HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Comodo vatrozid

CCERT-PUBDOC-2007-02-184

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, **www.lss.hr -** laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

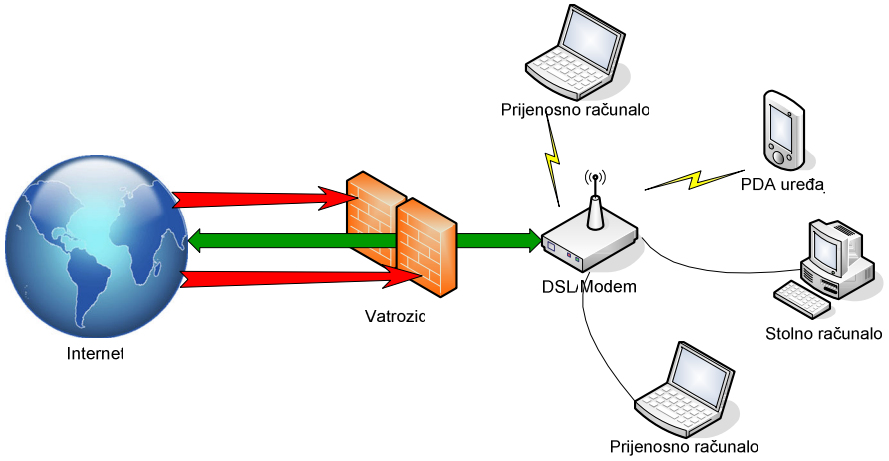
Gotovo svi korisnici računala susreli su se s pojmom vatrozida (eng. *firewall*). Korisnici osobnih računala s novijim Windows operacijskim sustavima, poput Windows XP ili Vista sustava, susreli su se s aplikacijom Windows Security Center koja implementira funkcionalnosti vatrozida. Korisnici Unix operacijskih sustava jednako tako imaju priliku koristiti slične aplikacije, budući da se one podrazumijevano isporučuju s njihovim operacijskim sustavima. Mnogi korisnici računala u tvrtkama zasigurno koriste vatrozid, a da toga najčešće nisu svjesni. S druge strane, korisnici kućnih DSL linija vjerojatno su došli u doticaj s vatrozidima za kućnu računalnu mrežu. Iz navedenog je moguće zaključiti kako je vatrozid trenutno nezaobilazan i elementaran dio zaštite svakog računala koje je u doticaju s Internetom.

Budući da je Comodo vatrozid sve prisutniji zaštitni program, u ovom će dokumentu biti detaljno opisan način preuzimanja, instalacije i korištenja tog sigurnosnog rješenja. Prethodno će se dati detaljniji uvid u općenite funkcionalnosti vatrozida te na taj način dodatno ukazati na potrebu za aplikacijama ove vrste. Dodatno, u dokumentu je iznesen i kratak pregled ispitivanja efikasnosti Comodo vatrozida. Na koncu, opisani su i ostali konkurentski proizvodi – komercijalna, ali i velikom broju korisnika važnija – besplatna rješenja. Budući da se radi o aplikaciji čije je korisničko sučelje grafičko, u dokumentu je dan niz prikaza njegovog izgleda.

Kako je tema ovog dokumenta jednako važna naprednim korisnicima, ali i početnicima, neki važniji postupci poput ispravne instalacije i korištenja su podrobno opisani, tako da je dokument prihvatljiv korisnicima s različitim razinama predznanja.

2. Općenito o vatrozid aplikacijama

Vatrozid je rješenje koje u velikoj mjeri smanjuje potencijalne internetske prijetnje, a korisnicima je dostupno u obliku programske potpore ili zasebnih uređaja. Rješenje u obliku programske potpore koristi se uglavnom na osobnim računalima koja nisu dio računalne mreže ili su dio manje mreže, na primjer, kućne. Drugi oblik vatrozida je korišten prvenstveno u kompleksnim mrežama kakve se nalaze u tvrtkama. Ovdje je naglasak stavljen na programske implementacije vatrozida.
Jednostavnim rječnikom, vatrozid filtrira podatke koji prolaze kroz njega – omogućuje ili onemogućuje njihov prolaz unutar ili van objekta ili sustava na čijem se ulazu nalazi. Ovdje je taj objekt korisničko računalo. Na taj način svi će uočeni zlonamjerni podaci biti odbačeni već na ulazu. Vatrozid omogućava postavljanje sigurnosnih pravila kojima se određuje hoće li određeni promet biti propušten ili zaustavljen. Ovisno o konkretnoj vatrozid aplikaciji, moguće je ograničiti pristup mreži prema IP adresama ili imenima domena, a jednako tako moguće je zaustavljanje temeljiti na TCP/IP priključku (eng. *port*).



Slika 1: Shematski prikaz vatrozida

U osnovi postoje četiri mehanizma koja se koriste za ograničavanje prometa podataka. Vatrozidna aplikacija može implementirati i više od jednog mehanizma koji međusobno surađuju te na taj način ostvariti kvalitetniju zaštitu. U nastavku slijedi podrobniji opis spomenutih mehanizama.

1. **Filtar paketa** (eng. *packet filter*) stoji na putu svim odlaznim i dolaznim podacima te na njih primjenjuje sigurnosna pravila koja je korisnik zadao. Najčešće filtar paketa ima pristup informacijama poput izvorne i odredišne IP adrese te izvornog i odredišnog priključka (eng. *port*). To je najčešći kriterij prema kojemu se zadaju pravila ovom mehanizmu.
2. **Poveznik** (eng. *circuit-level gateway*) je najčešće korišten mehanizam u slučaju kada se vatrozid nalazi između vanjskog svijeta i računalne mreže. U tom slučaju, vatrozid prihvaća sav promet i onemogućuje prolaz ulaznih podataka računalima s branjene mreže. Svim računalima s lokalne mreže omogućena je uspostava veze jedino s poveznikom. Ostala računala s vanjskog svijeta nemaju informaciju o tome kako sudjeluju u komunikaciji s računalom iz mreže nego kao drugu stranu vide samo spomenuti poveznik.
3. **Posrednik** (eng. *proxy*) se načelno koristi za poboljšanje performansi mrežne komunikacije, ali može djelovati i kao vatrozid. Ovakvi poslužitelji skrivaju privatnu korisnikovu IP adresu tako da se vanjskom računalu čini kao da oni uspostavljaju komunikaciju. Pored toga, temeljna zamisao koja stoji iza njih jest spremanje svih dohvaćenih web stranica u spremnik nakon prvotnog zahtjeva za njima. Svi ostali zahtjevi za spremljenom stranicom odvijaju se tako da se usporedi inačica pohranjene web stranice s onom na Internetu. Ako se ustanovi da je riječ o istoj inačici stranice, ona se ne mora dohvaćati s odgovarajućeg poslužitelja nego ju posrednik jednostavno isporuči onom računalu koje ju je zatražilo budući da ju ima pohranjenu u svojem spremniku. Na taj način može se onemogućiti pristup pojedinim web stranicama ili ograničiti korištenje određenih mrežnih priključaka i slično.

4. **Aplikacijski poveznik** (eng. *application gateway*) je samo jedna inačica prethodno opisanog poveznika. Njegova funkcionalnost zasniva se na sljedećem postupku. Računalo s mreže najprije uspostavi vezu s aplikacijskim posrednikom. Zatim se određuje nalazi li se veza u skupu zabranjenih ili dozvoljenih veza. Tek tada ju se odbacuje ili se omogućuje njezina potpuna uspostava sa željenim računalom na Internetu. Zbog prirode funkcioniranja i ovaj poslužitelj prikriva izvornu adresu računala koje je zatražilo uspostavu veze.

Svaki od navedenih mehanizama ima svojih prednosti i mana. Aplikacijski poveznik se smatra sigurnijim i naprednijim oblikom vatrozida nego ostala tri mehanizma, ali zato koristi više računalnih resursa (memorije i procesorske snage). Filtriranje paketa je lakše implementirati, ali je podložno napadima kod kojih se postavlja lažna izvorna adresa ili priključak u mrežne pakete.

