SSL, TLS, STARTTLS - sličnosti i razlike

SSL (Secure Sockets Layer) vam je možda najpoznatiji od prije kao SSLeay, sustav koji je omogućavao sigurni, odnosno enkriptirani promet između klijenta i poslužitelja. Najčešće ga se instaliralo kao dodatak u Apache u prvim on-line web trgovinama. Prvu inačicu SSL-a je napisao Netscape, i ona nije ugledala svjetlo dana, nego je vrlo brzo zamijenjena inačicom 2.0 u veljači 1995. godine. SSL (i TLS) se danas bazira na OpenSSL biblioteci otvorenog koda.

SSL je u svojim inačicama 2.0 i 3.0 zaživio i u mnogim drugim primjenama, koje do tada nisu imale podršku za siguran prijenos podataka preko TCP/IP mreže (ili su imale neka vlastita rješenja).

Par godina kasnije, protokol je dodatno standardiziran i opisan u RFC-u 2246, te je preimenovan u TLS (Transport Layer Security). Može se reći da je TLS 1.0 nadgradnja SSL-a 3.0, te se ponegdje može pronaći da je TLS 1.0 zapravo SSL 3.1, no uglavnom ćete sresti da je TLS == SSL3. No, ova dva protokola nisu u potpunosti identična, pa to treba imati na umu. Iako se protokoli pomalo razlikuju, aplikacije će znati prijeći sa TLS-a na SSL3

Danas nije poželjno rabiti bilo koju inačicu SSL-a nižu od 3. Aktualna je inačica TLS/a 1.2, izašla 2008. godine.

Dolazimo do pojma STARTTLS. STARTTLS nije nikakav poseban protokol, nego se upotrebljava kada želimo neenkriptirani link pretvoriti u enkriptirani. Ovo se najčešće rabi kod mail klijenata i poslužitelja, primjerice u Postfixu. Ovo je drugačije ponašenje nego primjerice kod HTTPS-a, koji odmah dogovora enkriptirani kanal (dakle, radi na drugom OSI sloju).

Konkretno, kako ćemo znati da određeni SMTP poslužitelj podržava TLS? Spojit ćemo se na port 25 i vidjeti koje opcije poslužitelj nudi:

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.domena.hr.
Escape character is '^]'.
220 posluzitelj.domena.hr ESMTP Postfix (Debian/GNU)
ehlo test.hr
250-posluzitelj.domena.hr
250-PIPELINING
250-SIZE 20000000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
starttls
220 2.0.0 Ready to start TLS
^C
#
```


Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Iz ispisa možemo saznati mnoge zanimljive stvari (npr. poslužitelj podržava poruke do 20 MiB i SMTP AUTH autentikaciju). No, nas zanima samo redak STARTTLS ukucavanjem ključne riječi "starttls" pokrećemo enkripciju, što možemo vidjeti po poruci:

```
220 2.0.0 Ready to start TLS
```

Sada će prijenos maila biti enkriptiran i siguran, naravno, sve dok ne dođe u korisnikov mailbox i time izgubimo uvid što se dalje s porukom događa.

Do ovdje je vjerujemo bilo sve jasno. No, kako svaki protokol koji rabi TLS dobiva novi port, te da se u nekim slučajevima promet može odvijati preko "starog" porta (npr. 25). Na kraju, pojedini softveri mogu imati malo drugačiju terminologiju, što na kraju može dovesti do zbunjenosti kako korisnika, tako i sistemaca.

Za početak, navest ćemo uobičajene portove i njihove "sigurne" inačice (svi portovi su TCP):

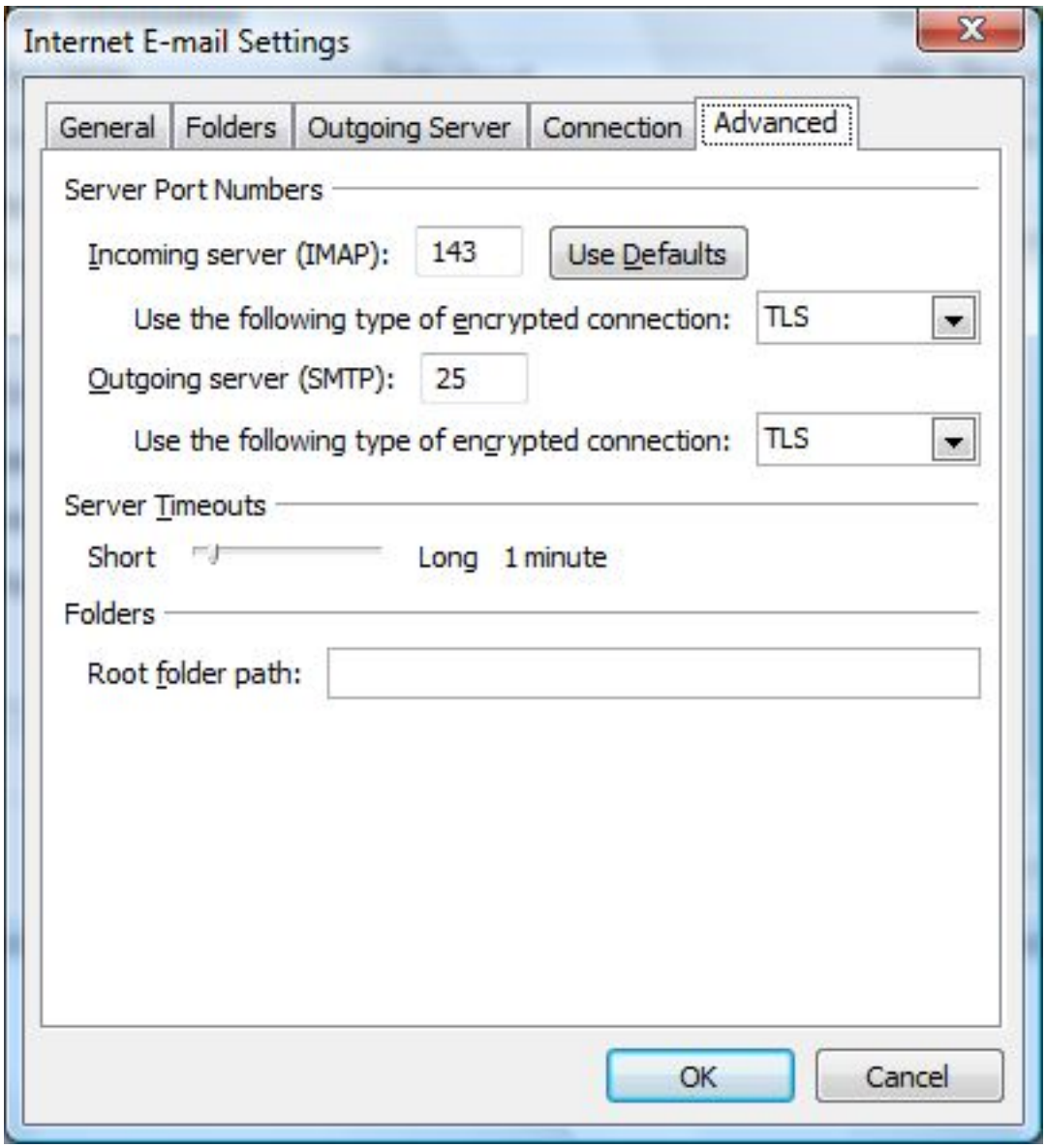
```
smtp 25 Simple Mail Transfer
submission 587 Submission for Simple Mail Transfer
smtps 465 smtp protocol over TLS (was ssmtp)

