potvrdite sve izmene i sada ste kreirali zonu od poverenja I zonu koja sadrži IP adrese računara kojima iz nekog razloga ne želite da verujete tak oda će se shodno polisama Comodo-a primenjivati određena pravila na računare obe zone. Ove polise možete videti nakon klika na