Za povećanje sigurnosni kod filtriranja paketa, dizajniran je postupak filtriranja s nadzorom stanja veze (eng. *stateful inspection*). Riječ je o proširenoj funkcionalnost filtra paketa čija je temeljna funkcionalnost ostala nepromijenjena, ali je omogućen nadzor nad uspostavljenim vezama te je dozvoljen detaljniji pregled sadržaja paketa - na višim slojevima OSI modela (eng. *Open Systems Interconnection Basic Reference Model*). Praćenje uspostavljenih veza dovodi do mogućnosti detektiranja prometa koji nije u postojećem kontekstu neke od uspostavljenih veza, čak i ukoliko zadovoljava pravila vezana uz IP adresu i priključak. U tom slučaju paket se odbacuje. Dakle, riječ je o naprednijoj metodi filtriranja koju većina današnjih vatrozida podržava.

Mnogi ADSL modemi imaju ugrađene funkcionalnosti vatrozida, a najčešće je riječ o jednostavnim filtrima paketa. Korisniku je omogućeno postavljanje sigurnosnih pravila poput blokiranja svih pokušaja uspostave veze s vanjske strane. Ukoliko korisnik želi omogućiti pristup web poslužitelju na nekom od računala iz mreže, mora to eksplicitno učiniti. Savjet je koristiti upravo ovaj redoslijed postavljanja: prvo ograničiti sav promet, a onda dodavati pravila za propuštanje prometa. Ovo vrijedi ukoliko se ADSL modem koristi u usmjerivačkom načinu rada (eng. *router mode*).

Pored sklopovskih rješenja poput navedenog, koriste se i rješenja u obliku programske podrške. Takve aplikacije također obavljaju nadzor nad svim dolaznim i odlaznim podacima, a nazivaju se osobnim (eng. *personal*) vatrozidima.

Ranjivosti aplikacija i operacijskih sustava te implementacija protokola uočavaju se svakodnevno. Napadači ih zloupotrebljavaju za ostvarivanje nedozvoljenog pristupa ranjivim računalima. Tako preuzimaju potpunu ovlast, stječu pristup potencijalno osjetljivim korisnikovim podacima i izvode napade uskraćivanja resursa. Zato je važno redovito primjenjivati zakrpe za aplikacije i operacijske sustave i osvježavati antivirusne aplikacije. Pored toga, za potpunu sigurnost od velike važnosti je i korištenje vatrozida te njegovo redovito osvježavanje.

3. Comodo vatrozid

Prethodno je ustanovljeno kako su vatrozidi vrlo važan dio obrane od zlonamjernih korisnika i aplikacija koji prijete s Interneta. U ovom poglavlju dan je uvod u Comodo vatrozid i potpuni tehnički opis aplikacije.

3.1. Opće informacije

Comodo Firewall jedan je u nizu proizvoda tvrtke Comodo. Detaljnije informacije o samoj tvrtci kao i o vatrozidu dostupne su na web stranicama:

- http://www.comodo.com/ i
- http://www.personalfirewall.comodo.com/.

Ostali proizvodi su antivirusne aplikacije, digitalni certifikati za poruke elektroničke pošte, sigurnosni pregledi poslužitelja i upravitelji zaporkama. Važno je spomenuti da su svi navedeni proizvodi besplatni u svojim temeljnim inačicama, a vatrozid čak i u profesionalnoj inačici. Naziv te inačice je **Comodo Firewall Pro**. Razlog naizgled opasnom tržišnom pothvatu leži u komercijalnoj politici koju koristi tvrtka. Ideja im je razviti potpuna sigurnosna rješenja za osobna računala i na taj način steći ugled na tržištu. To je zapravo radikalan način reklamiranja od kojeg krajnji korisnici imaju koristi. Tvrtka ostvaruje zaradu prodajom digitalnih sigurnosnih potvrda (eng. *digital certificate*) drugim tvrtkama.

3.2. Svojstva Comodo vatrozida

Comodo Firewall Pro, prema navodima proizvođača, jedan je od „najpametnijih" vatrozida dostupnih u današnje vrijeme. Prilikom pokušaja uspostave veze prema Internetu ili s Interneta, većina vatrozida postavlja pitanje korisniku vezano uz omogućavanje ili onemogućavanje uspostave veze ili slično. Često je slučaj da korisnici ne razumiju ta pitanja pa na njih nasumično odgovaraju. Jasno je da se u tom slučaju javlja potencijalna opasnost od omogućavanja pristupa Internetu i zlonamjernim aplikacijama. Comodo vatrozid pomaže korisniku u razumijevanju tih pitanja sugerirajući mu odgovore na svako postavljeno pitanje. Paket sadrži i ugrađenu bazu aplikacija s više od 10 000 zapisa s odgovarajućim atributima poput *SAFE*, *SPYWARE*, *ADWARE*, itd.

Neke važne karakteristike ovog proizvoda, prema navodima proizvođača, su:

- *Application Component Authentication* – provjerava pouzdanost svih komponenata aplikacije prije nego joj dozvoli uspostavu veze prema Internetu,
- *Application Behavior Analysis* – analizira ponašanje aplikacije prije nego joj dopusti pristup Internetu,
- *Defense against Trojan Protocols* – napredna obrana od trojanskih konja,
- *Smart Alerts* – svako upozorenje ili upit popraćeno je sugestijom odgovora i odgovarajućim opisom aplikacije,
- *Windows Security Center Integration* - Windows XP SP2 sustav ispravno prepoznaje Comodo kao sistemski vatrozid,
- *Self Protection against Critical Process Termination* – virusi, trojanski konji i slične zlonamjerne aplikacije ga ne mogu programski isključiti,
- *PC Security during PC Start Up* – zaštita i prilikom pokretanja operacijskog sustava,
- *Automatic Updater* – sadrži i modul za interaktivnu nadogradnju kojeg korisnici mogu i *ručno* pokrenuti u proizvoljnom trenutku,
- *Error Reporting Interface* – sučelje za prijavu pogrešaka aplikacije (eng. *bug*) odgovara onomu kod WinXP sustava,
- *Firewall Logging* – zapis svih aktivnosti s detaljnim obrazloženjima,
- *Security Rules Interface* – grafičko korisničko sučelje za postavljanje sigurnosnih pravila,
- *Application Activity Control* – podaci o svakoj aplikaciji vezani uz IP adresu i *port* te količinu podataka koju je razmijenila s odredištem,
- *Graphical User Interface* – grafičko korisničko sučelje omogućuje potpunu kontrolu nad vatrozidom i
- *Application Recognition Database* – prepoznaje više od 10 000 aplikacija i potencijalnih opasnosti koje prijete od njih.

Comodo vatrozid je aplikacija namijenjena sljedećim inačicama Windows operacijskih sustava:

- Windows 2000 (32 bit),
- Windows XP (32 bit),
- Windows 2003 (32 bit),

te ima slijedeće zahtjeve za resursima:

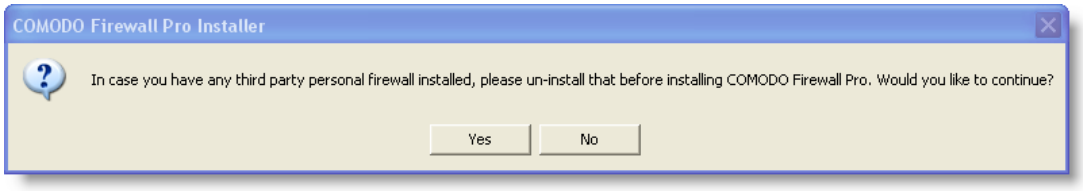
- 64MB radne memorije (eng. *RAM – Random Access Memory*) i
- 32MB slobodnog mjesta na disku.

Svi korisnici čija računala zadovoljavaju navedene specifikacije mogu započeti instalaciju paketa.

