HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

SSL-Explorer

CCERT-PUBDOC-2005-01-104

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

Pojam VPN-a (eng. *Virtual Private Network*) poznat je i opisuje tehnologije koje se koriste za povezivanje u sigurne virtualne privatne mreže preko nesigurne javne infrastrukture. VPN tehnologije koriste se za povezivanje udaljenih računala, udaljenih lokacija, poslovnih partnera ili kupaca.

Općenito govoreći, VPN mreže mogu se implementirati korištenjem raznih tehnologija i komunikacijskih kanala kao što su npr. Internet, dijeljene ATM mreže ili druge infrastrukture koje pruža ISP.

Također, VPN sustavi mogu biti implementirani sklopovski ili programski, a često se integriraju i u postojeće sustave (operacijske sustave na poslužiteljima ili vatrozide).

Osnovni cilj VPN sustava je tuneliranje podataka i istovremeno osiguranje integriteta i tajnosti podataka. Na IP mrežama postoji nekoliko različitih tehnologija koje se koriste za implementaciju VPN sustava:

- PPTP,
- IPSec,
- L2TP,
- SSH,
- SSL.

Neke od tih tehnologija opisane su u drugim CERT-ovim dokumentima (CCERT-PUBDOC-2003-02-05: Osnovi koncepti VPN tehnologije – http://www.cert.hr/filehandler.php?did=40 i CCERT-PUBDOC-2004-01-58: IPSec – http://www.cert.hr/filehandler.php?did=89).

Ovaj dokument opisuje SSL Explorer, *open source* programsko rješenje za implementaciju VPN servisa korištenjem SSL-a.

Općenito govoreći, korištenje SSL-a (eng. *Secure Socket Layer*) za implementaciju VPN sustava relativno je novo.

SSL bazirani VPN sustavi tajnost, integritet i autentikaciju podataka temelje na samom SSL protokolu (CCERT-PUBDOC-2000-07-01: Secure Socket Layer – http://www.cert.hr/filehandler.php?did=70). SSL Explorer, programski paket koji je opisan u ovom dokumentu konkretno koristi raširen HTTPS protokol tj. HTTP preko SSL-a.

Najveća prednost SSL VPN sustava je u tome što ne zahtijevaju posebne aplikacije na klijentskoj strani, već je za uspostavu VPN-a s klijentske strane dovoljan bilo koji Web preglednik s ugrađenom SSL podrškom (što podržavaju svi preglednici). Na taj način VPN pristup moguć s bilo koje lokacije gdje postoji veza na Internet i mogućnost korištenja Web servisa (Internet caffe, Internet kiosci, PDA uređaji i sl.). SSL Explorer dodatno zahtijeva i instaliranu podršku za Javu, no u većini slučajeva to ne predstavlja ograničenje.

S druge strane, nedostatak SSL VPN sustava je taj što udaljenim korisnicima ne pruža punu LAN funkcionalnost, već ograničava pristup samo na Web-bazirane aplikacije. U većem broju slučajeva i za veći broj korisnika to ne mora biti ograničavajući faktor, no kada je potrebno osigurati pristup aplikacijama i servisima kao što su SAP ili baze podataka, te pristup na razini transportnog ili mrežnog sloja to postaje nedostatak. SSL Explorer, osim aplikacija koje dolaze s njim, daje API sučelje u kojem je moguće razvijati vlastite aplikacije i na taj način osiguravati tražene VPN funkcionalnosti.

U nastavku dokumenta opisan je proces instalacije i konfiguracije SSL Explorer VPN sustava te način njegovog korištenja. Na kraju je opisano ponašanje pri radu, sigurnosne značajke, te je dana i ukupna ocjena kvalitete SSL Explorer paketa.

2. Instalacija

Pretpostavka je da će se SSL Explorer instalirati na računalo/poslužitelj unutar demilitarizirane zone (DMZ). Preporučeni sklopovski zahtjevi su PIII procesor, 512MB RAM-a i 150MB diskovnog prostora.
Cijeli paket napisan je u Javi i kao takav se može pokrenuti na bilo kojem sustavu s instaliranim Java 5 Runtime Environment. Trenutno su službeno podržane platforme:

- Windows 2000/XP/2003 i
- Red Hat Linux 8.0 i noviji.