http 80 World Wide Web HTTP
https 443 http protocol over TLS

pop3 110 Post Office Protocol - Version 3
pop3s 995 pop3 protocol over TLS

imap 143 Internet Message Access Protocol
imaps 993 imap4 protocol over TLS

ldap 389 Lightweight Directory Access Protocol
ldaps 636 sldap ldap protocol over TLS
```

Prvo stvar, svaki ne-enkriptirani protokol ima svoj port, a svaki enkriptirani drugačiji, preko kojeg ide identičan promet, samo je razlika u tome što je enkriptiran.

Drugo, enkripcija može ići i preko starog porta, ako to podržava poslužitelj, ali i klijent (naveli smo primjer starttls naredbe koja radi upravo to).

Kako onda uključiti ove enkripcijske protokole u najpopularnijim programima?

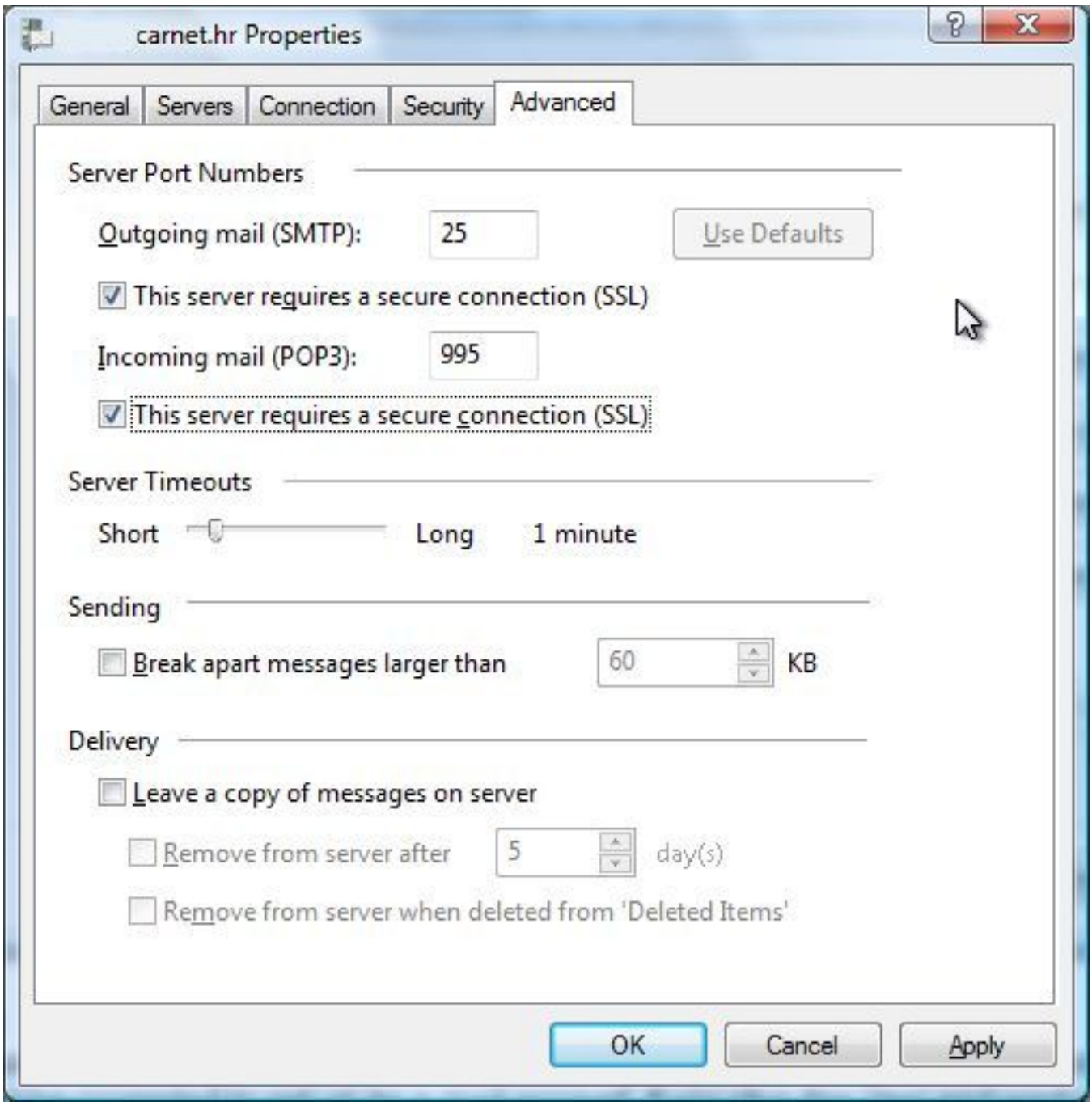
Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr



Za **Outlook**, odite na Tools -> Account Settings -> <dvoklik na profil> -> More Settings -> Advanced -> <odaberite SSL, TLS ili AUTO> za "Incoming" i "Outgoing" poslužitelje.