3.3. Preuzimanje i instalacija paketa

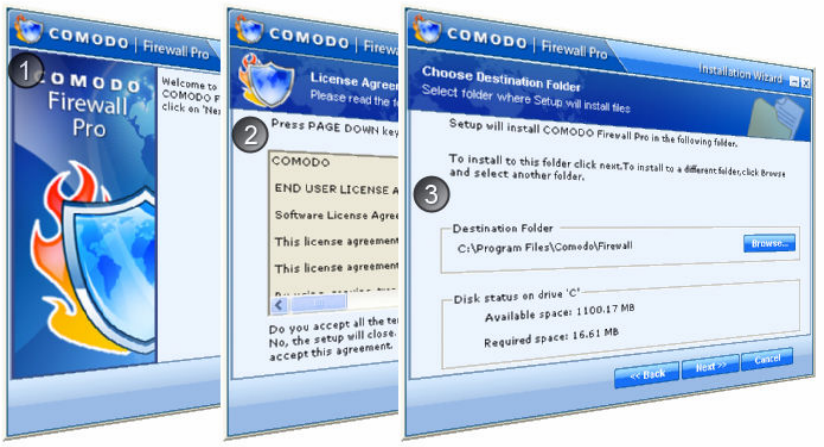
Odabirom poveznice *Download now* na web stranicama vatrozida započinje postupak preuzimanja paketa. U trenutku pisanja ovog dokumenta najnovija inačica je Comodo Firewall Pro 2.4 veličine 7.5MB. Prethodno je potrebno odabrati jezik aplikacije, a budući da hrvatski nije ponuđen najčešći odabir bit će engleski. Paket je dan u obliku jedne izvršne instalacijske datoteke.

Instalacija započinje pokretanjem navedene izvršne datoteke. Na samom početku aplikacija upozorava da ako već postoji vatrozid na računalu, treba ga najprije ukloniti.



Slika 2: Upozorenje o potrebnoj de-instalaciji

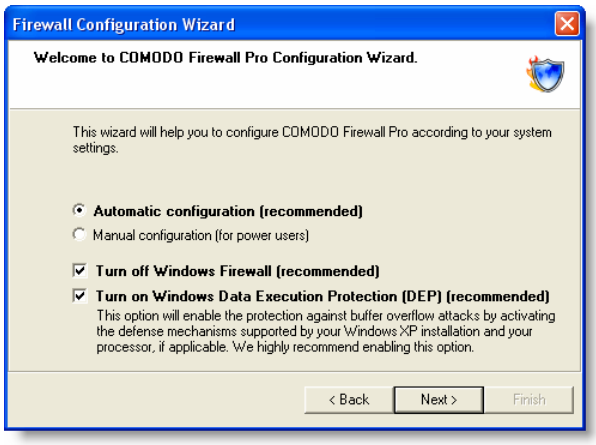
Ostatak instalacijske procedure je karakterističan za većinu programskih paketa pa se ovdje neće posebno opisivati nego samo prikazati na slici ispod.



Slika 3: Postupak instalacije

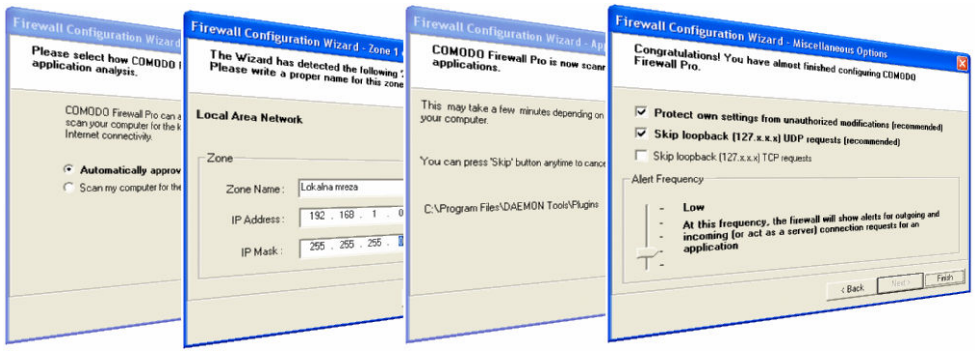
Slijedi izvedba postupka vezanog uz registraciju vatrozida. Od korisnika se traži jedino upisivanje ispravne adrese elektroničke pošte te uključivanje ili isključivanje mogućnost primanja obavijesti vezanih uz paket.

Važniji dio je postavljanje samog vatrozida koje započinje prema primjeru na slici ispod.



Slika 4: Postavke vatrozida

Ukoliko se korisnik odluči za *ručno* postavljanje opcija, slijedit će različite postavke vezane uz pregled svih instaliranih programa, razinu učestalosti pojavljivanja upozorenja, postavljanje zone i slično. Iste se postavke mogu izmijeniti i kasnije korištenjem središnjeg upravljačkog sučelja.



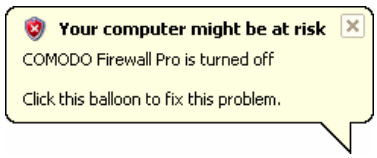
Slika 5: Napredno postavljanje

Daleko najjednostavnije je ostaviti sve podrazumijevane vrijednosti i na taj način privesti instalaciju kraju. Preostaje još ponovno pokretanje operacijskog sustava i postupak instalacije je uspješno završen.

Slika 6: Završetak instalacije

3.4. Upozorenja i odluke

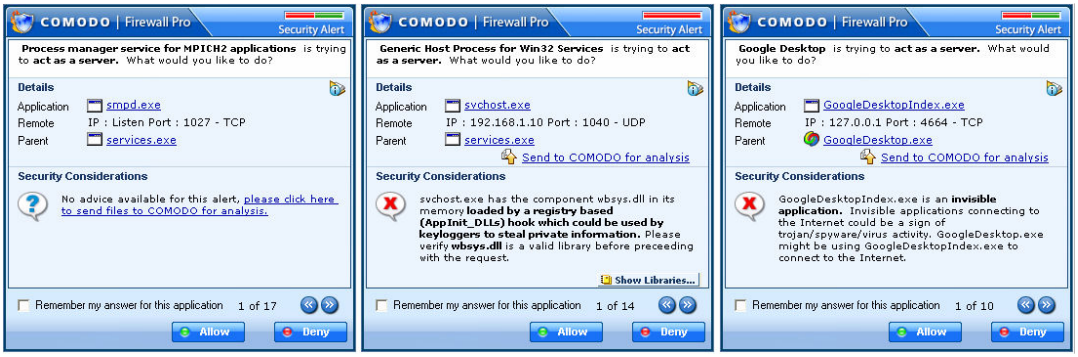
Nakon ponovnog pokretanja računala postoji mogućnost pojave poruke prikazane na slici ispod.



Slika 7: Upozorenje kod pokretanja sustava

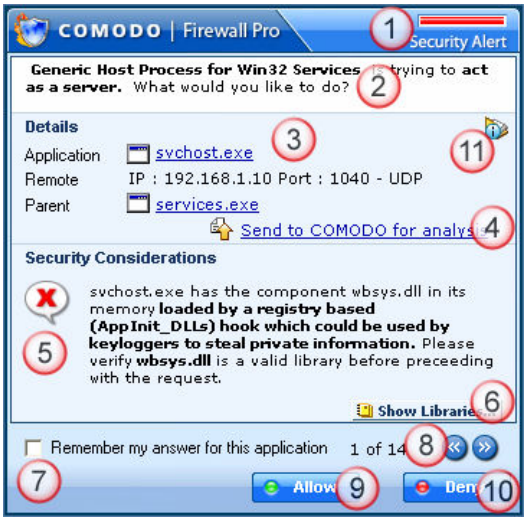
Poruka objšnjava kako je Windows operacijski sustav registrirao Comodo kao vatrozid sustava, ali je isto tako uočio da on nije pokrenut. Razlog tomu je redoslijed pokretanja: Comodo će se u tom slučaju pokrenuti tek nakon Windows modula za detekciju vatrozida na sustavu. Dakle, u slučaju pojavljivanja ove poruke samo treba pričekati da se i vatrozid učita. Ista poruka se pojavljuje ukoliko vatrozid zaista nije u pogonu, primjerice, ako ga je korisnik eksplicitno isključio.