Instalacijski paketi u izvršnom (.exe) formatu za Windows sustave i RPM formatu za Linux sustave mogu se dohvatiti na stranici http://sourceforge.net/projects/sslexplorer.
Instalacija na Windows sustavima je jednostavna i izvodi se korištenjem pomoćnika (*Wizarda*). Iako će instalacijski postupak provjeriti da li na sustavu postoji Java 5 Runtime Environment i instalirati ga ukoliko ne postoji, zbog uočenih problema pri takvom postupku, preporuča se prethodna ručna instalacija Java paketa.
Prije samog kraja postupka instalacije potrebno je pokrenuti SSL Explorer u tzv. *Setup* načinu rada i podesiti konfiguracijske postavke nužne za ispravno funkcioniranje paketa. Detaljni opis konfiguracijskih postavki dan je u poglavlju 3.
Nakon uspješne instalacije u *Programs* izbornik dodaje se programska grupa SSL Explorer.
Sam paket na Windows sustave instalira se kao servis, a njegovo ručno ili automatsko pokretanje i zaustavljanje (u normalnom načinu rada) može se provesti iz *Services* konzole *Administrative Tools*-a.
Setup način rada pokreće se korištenjem prečaca iz definirane programske grupe.

3. Konfiguracija

3.1. Setup način rada

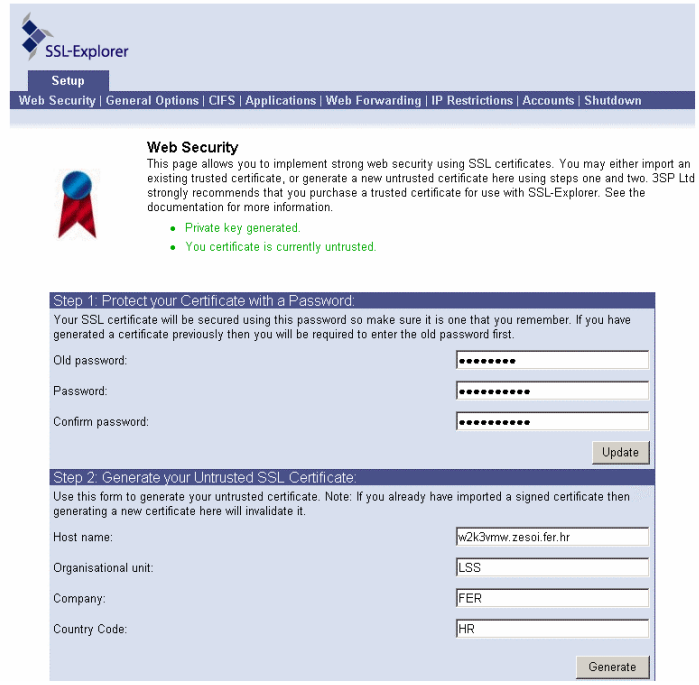
Da bi SSL Explorer uopće mogao biti pokrenut potrebno je podesiti osnovne konfiguracijske postavke.
Inicijalna konfiguracija (odnosno *Setup* način rada) omogućava podešavanje sljedećih grupa postavki:

- Web Security,
- General Options,
- CIFS,
- Applications,
- Web Forwarding,
- IP Restrictions,
- Accounts i
- Shutdown.

Ovisno o postavkama **General Options** kartice moguće je podešavanje dodatnih grupa postavki:

- Active Directory i
- Client.

Web Security kartica omogućava podešavanje HTTPS protokola, odnosno generiranje i instalaciju digitalnog certifikata nužnog za ispravno funkcioniranje SSL-a. Prije svega je potrebno postaviti zaporku kojom se štiti certifikat i definirati osnovne parametre certifikata (ime računala, organizacija, tvrtka i oznaka države). Nakon toga je moguće generirati vlastiti certifikat, te ga opcionalno u obliku CSR (eng. *certificate signing request*) zahtjeva poslati odgovarajućem CA (eng. *certificate authority*) na ovjeravanje i zatim naknadno instalirati.
Za uobičajenu uporabu SSL Explorer-a u većini slučajeva dovoljno je korištenje vlastito generiranog digitalnog certifikata.

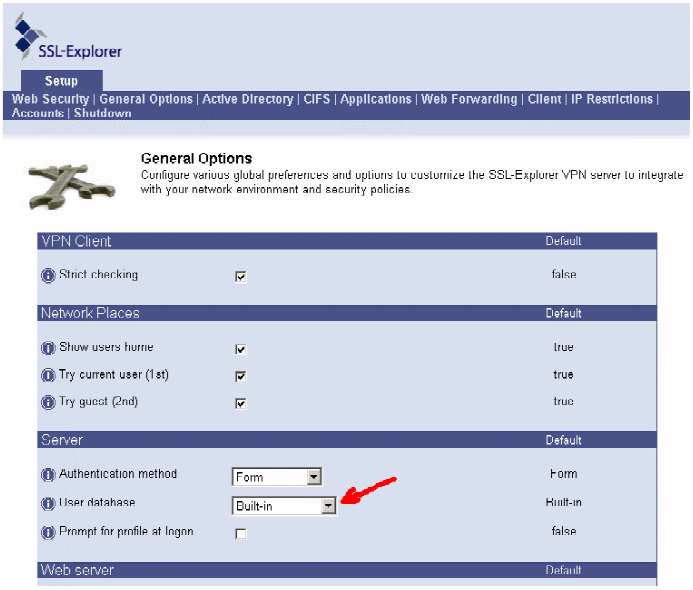


Slika 1: Generiranje SSL certifikata

General Options omogućava podešavanje osnovnih postavki SSL Explorer-a. Postavke raspoložive kroz ovu karticu su grupirane na sljedeći način:

- VPN Client – uključivanjem ove opcije moguća je provjera postavki VPN klijenta koji pristupa SSL Exploreru i ograničavanje pristupa.
- Network Places – omogućava podešavanje postavki vezanih uz mrežni pristup (prikaz korisničkog *home* direktorija i korištenje autentikacijskih parametara za pristup mrežnim resursima).
- Server – ova grupa postavki omogućava podešavanje načina autentikacije korisnika. Moguće je korištenje ugrađene baze korisnika ili Active Directoryja, a također je moguće podesiti i način autentikacije (korištenjem formi ili korištenjem HTTP *basic* autentikacije).
- Web server –kroz ovu grupu postavki moguće je podesiti parametre (Apache) Web poslužitelja na kojem je pokrenut SSL Explorer. Najvažniji parametar u ovoj grupi je TCP port na kojem je pokrenut poslužitelj (predefinirano 443). Ukoliko se na istom računalu-poslužitelju već koristi neki drugi poslužitelj koji omogućava SSL pristup, potrebno je promijeniti predefinirani port.
- Proxies – kroz ovu grupu postavki moguće je podešavanje postavki opcionalnih HTTP i SOCKS *proxy* poslužitelja (ime, autentikacijski podaci, iznimke).

CIFS kartica omogućava podešavanje opcija vezanih uz Microsoftov CIFS (eng. *Common Internet File Services*) protokol namijenjen dijeljenju datoteka na mreži. Osnovne opcije koje je moguće podesiti su predefinirana Windows domena, predefinirani korisnički račun za pristup (korisničko ime i zaporka), predefinirani račun za goste, te brojne NetBIOS opcije.



Slika 2: Podešavanje načina autentikacije u osnovnim postavkama SSL Explorer-a

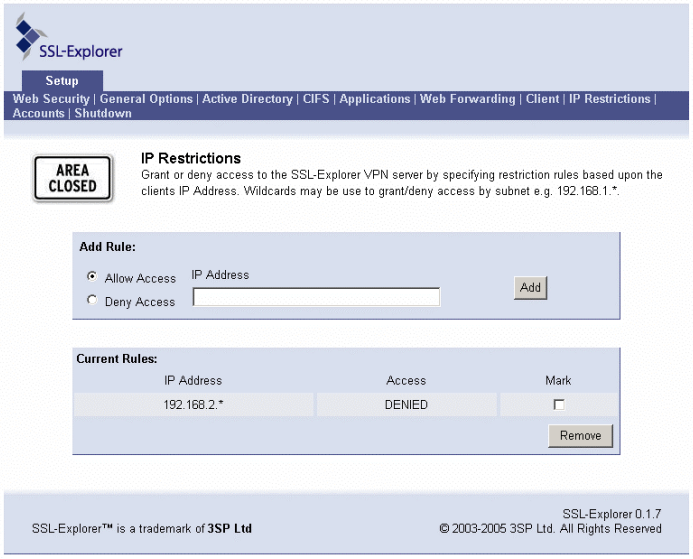
Applications kartica omogućava uključivanje/isključivanje aplikacija koje su korisnicima dostupne za korištenje preko VPN-a uspostavljenog kroz SSL Explorer. Trenutna inačica SSL Explorera podržava sljedeće aplikacije:

- Linux rdesktop command,
- Microsoft RDP Client,
- PJIRC Java-based Webchat Client,
- Remote Desktop Protocol (RDP) i
- Virtual Network Computing (VNC).