Ukoliko odaberete SSL, port za dolazni IMAP poslužitelj će se promijeniti na 993 (imaps), dok TLS podržava i enkripciju preko starog porta (slično je i za POP3 poslužitelj). Ovo je važno ukoliko ne želite u vatrozidu otvarati nove portove. Također, Outlook odmah nudi da testirate navedene postavke, pa to učinite. U logovima na poslužitelju ćete vidjeti zašto ne radi, ako se pojavi problem (ne zaboravite prilagoditi vatrozid između klijenta i poslužitelja!).

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr



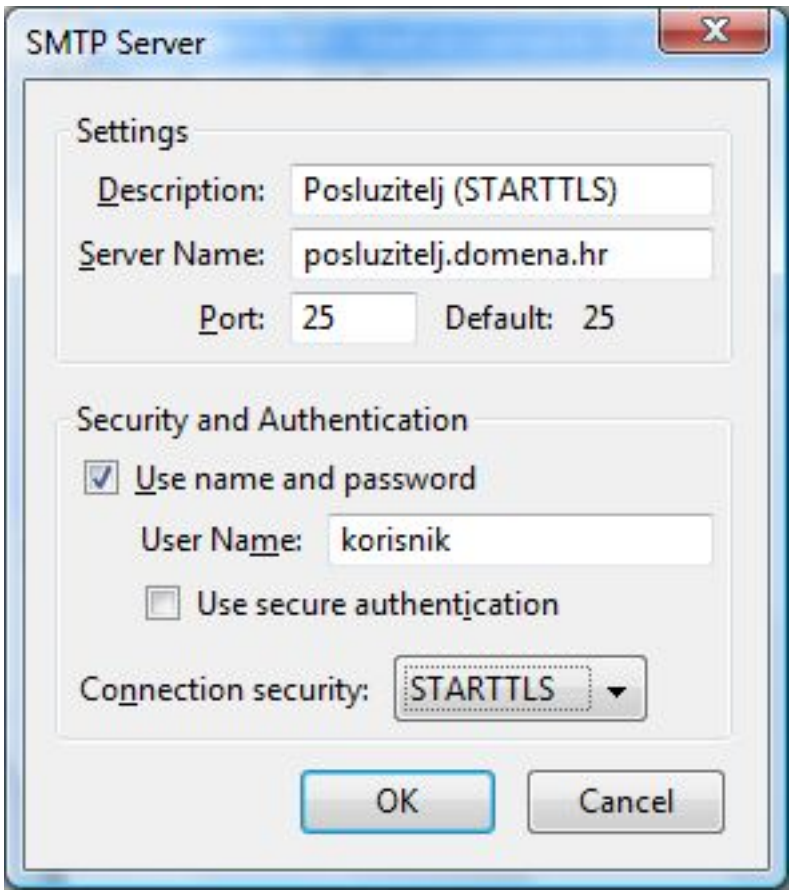
Za **Windows Mail** (gornji primjer je za POP3 protokol), odite na Tools -> Accounts -> <dvoklik na profil> -> Advanced -> Uključite "This server requires secure connection (SSL)" za "Outgoing server (SMTP)" -> Uključite "This server requires secure connection (SSL)" i za "Incoming mail (SSL)" (port će se promijeniti na 995, pop3s).

Za **Mozilla Thunderbird** dolazni poslužitelj, odite na: Tools -> Account Settings -> Server Settings željenog poslužitelja -> Security Settings -> Odaberite STARTTLS ili SSL/TLS

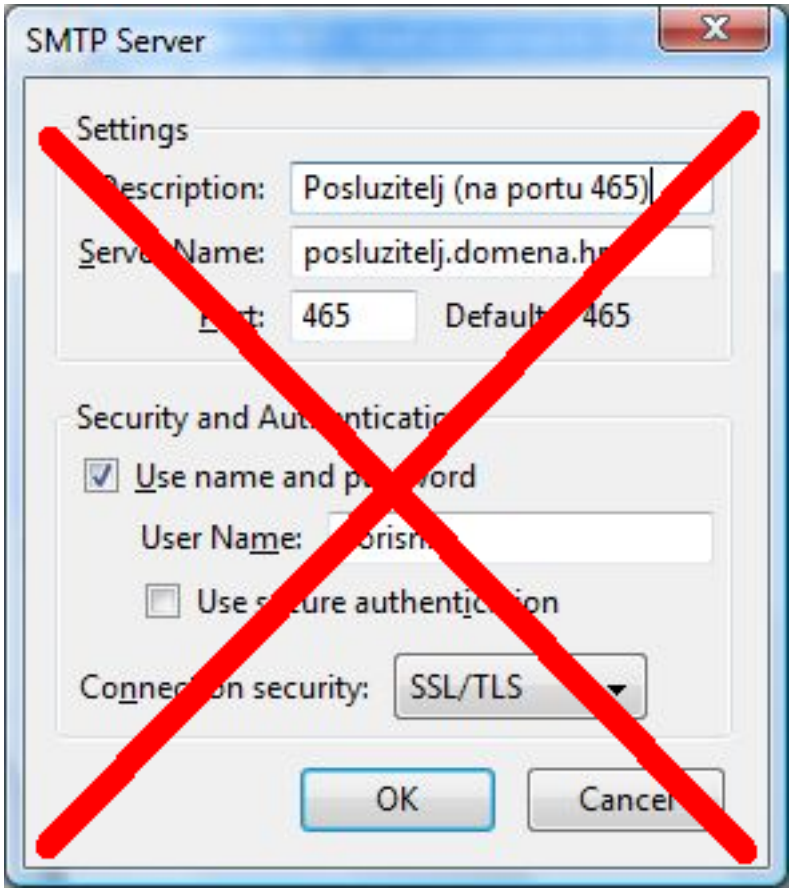