Korisnika će u početku dočekati niz poruka o pokušaju uspostave veze na Internet. Radi se o upozorenjima koja se javljaju kada vatrozid detektira pokušaj uspostave veze za koju ne postoji odgovarajući zapis u njegovoj bazi.



Slika 8: Primjeri upozorenja

Negativna strana niza ovakvog obavješćivanja je dekoncentracija korisnika nakon nekoliko odgovora. Ona dovodi do slučajnog odabira dozvole/zabrane uspostave veze. Još jedan uočeni nedostatak je nepostojanje zapisa u bazi za neke često korištene aplikacije poput Internet Explorer 7 web preglednika.
Na slijedećoj slici prikazano je upozorenje vezano uz proces koji je sastavni dio Window sustava te su brojevima naznačeni važniji dijelovi upozorenja. Vatrozid prepoznaje zahtjev za uspostavom veze prema Internetu i svih biblioteka koje koristi neka aplikacija, a to svakako spada u naprednije mogućnosti.



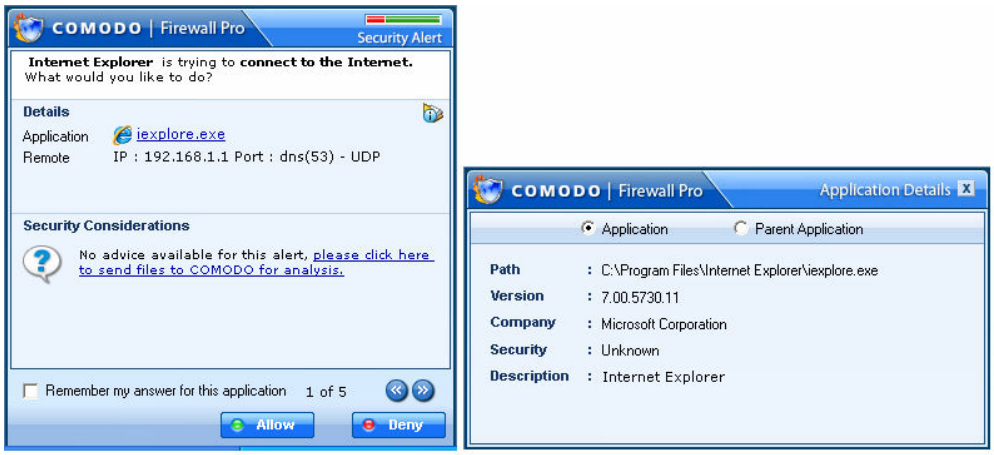
Slika 9: Upozorenje

Slijedi analiza pojedinih dijelova ovoga, možda i najvažnijeg, prozora u aplikaciji.

1. Indikator potencijalne opasnosti. Crvena boja označava faktor opasnosti, a zelena sigurnosti. U ovom slučaju čitava linija je crvena što znači da je najviši stupanj opasnosti prijeti od uspostave ove konekcije.
2. Opis uloge koju aplikacija ima u vezi koju pokušava uspostavit. Aplikacija je ovdje u funkciji poslužitelja.
3. Ime aplikacije koja traži uspostavu veze i ime aplikacije koja ju je pokrenula (eng. *parent*). U ovom slučaju roditelj je program `services.exe`, a aplikacija koja želi uspostavu veze je `svchost.exe`. Također se prikazuje i IP adresa te mrežni priključak udaljenog računala s kojim se veza želi uspostaviti. Ovdje je riječ o istom računalu na komu je pokrenut vatrozid.
4. Postoji mogućnost da korisnik pošalje čitavu datoteku proizvođaču vatrozida na analizu.
5. Opis o aplikaciji i njezinoj komponenti koja želi vezu na Internet. Svako upozorenje popraćeno je određenom sugestijom, a sve tri mogućnosti dane su na slici ispod: sigurno, nesigurno, nepoznato, sumnjivo. Posljednje zahtijeva daljnju provjeru komponenata/modula sporne aplikacije.

Slika 10: Sugestije o dopuštanju uspostave veze

6. Otvara se novi prozor s prikazom biblioteka.
7. Ukoliko se uključi ova opcija, u bazu će biti unesen korisnikov odabir koji će biti primijenjen u slučaju ponovnih pokušaja za uspostavljanjem veze.
8. Strelicama lijevo i desno moguće je prolaziti kroz popis upozorenja.
9. Dozvola za uspostavljanje veze.
10. Onemogućavanje uspostavljanja veze.
11. Otvara novi prozor s detaljnijim informacijama o aplikaciji i o *parent* aplikaciji.



Slika 11: Primjer upozorenja i informacija o aplikaciji

Primjer iznad pokazuje kako baza pored velikog broja aplikacija ne sadrži i podatke o web pregledniku IE7. Parametar *Security* je postavljen na *Unknown*.

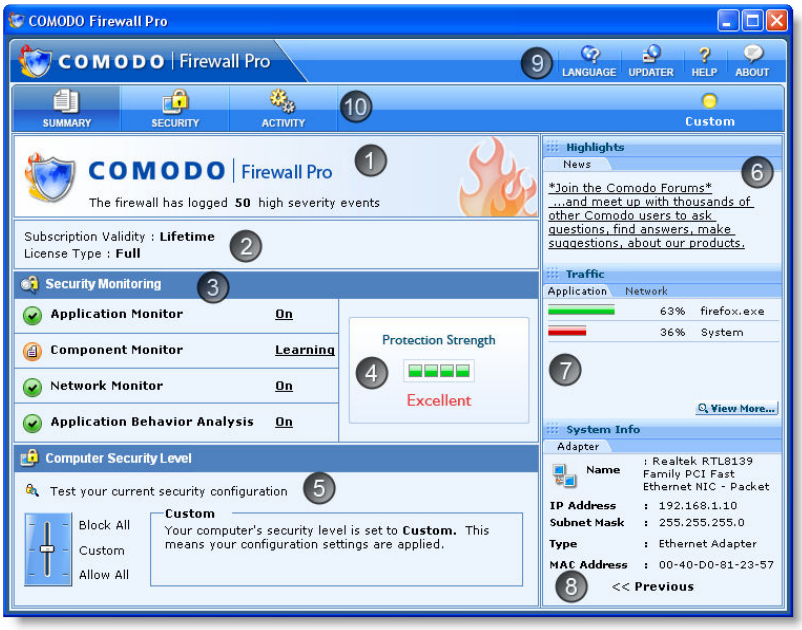
3.5. Korisničko sučelje vatrozida

Nakon instalacije Comodo dodaje indikator u prostor pored sata (eng. *tray*). Isto tako, dodaje se i kratica (prečac, eng. *shortcut*) na radnu površinu (eng. *desktop*) kao i zapis u *All Programs* izborniku. Pokretanje središnje aplikacije može se uraditi odabirom jednog od prečaca ili dvostrukim klikom na ikonu Comodo vatrozida u *tray*-u. Glavni izbornik prikazan je na sljedećoj slici.

Slika 12: Glavni izbornik

3.5.1. Izbornik *Summary*

Odabirom *Summary* izbornika dobiva se cjelovit pregled statusa vatrozida. To se preglednije vidi na slijedećoj slici.



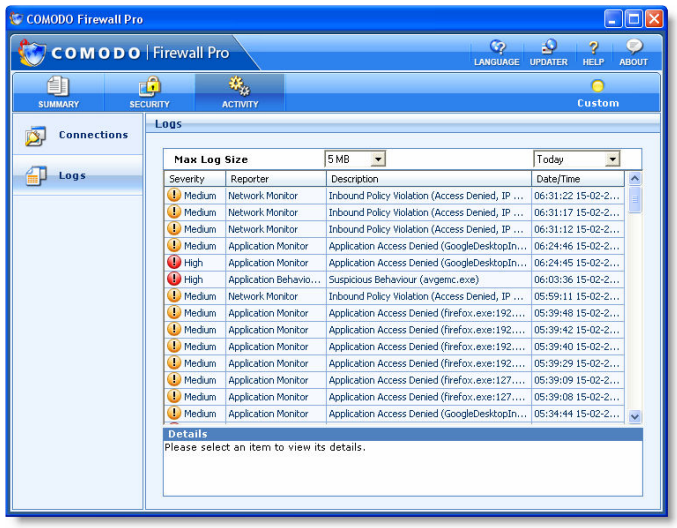
Slika 13: Sučelje vatrozida

1. Prikaz općih podataka o aplikaciji te broja zapisa potencijalnih incidenata.
2. Informacije o licenci.
3. Indikator statusa funkcionalnosti pojedinih modula (podsustava): nadzornik aplikacija (*Application Monitor*), mreže (*Network Monitor*) i ponašanja aplikacija (*Application Behaviour Analysis*) su pokrenuti dok nadzornik komponenata (*Component Monitor*) je u procesu učenja reakcije na pojedini pokušaj uspostave veze.
4. Ukupna trenutna kvaliteta obrane.
5. Dio za brzo postavljanje trenutne sigurnosti s opisom odabrane. Opcija *Test your current security configuration* provodi test ranjivosti lokalnog računala.
6. Vijesti i obavijesti o najnovijim sigurnosnim zakrpama.
7. Grafički prikaz količine prometa koji je prošao kroz vatrozid. Druga kartica omogućuje pogled na statističke podatke iz perspektive mreže – brojčani odnosi paketa u ovisnosti o protokolu (UDP, TCP/IP).
8. Informacije o fizičkim sučeljima prema mreži.

Žuta oznaka u gornjem desnom kutu aplikacije indikator je trenutne sigurnosne razine.

3.5.2. Izbornik *Activity*

Pregled dnevničkih zapisa (eng. *log*) obavlja se odabirom opcije *Activity* iz glavnog izbornika.

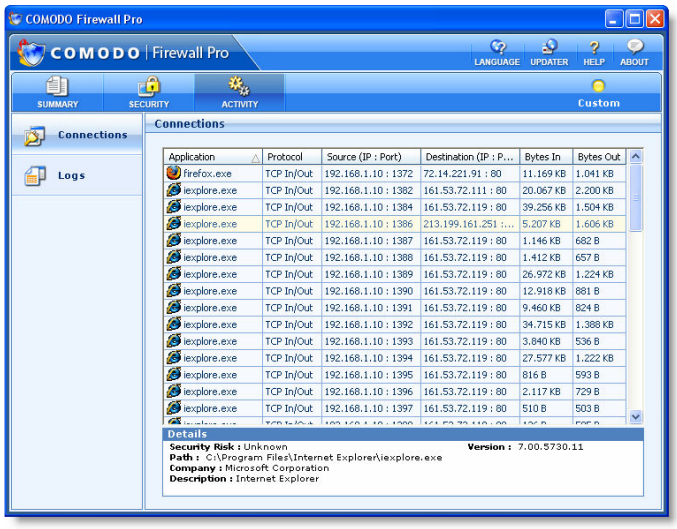


Slika 14: Pregled dnevnika

Moguće je odrediti gornju granicu veličine dnevnika, u ovom slučaju postavljena je na 5MB. Popis svih aktivnosti može se pregledavati za jedan dan, tjedan dana unazad i mjesec dana unazad (eng. *Today, Last 7 days, Last 30 days*). Događaji se spremaju i prikazuju u HTML formatu. Važno je još opisati značenje pojedinih stupaca.

- *Severity* – stupnjevi opasnosti, a podijeljeni su na visoki (eng. *high*), srednji (eng. *medium*) i niski (eng. *low*). Visoki označava napade poput pregleda priključaka (eng. *port scanning*) ili napada uskraćivanja resursa. Ostale dvije razine manje su opasne.
- *Reporter* – opisuje koji je podsustav uočio opasnost (*Application monitor, Network monitor, Component monitor* ili *Application behaviour monitor*).
- *Description* – opis uzroka pojave upozorenja.
- *Date/Time* – vremenski trenutak u kojemu se potencijalna opasnost pojavila.

Odjeljak *Details* pruža detaljnije informacije o odabranom zapisu.



Slika 15: Dnevnički zapisi prometa

Izbornik *Activity* omogućuje i pregled svih veza prema aplikacijama koje su ih inicirale, pripadne IP adrese, protokole te količinu odaslanih i primljenih podataka.

3.5.3. Izbornik *Security*

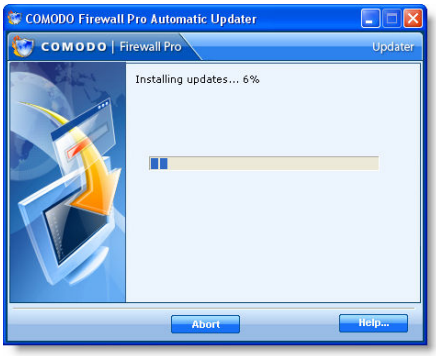
Sve postavke vatrozida mogu se uređivati korištenjem ovog izbornika. Sastoji se od pet podizbornika:

- *Tasks* - definiranje sigurnosnih pravila, zona, određivanje aplikacija kojima će se dozvoliti ili zabraniti pristup Internetu itd.,
- *Application monitor* – popis svih aplikacija kojima se eksplicitno dozvoljava i onemogućava uspostava veze prema Internetu,
- *Component monitor* – pregled i upravljanje komponentama koje su učitane u aplikacije i ponašaju se kao samostalne cjeline,
- *Network monitor* – postavljanje pravila koja se odnose na IP adrese, mrežne priključke i protkole,
- *Advanced* – podešavanje naprednijih postavki prepoznavanja napada.

Slika 16: Izbornik *Security*

Podizbornik *Tasks* omogućava korisniku stvaranje pravila vezanih uz aplikacije i mrežne postavke kroz niz prečaca (eng. *shortcut*) i čarobnjaka (eng. *wizard*). Sastoji se od dviju grupa s nazivima *Common Tasks* i *Wizards*. Slijedi podrobniji opis elemenata:

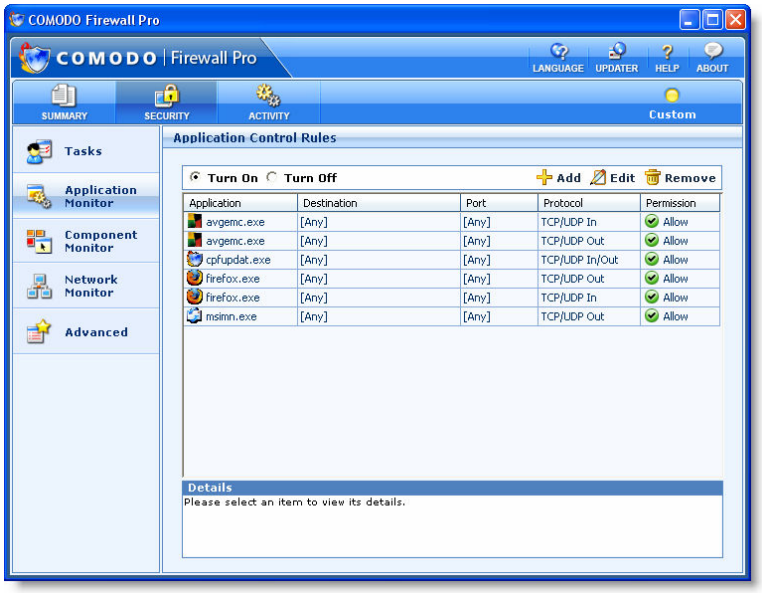
- *Define a New Trusted Application* – pojednostavljen način automatskog stvaranja pravila određujući razinu povjerenja za svaku pojedinačnu aplikaciju,
- *Define a New Banned Application* – ovim postupkom može se odrediti popis aplikacija kojima se izričito ne dozvoljava uspostava veze,
- *Add/Remove/Modify a Zone* – pojedino računalo ili računalnu mrežu može se predstaviti kao zonu kojoj se pristup može dozvoliti ili ne dozvoliti,
- *Send files to Comodo for analysis* – ukoliko korisnik ne može odlučiti treba li omogućiti ili onemogućiti komunikaciju određenoj aplikaciji, spornu aplikaciju može proslijediti proizvođaču vatrozida na daljnju analizu,
- *Check for Updates?* – koristi se za pokretanje postupka nadogradnje, a sam postupak je vrlo jednostavan i prikazan je na sljedećoj slici.



Slika 17: Nadogradnja vatrozida

- *Define a new Trusted Network* – određivanje zone kojoj će se omogućiti ili onemogućiti pristup,
- *Scan for Known Applications* – pregled postojećih aplikacija na sustavu u svrhu njihovog postavljanja u popis aplikacija kojima se sigurnosna pravila automatski postavljaju.

Podizbornik *Application monitor* omogućava korisniku postavljanje sigurnosnih pravila odnosno dozvola vezanih uz aplikacije.



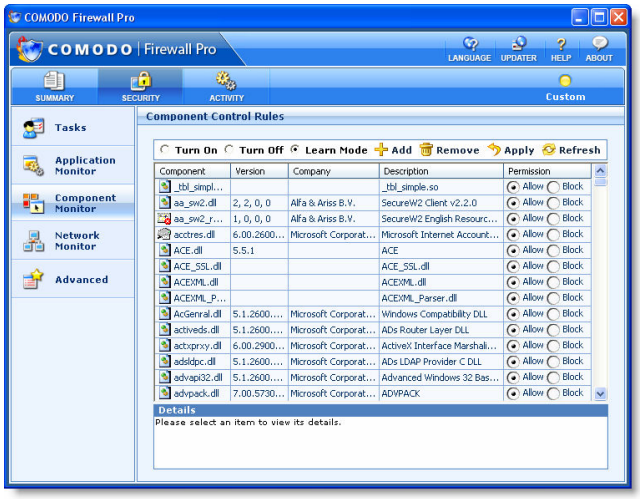
Slika 18: Postavke vezane uz aplikacije

Čitav modul moguće je uključiti i isključiti korištenjem opcija *Turn On* i *Turn Off*, respektivno. Dodavanje novih aplikacija izvodi se odabirom opcije *Add*, a uređivanje postojećih zapisa s *Edit*. Uklanjanje zapisa se obavlja odabirom opcije *Remove*. Popis aplikacija je organiziran u tablicu čiji su stupci redom:

- *Application* – ime aplikacije,
- *Destination* – odredište kojemu aplikacija pokušava pristupiti,
- *Port* – mrežni priključak kojeg aplikacija koristi,
- *Protocol* – određuje protokol koji aplikacija koristi i
- *Permission* – dozvola ili onemogućavanje spajanja.

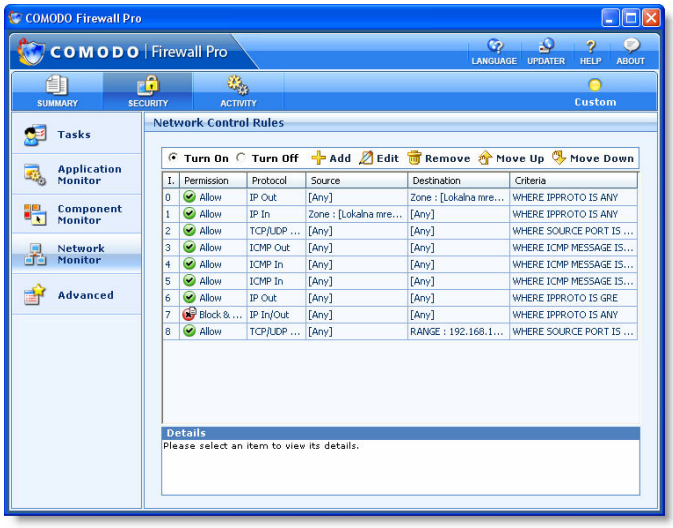
Podizbornik *Component monitor* koristi se za određivanje programskih modula koji su dio aplikacije, ali se ponašaju kao zasebne cjeline i pokušavaju uspostaviti vezu. U tom slučaju komponente imaju potpuno ista prava kao i aplikacije čiji su dio. Comodo provjerava svaki modul zasebno prije nego mu omogući pristup vanjskom svijetu. Često je ovo slučaj kod ActiveX komponenata koje koristi neka aplikacija. Pravila vezana uz komponente mogu se dodavati, uređivati i brisati. Način rada ove komponente vatrozida najčešće je postavljen na *Learning mode* što znači da će vatrozid za svaki pokušaj uspostavljanja veze od korisnika zatražiti dozvolu. Opcije *Turn On* i *Turn off* uključuju i isključuju primjenu postojećih pravila. Tablica u kojoj su pravila određena je stupcima:

- *Component* – naziv komponente,
- *Version* – inačica komponente,
- *Company* – proizvođač komponente (radi lakšeg donošenja odluke o dozvoli),
- *Description* – opis komponente i
- *Permission* – postavljanje ili onemogućavanje pristupa Internetu.



Slika 19: Pravila vezana uz komponente

Podizbornik *Network monitor* omogućava korisniku uređivanje postavki vezanih uz svojstva mrežne komunikacije. Ta se pravila primjenjuju na razini mrežnih paketa i odnose se na postavljanj IP adresa, mrežnih priključaka, protokola i slično. Pravila se mogu dodavati, uređivati i uklanjati. Ukoliko ima više sličnih pravila primjenjuje se ono koje je na vrhu popisa.



Slika 20: Mrežne postavke

Popis se sastoji od:

- *ID* – Rednog broja pravila,
- *Permission* – dozvole,
- *Protocol* – određivanje protokola,
- *Source* – izvorišna IP adresa paketa,
- *Destination* – odredišna IP adresa i
- *Criteria* – potpuni opis pravila.

Posljednji podizbornik *Advanced configuration* jedna je od najvažnijih mogućnosti Comodo vatrozida. Detekcija nedozvoljenog pristupa (eng. *Intrusion detection*) i prevencija (eng. *Intrusion prevention*) napredne su mogućnosti koje ne implementira svaki vatrozid. Ovaj mehanizam obuhvaća analizu mrežnih paketa i njihovo uspoređivanje s poznatim napadima i zlonamjernim uzrocima.

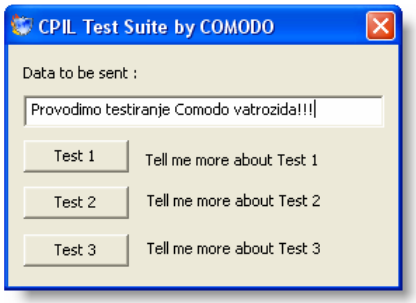
Slika 21: Postavljanje naprednih mogućnosti vatrozida

U nastavku je dan kratak opis pojedine napredne mogućnosti.

- *Application Behaviour Analysis* – analizira se ponašanje aplikacije te se određuju potencijalno opasne (zlonamjerne) aktivnosti prije nego se aplikaciji dopusti pristup Internetu. Na taj način povećan je stupanj ispravnog uočavanja trojanskih konja.
- *Advanced Attack Detection and Prevention* – osigurana je obrana od napada uskraćivanjem resursa (eng. *DoS – Denial of Service*). Kada se to dogodi, vatrozid odlazi u tzv. *Emergency mode* način rada i u njemu ostaje dvije minute. Radi se o prekidu svih veza s vanjskim svijetom i onemogućavanju uspostave novih veza tijekom napada.
- *Miscellaneous* – dio je sučelja koji omogućuje korisniku izmjenu postavki vezanih uz pojavu upozorenja i sl.

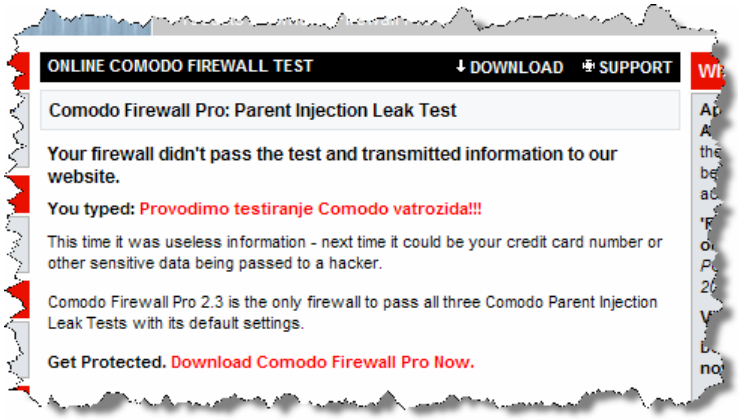
4. Testiranje

Korisnici Interneta svakodnevno su izloženi opasnostima od virusa, crva i ostalih zlonamjernih aplikacija. Osobni vatrozidi tvore prvu liniju obrane od tih aplikacija. Filtriranje mrežnog prometa i praćenje odlaznih veza dvije su važne karakteristike svakog vatrozida. Razvoj zlonamjernih aplikacija napreduje velikom brzinom, a mnoge od njih implementiraju vrlo složene tehnike prikrivanja svojih zlonamjernih aktivnosti. Na taj način jednostavno prolaze mimo sigurnosnih mehanizama vatrozidnih aplikacija. Uvriježen naziv za njih je tehnike propuštanja (eng. *leak techniques*).
Testiranje kvalitete obrane koju pruža vatrozid može se izvesti na više načina. Odabirom opcije *Test your current security configuration* započinje postupak provjere. Unutar web preglednika otvara se web stranica Comodo tvrtke s koje se može preuzeti aplikacija za testiranje. Riječ je o testovima poznatim pod nazivom *Comodo Parent Injection Leak Test Suite (CPILSuite).* Aplikacija se može vidjeti na sljedećem prikazu.



Slika 22: Test vatrozida

Test broj 1 tipičan je pokušaj postavljanja vatrozida u temeljni način rada onemogućavanjem rada u naprednom režimu. Nakon toga pokušava se dodati u memoriji `explorer.exe` datoteci programski kôd koji pokreće web preglednik. To je najčešći princip kojim se služe tzv. *malware* programi. Samo pogrešno postavljeni vatrozidi dopuštaju uspješno izvođenje ovog testa. Ukoliko je vatrozid ranjiv, a ispravno je postavljen, tada je riječ o vatrozidu vrlo slabih karakteristika te se korisnicima savjetuje da ga zamijene.



Slika 23: Test broj 1 - rezultati

U svrhu ovog testa Comodo vatrozid je oslabljen i prvi test je pokazao da vatrozid ne radi dobro. Željeni tekst prenesen je kao parametar na web stranicu. Napadači koriste ovaj mehanizam za prijenos potencijalno osjetljivih podataka poput zaporki, korisničkih imena, brojeva kreditnih kartica i slično. Kada radi ispravno, vatrozid treba uočiti pokušaj zlonamjerne aktivnosti kao što se vidi na prikazu ispod.

Slika 24: Vatrozid je uočio pokušaj napada

Drugi test je nova tehnika testiranja koju je razvila tvrtka Comodo. Većina vatrozida ima mehanizam obrane od napada umetanjem koda u programske biblioteke (eng. *DLL injection attacks*). Proizvođač ovog vatrozida uočio je da Windows Accessibility API (eng. *Application programming interface*) sarži vrlo snažnu funkciju koja se može iskoristiti u zlonamjerne svrhe, a mnogi vatrozidi ju ne uvažavaju. Čitava ideja je umetanje proizvoljne DLL datoteke u `explorer.exe` te prijenos proizvoljnih podataka preko parametara na web stranicu. Oslabljeni Comodo vatrozid propustio je prijenos podataka na web stranicu. Prikazi su identični onima za prvi test. U slučaju potpune funkcionalnosti, Comodo je uspješno prepoznao pokušaj uspostave veze.

Treća provjera je samo proširenje druge provjere. Implementiran je postupak koji još više otežava detekciju ove vrste napada. Ishod je isti kao u prva dva.

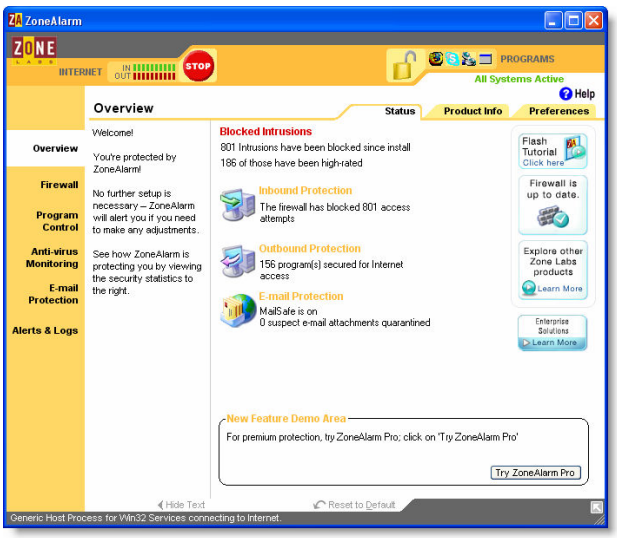
Proizvođač navodi kako je Comodo jedini vatrozid imun na ove napade, a zbog ograničenja opsega ovog dokumenta daljnji testovi nisu provedeni, npr. na vatrozidima drugih proizvođača.

5. Konkurentske aplikacije

Na tržištu je dostupan velik broj vatrozidnih aplikacija. Ne postoji vatrozid koji će zadovoljiti sve sigurnosne zahtjeve svakog korisnika. Ovdje će biti dan pregled nekih od dostupnih osobnih (eng. *personal*) vatrozidnih aplikacija. Osobni *firewall*-i se razlikuju po broju opcija, grafičkim sučeljima, stupnju jednostavnosti konfiguracije i mogućnostima stvaranja izvješća o svojim aktivnostima. U nastavku je prikazano nekoliko najčešće korištenih vatrozida te su dane kratki osvrti na svakog od njih.

5.1. Zone Alarm

Tvrtka Zone Labs proizvela je jedan od najčešće korištenih vatrozida – Zone Alarm. To je besplatna inačica kojoj je dio funkcionalnosti ograničen. Naprednija inačica, Zone Alarm Pro, ima komercijalnu licencu i pruža zavidnu količinu funkcionalnosti. Naprednija inačica nudi zaštitu od *spyware* aplikacija, detekciju sumnjivih poruka elektroničke pošte i slične funkcionalnosti koje nisu temeljni dio vatrozidnih aplikacija. Obje inačice omogućuju postavljanje sigurnosnih zona. Zone Alarm aplikacija udomaćila se među korisnicima osobnih računala, a njezine mogućnosti na razini su prosječnog korisnika.



Slika 25: Zone Alarm

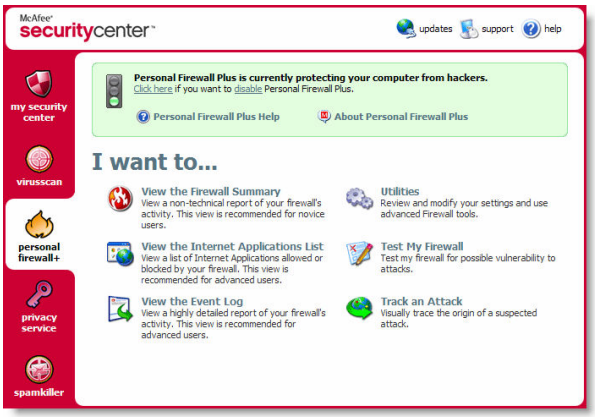
5.2. Norton Personal Firewall

Norton je renomirani proizvođač sigurnosnih aplikacija za osobna računala, a ovim proizvodom ostao je na svojoj razini kvalitete. Vatrozid nije samo vatrozid, nego se s njim isporučuje i *Norton Protection Center* koji integrira cjelovitu zaštitu Windows operacijskog sustava. Korisnici koji žele isključivo vatrozid ovim pristupom neće biti zadovoljni. Paket je dobro rješenje za prosječnog korisnika koji često koristi određen skup aplikacija budući da Norton vatrozid dolazi s već unaprijed određenim sigurnosnim pravilima o dozvolama vezanim uz aplikacije. Što se tiče općih funkcionalnosti, vatrozid omogućuje određivanje vlastitih sigurnosnih pravila te uređivanje niza drugih funkcionalnosti.

Slika 26: Norton Personal Firewall

5.3. McAfee Personal Firewall Plus

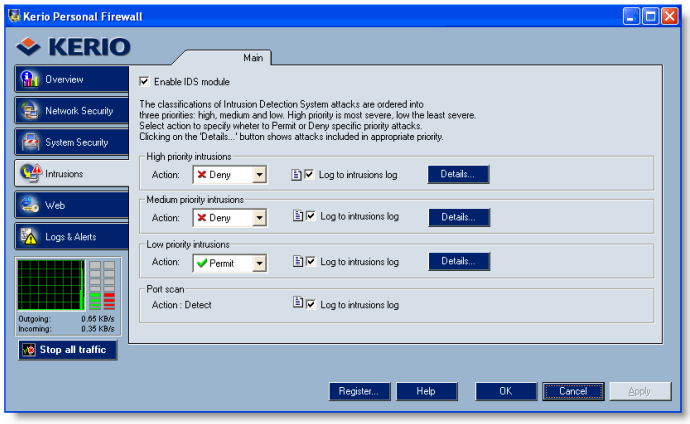
Kao i mnoge sigurnosne aplikacije, i ovaj vatrozid dolazi sa sigurnosnim centrom – aplikacijom koja objedinjuje korištenje svih proizvoda iz kategorije računalne sigurnosti. Vatrozid omogućava stvaranje sigurnosnih pravila kao što je to i uobičajeno, a novitet je da se pristup ili blokiranje pristupa mogu i vremenski ograničiti. Općenito, radi se aplikaciji pristojnih funkcionalnosti s dodatnim naprednim mogućnostima.



Slika 27: McAfee Personal Firewall Plus

5.4. Sunbelt Kerio WinRoute Firewall

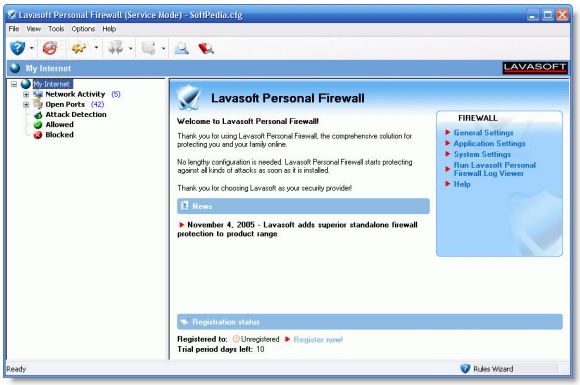
Sunbelt Kerio WinRoute Firewall besplatni je vatrozid čiji razvoj je preuzela tvrtka Sunbelt, a naziv prethodne tvrtke ostavljen je u nazivu paketa kako bi korisnici znali da se radi o proizvodu s tradicijom. Aplikacija posjeduje sve klasične funkcije prosječnog vatrozida te implementira i mogućnost blokiranje reklama i zlonamjernih sadržaja. Paket ima sučelje i na hrvatskom jeziku što će sigurno odgovarati nekim korisnicima. Nažalost, prijevod je dosta nekvalitetan, a temeljna inačica, uz to što je besplatna, ima osrednje mogućnosti.



Slika 28: Sunbelt Kerio WinRoute Firewall

5.5. Lavasoft Personal Firewall

Riječ je o komercijalnom proizvodu tvrtke Lavasoft koja se već dokazala uspješnim programom za uklanjanje *spyware* aplikacija. Ovaj vatrozid je namijenjen osobnim i manjim te srednjim računalnim mrežama. Aplikacija posjeduje sve karakteristične funkcionalnosti prosječnog vatrozida, a između ostalih odlikuje se preglednim sučeljem, posebnim načinom rada ukoliko se uoči napad i sl.



Slika 29: Lavasoft Personal Firewall

5.6. Agnitum Outpost Firewall Pro

Radi se dosta često korištenom komercijalnom paketu. Pored vatrozidnih funkcionalnosti, aplikacija sadrži i mogućnosti filtriranja poruka elektroničke pošte i alat za borbu protiv *spyware* aplikacija. Posjeduje i mogućnost spremanja DNS upita i odgovora (eng. *DNS caching*) za ubrzanje komunikacije na Internetu. Postoji i popis unaprijed određenih aplikacija kojima se automatski dozvoljava promet prema vanjskom svijetu. Vatrozid je primjereniji naprednijim korisnicima s obzirom na mogućnosti izmjene postavki.

Slika 30: Agnitum Outpost Firewall Pro

6. Zaključak

Comodo Firewall aplikacija se pokazala vrlo dobrim izborom obzirom na nekoliko različitih zahtjeva. Između ostalih, tu su i zahtjev za jednostavnošću korištenja, preglednost grafičkog korisničkog sučelja, korištenje što manje resursa i precizno određivanje odnosno onemogućavanje uspostave zlonamjernih veza.

Jedna od važnijih značajki svakako je i besplatnost paketa. Međutim, paket nije u potpunosti besplatno distribuiran nego je njegova potpuna funkcionalnost omogućena samo kod registracije korisnika. Kako je postupak registracije vrlo jednostavan, a njime se dobiva doživotna korisnička licenca, može se slobodno reći kako je riječ o besplatnom paketu.

Broj poruka o pokušaju uspostave konekcije vrlo je velik i u određenim uvjetima može preći razumnu granicu. To ovisi o broju prepoznatih programskih paketa instaliranih na sustavu. Valja primijetiti kako se korisnik ne smije u potpunosti osloniti na vatrozid budući da ljudski faktor ima velikog udjela u sigurnosti računalnih sustava. Naime, korištenje prejednostavnih zaporki na računalu lako je probiti bez obzira na kvalitetu vatrozida koji brani sustav. Korisnicima se preporuča da budu pri oprezu bez obzira koje vatrozidno rješenje koriste.

7. Reference

[1.] Comodo Firewall, http://www.personalfirewall.comodo.com, veljača 2007.

[2.] Comodo Personal Firewall 2.0: Full Review, http://www.pcmag.com/article2/0,1895,1969207,00.asp, svibanj 2006.

[3.] Bug: Comodo Firewall 2.3.6, http://www.bug.hr/program/index.asp?id=74974&page=1, studeni, 2006.

[4.] Comodo Firewall 2.3 vs. The Leak Tests, http://www.personalfirewall.comodo.com/Comodo_Firewall_2.3_vs_The_Leaktests.pdf, veljača 2007.

[5.] Comodo Firewall Pro2.4 User Guide, https://support.comodo.com/, veljača 2007.

[6.] Jeff Tyson: How Firewalls Work, http://www.howstuffworks.com/firewall.htm, veljača 2007.

[7.] Agnitum Outpost Firewall Pro, http://www.agnitum.com/products/outpost/, veljača 2007.

[8.] Lavasoft Personal Firewall, http://www.lavasoft.de/software/firewall/, veljača 2007.

[9.] Sunbelt Kerio WinRoute Firewall, http://www.sunbelt-software.com/Kerio-Server.cfm, veljača 2007.

[10.] Zone Alarm, http://www.zonelabs.com/, veljača 2007.

[11.] McAfee Personal Firewall Plus, http://www.mcafee.com/, veljača 2007.

[12.] Norton Personal Firewall, http://www.symantec.com/sabu/nis/npf/, veljača 2007.