Većina trenutno dostupnih naredbi odnosi se na razne alate za udaljeni pristup računalu (eng. *remote desktop*), s izuzetkom *Java PJIRC* aplikacije koja predstavlja klijenta za IRC *chat*. Također, moguće je dodavanje i drugih aplikacija sa 3SP Weba (http://www.3sp.com), kada one budu dostupne, ili dodavanje samostalno razvijenih aplikacija. Samostalni razvoj aplikacija moguć je uz korištenje raspoloživog API (eng. *application programming interface*) sučelja.

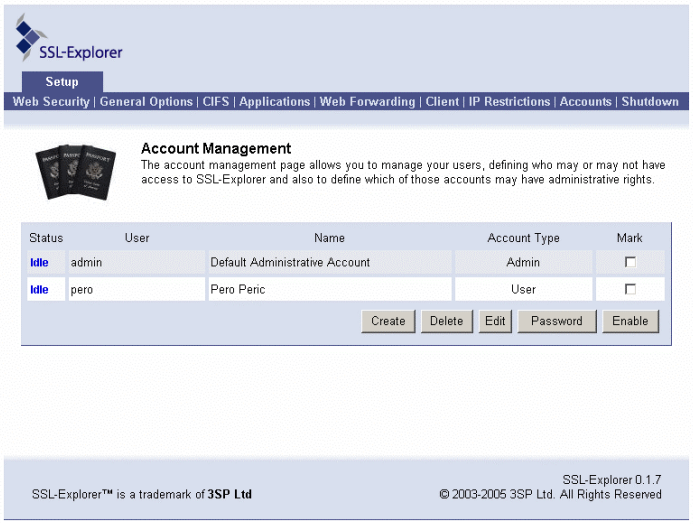
Web Forwarding kartica omogućava podešavanje postavki pri korištenju Web Forwarding opcije (svaki korisnik može koristiti tu opciju). Moguće je podesiti radni direktorij (predefinirano `%TMP%/webcache`), maksimalno zauzeće prostora i broj objekata po korisniku, te uključiti brisanje datoteka nakon odjave korisnika.

IP Restrictions kartica omogućava ograničavanje pristupa na pojedine IP adrese. Moguće je podešavanje pravila koja omogućavaju pristup (eng. *allow*) i zabranjuju pristup (eng. *deny*). Također je moguće i korištenje tzv. *wildcarda* (*) za identifikaciju čitavih mreža (npr. `192.168.2.*`). Korištenje rangova IP adresa nije moguće, što ograničava mogućnost preciznog podešavanja pristupa za pojedine grupe IP adresa unutar određenih mreža.



Slika 3: IP restrikcije mogu se primijeniti na pojedino računalo ili cijelu mrežu

Accounts kartica omogućava dodavanje novih korisnika SSL Explorera i to isključivo ukoliko se koristi ugrađena baza podataka. Kroz *Accounts* karticu moguće je dodavati i brisati korisnike, odnosno korisničke račune, uređivati korisničke račune (ime i prezime, e-mail adresa i ime korisničkog računa), mijenjati zaporku korisnicima i postavljati njihove ovlasti. SSL Explorer prepoznaje obične korisnike i administratore.



Slika 4: Korištenje ugrađene baze korisnika

Ukoliko se kao baza korisnika koristi *Active Directory* korištenje postavki ove kartice je onemogućeno.
Shutdown kartica omogućava zaustavljanje *Setup* načina rada SSL Explorera. Prilikom svake promjene konfiguracije SSL Explorera u *Setup* načinu rada potrebno je zaustaviti *Setup* način rada i pokrenuti SSL Explorer u normalnom načinu (kao servis), pošto u *Setup* načinu rada korisnicima pristup nije omogućen.
Sve opisane konfiguracijske postavke dostupne u *Setup* načinu rada dostupne su i u normalnom računu rada za korisnike koji imaju administrativne ovlasti na sustavu. Zbog toga se *Setup* način rada koristi samo pri inicijalnoj konfiguraciji i u iznimnim slučajevima (problemi pri radu i sl.).

3.2. Opcionalne konfiguracijske postavke

Opcionalne konfiguracijske postavke raspoložive su ovisno o postavkama podešenim u *General Options* kartici.

Client. Ukoliko je u *General Options* kartici uključena *VPN client* opcija *strict checking* pojavljuje se dodatna kartica *Client* u kojoj je moguće ograničiti VPN pristup samo na klijente koji zadovoljavaju uvjete: proizvođač Java paketa kojeg klijent koristi, inačica Jave, arhitektura i inačica operativnog sustava i razina zakrpanosti (samo korištenjem Java Runtime). Sve te opcije moguće je podesiti za predefinirane operativne sustave (Windows 95/NT/XP, Mac OS, Linux, Solaris, OS/2, AIX, HP-UX i FreeBSD).

Active Directory. Ukoliko je u *General Options* kartici podešeno da se za autentikaciju korisnika koristi *Active Directory*, pojavljuje se dodatna kartica *Active Directory* u kojoj je moguće podesiti postavke bitne za takav način autentikacije. U tom slučaju je nužno podesiti ime Windows domene, FQDN DC (eng. *domain controller*) poslužitelja i TCP port na kojem je pokrenut *Active Directory* servis (predefinirano 389).

Također, potrebno je navesti grupu korisnika koja predstavlja administratore. Korisnici iz te grupe u tom slučaju imat će administrativna prava pristupa SSL Explorer VPN sučelju. Predefinirano je postavljena grupa *Administrators* koja se odnosi na administratore Windows domene.

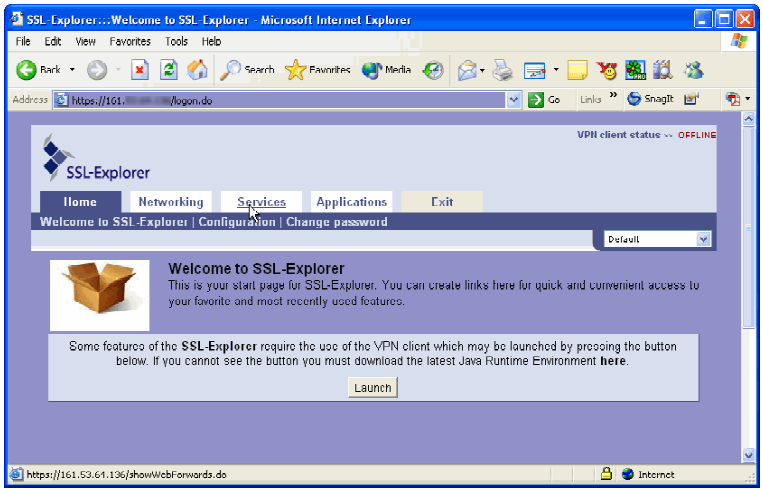
Također, u slučaju da se svi korisnici i grupe korisnika koje će koristiti SSL Explorer VPN pristup ne nalaze u predefiniranom *containeru Active Directory* servisa (*Users*), odnosno nalaze se u nekoj zasebnoj organizacijskoj jedinici (OU), potrebno je kroz sučelje definirati LDAP putanju za te korisnike i grupe.

Slika 5: Podešavanje postavki za Active Directory autentikaciju

4. VPN pristup korisnika

VPN pristup korisnika realiziran je kroz Web sučelje. Korisnik iz Web preglednika, korištenjem HTTPS protokola pristup sučelju SSL Explorera i koristi raspoložive opcije. Jedini zahtjev na klijentskoj strani je instalirana podrška za Javu.

Prilikom spajanja korisnik se mora autenticirati. Autentikacija se provodi korištenjem Web forme ili HTTP Basic autentikacijom, ovisno o konfiguraciji SSL Explorera. Nakon uspješne autentikacije korisnik je prijavljen za rad, no VPN klijent nalazi se u *offline* načinu rada, u kojem je moguće samo podešavanje postavki i promjena zaporke. Da bi dobio kompletnu funkcionalnost, odnosno mogućnost korištenja VPN servisa, korisnik mora preći u *online* način rada, što se postiže pritiskom na gumb u početnom prozoru VPN sučelja.



Slika 6: Korisničko sučelje SSL Explorer-a

Korisniku su na raspolaganju tri grupe VPN usluga koje može koristiti:

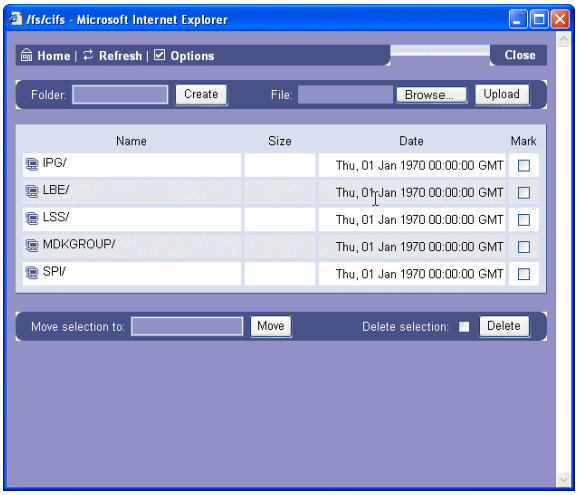
- Networking,
- Services i
- Applications.

Networking omogućava korisniku dvije mogućnosti:

- Network Neighbourhood – VPN pristup CIFS sustavu lokalne računalne mreže. Tim sučeljem korisniku je omogućena funkcionalnost Windows *Network Neighborhood* alata. Kroz Web sučelje korisnik može pregledavati računala, grupe računala i domene te pristupati dijeljenim resursima: mapama (eng. *folder*) i datotekama. Pristup resursima ograničen je na prava pristupa koja korisnik ima (unesena u konfiguraciju ili definirana eksplicitno prilikom pristupa pojedinom resursu) ili na ovlasti gosta (ako je u administrativnom sučelju podešen i omogućen takav pristup).

  Dohvaćanje i upload datoteka kroz ovo sučelje je riješeno vrlo efikasno. Postoji i mogućnost prikaza skrivenih datoteka (eng. *hidden files*), te mogućnost sortiranog prikaza.

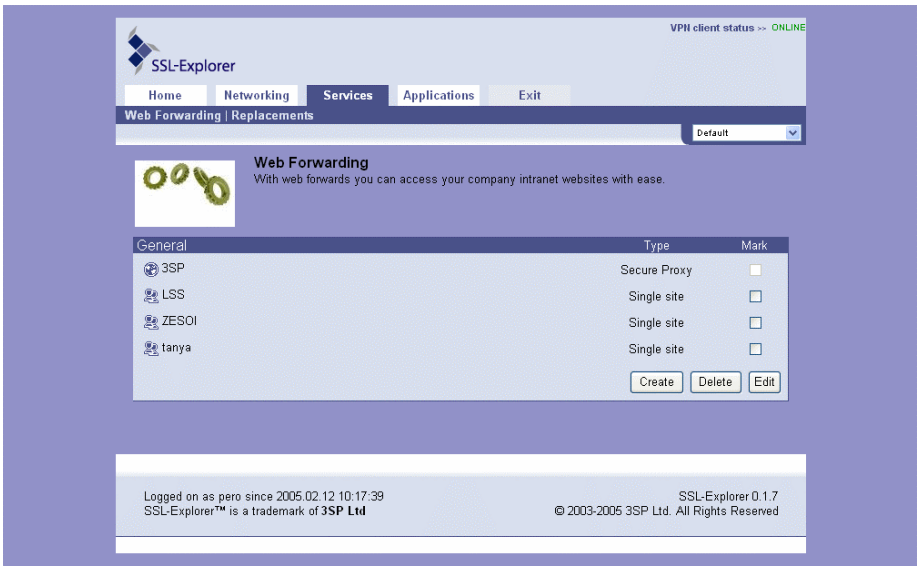
- SSL-Tunneling – omogućava tuneliranje bilo kojeg TCP ili UDP protokola između klijenta i računala/poslužitelja na lokalnoj mreži.



Slika 7: Network Neighbourhood funkcionalnost SSL Explorer-a

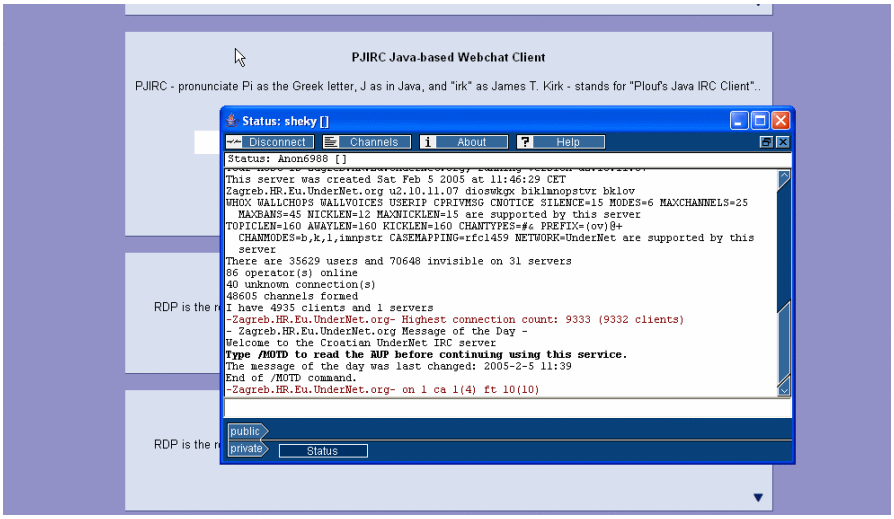
Services omogućava korisniku korištenje dviju opcija:

- Web forwarding – korištenjem ove opcije korisnik može podesiti pristup Web resursima korištenjem *forwardinga* ili sigurnog *proxyja*.
- Replacements – korištenjem ove opcije korisnik može korištenjem regularnih izraza (eng. *regular expressions*) vršiti zamjenu URL-ova ili drugih Web sadržaja koji se dohvaćaju. Korištenje ove opcije preporuča se samo iskusnim korisnicima.



Slika 8: Korištenje Web forwardinga kroz SSL VPN tunel

Applications – omogućava VPN pristup lokalnoj mreži ili udaljenim servisima korištenjem raspoloživih aplikacija (raspoložive aplikacije se dodaju ili brišu kroz administrativno sučelje SSL Explorera). Sa SSL Explorer paketom trenutno dolaze aplikacije za udaljeno administriranje računala korištenjem RDP (eng. *remote desktop/display protocol*) i VNC (eng. *virtual network computing*) protokola te Java bazirani IRC klijent.



Slika 9: Pristup IRC-u korištenjem SSL Explorer VPN-a

4.1. Korisnička konfiguracija

Svaki korisnik ima mogućnost podešavanja određenog broja postavki (*Configuration* kartica) podijeljenih u četiri grupe:

- VPN Client – omogućava podešavanje postavki VPN klijenta (automatsko pokretanje, periodi neaktivnosti, proxy postavke itd.).
- Network Places – omogućava podešavanje postavki za *Network Neighborhood* pristup (način sortiranja datoteka, prikaz nevidljivih datoteka itd.).
- User Interface – omogućava promjenu predefiniranih CSS predložaka Web sučelja.
- CIFS – omogućava podešavanje predefiniranih autentikacijskih podataka (korisničko ime, zaporka, Windows domena).

Također, moguće je generiranje profila sa zasebno definiranim postavkama.

5. Administrativni pristup

Administrativni pristup omogućen je korisnicima koji imaju administrativne ovlasti na sustavu. Korisnicima s tim ovlastima, prilikom prijave za rad, osim opisanih mogućnosti, na raspolaganju su i dvije dodatne kartice:

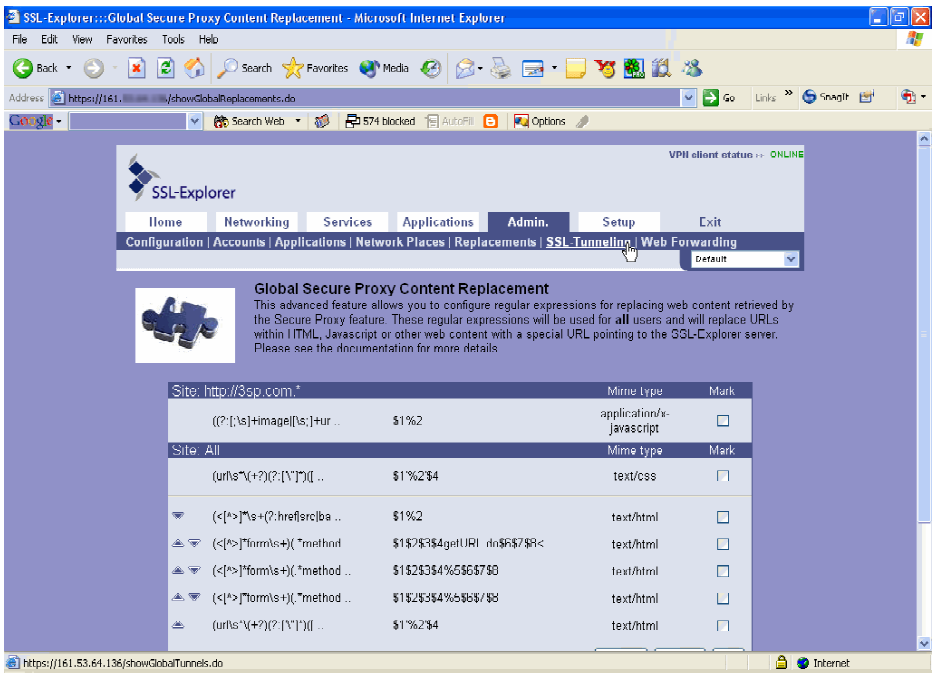
- Admin i
- Setup.

Setup opcije omogućavaju konfiguraciju paketa kako je to opisano u poglavlju 3, dok Admin sučelje administratoru daje mogućnost upravljanja SSL Explorerom kroz sljedeće opcije:

- Configuration,
- Accounts,
- Applications,
- Network places,
- Replacements,
- SSL Tunneling i
- Web Forwarding.

Configuration omogućava administratoru globalno podešavanje predefiniranih konfiguracijskih vrijednosti (poglavlje 4.1). Neke od tih konfiguracijskih vrijednosti korisnici mogu promijeniti prema svojoj želji, bez obzira na administrativne postavke.

Accounts omogućava upravljanje korisničkim računima (ako se koristi ugrađena baza korisnika). **Applications**, **Network Places**, **Replacements**, **SSL Tunneling** i **Web Forwarding** omogućavaju globalno podešavanje opcija opisanih u poglavlju 4.



Slika 10: Dio administrativnog sučelja

6. Ponašanje pri radu

Sam SSL Explorer kao VPN sustav za pristup lokalnoj mreži prvenstveno je zamišljen za manje organizacije. Samo korištenje SSL VPN pristupa vrlo je jednostavno i ne zahtijeva nikakve intervencije na klijentskoj strani osim instalacije Java podrške.

Korisničko sučelje je jednostavno i funkcionalno, sve stranice i aplikacije učitavaju se brzo (što često zna biti problem s Java aplikacijama), što rad s SSL Explorerom korisniku čini ugodnim.

Mogućnost integracije s *Active Directory* servisom također je opcija koju treba istaknuti. Nažalost, prilikom testiranja pokazalo se da postoje poteškoće, te integraciju nije bilo moguće provesti (na forumu projekta to je također uočeno kao problem).

Slični problemi postoje i s RDP klijentima od kojih neki ne funkcioniraju ispravno.

Obzirom da je trenutna inačica programa 0.1.7, za očekivati je da će opisani nedostaci biti uklonjeni u novijim inačicama. Također, podrška za FTP u postojećoj inačici ne postoji, no očekuje se da će se ona pojaviti u budućnosti.

7. Sigurnost

Uspostava VPN pristupa korištenjem SSL-a je rješenje koje zadovoljava sigurnosne zahtjeve velikog broja sustava. Da bi se razina sigurnosti podigla na još višu razinu u SSL Explorer bi bilo poželjno ugraditi i mogućnost klijentske autentikacije korištenjem digitalnih certifikata, no bez obzira na to sama komunikacija korištenjem SSL kanala može se smatrati sigurnom.

Što se tiče samog koncepta, SSL Explorer ima određenih nedostataka. Prvenstveno se to odnosi na mogućnost pokretanja paketa u *Setup* načinu rada bez korištenja zaporke. Rizik koji proizlazi iz tog nedostatka ipak nije kritičan, pošto je za to potrebna mogućnost lokalnog pristupa računalu/poslužitelju na kojem je pokrenut SSL Explorer.

Većim nedostatkom može se smatrati bilježenje zaporki prilikom prijave korisnika za rad i njihova pohrana u *log* datoteci u otvorenom tekstu. Mogućnost da bilo koji korisnik dođe do zaporki drugih korisnika, pa makar on bio i administrator sustava nije prihvatljiva sa sigurnosnog stajališta.

8. Zaključak

SSL VPN sustavi vrlo su popularni, jer uz vrlo male zahvate na klijentskoj strani mogu omogućiti VPN funkcionalnost koja može zadovoljiti potrebe velikog broja korisnika. SSL Explorer je *open source* rješenje koje se bazira na toj tehnologiji. Činjenica da je besplatan svakako mu ide u korist. Također, solidno korisničko sučelje, te deklarirana mogućnost integracije s *Active Directory* servisom su mu svakako dobre strane. Ograničen broj inicijalno dostupnih aplikacija (što uključuje i nepostojanje FTP podrške) ograničavajući je faktor, a isto se može utvrditi i na probleme pri radu (*Active Directory* autentikacija, problemi radom RDP aplikacija), te spomenute konceptualne sigurnosne nedostatke.

Zbog spomenutih nedostataka, SSL Explorer, iako potencijalno vrlo praktično rješenje za manje organizacije, u ovom trenutku nije preporučljivo koristiti u produkcijskom okruženju. Međutim, ukoliko novije inačice isprave spomenute manjkavosti, SSL Explorer alat mogao bi postati odličan VPN sustav prikladan za korištenje u priličnom broju tvrtki.