Ukoliko odaberete SSL/TLS, port će se promijeniti na 993 ili 995, u ovisnosti je li POP3 ili IMAP tipa.

Za odlazni poslužitelj, u opcijama s lijeve strane odaberite "Outgoing Server" -> <dvoklik na poslužitelj> -> odaberite STARTTLS ili SSL/TLS.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr



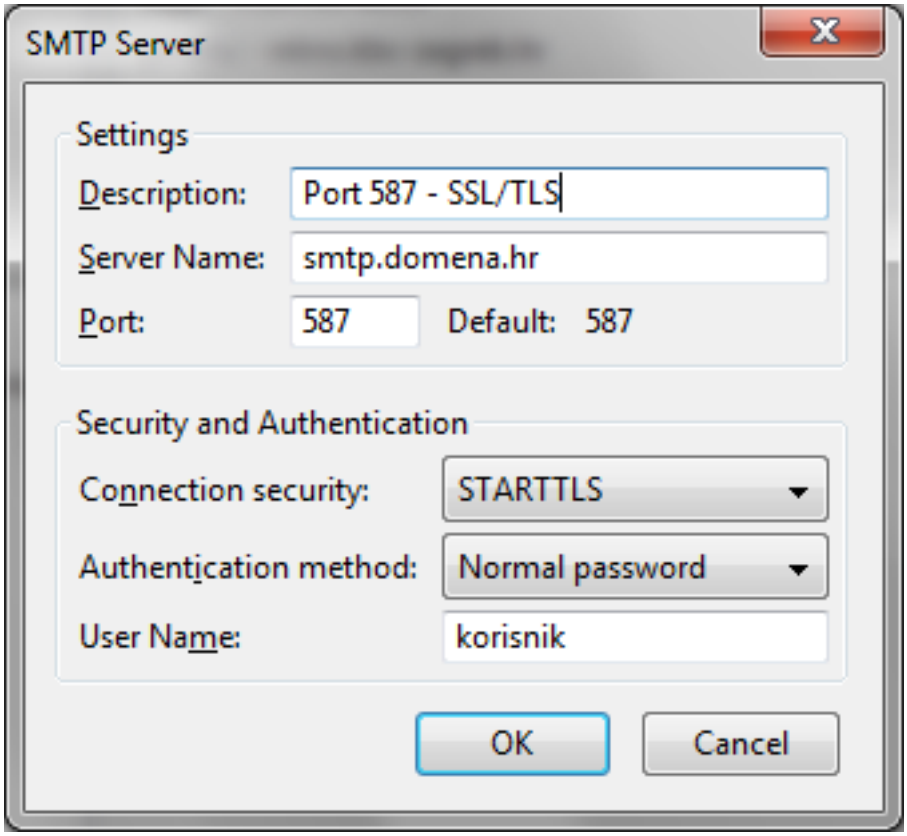
Ukoliko odaberete STARTTLS, port će ostati 25, a odaberete li SSL/TLS, port će se promijeniti na 465.



No, **port 465 se više ne rabi u ove svrhe**, štoviše, već je prenamijenjen za druge svrhe. **Port koji**

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

bi trebali rabiti je 587:



OSVJEŽENO: 2013-05-06

- Logirajte [1] se za dodavanje komentara

pet, 2010-09-17 14:58 - Željko Borš**Kuharice:** Linux [2]
Kategorije: Software [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr./node/771

Links
[1] https://sysportal.carnet.hr./sysportallogin
[2] https://sysportal.carnet.hr./taxonomy/term/17
[3] https://sysportal.carnet.hr./taxonomy/term/25

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr